PODER JUDICIÁRIO
DO ESTADO DO ACRE

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

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 11/2025

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

Processo Administrativo Nº 2025-415

Fornecer ao Poder Judiciário do Estado do Acre (PJAC) Serviços Especializados de Segurança Cibernética, abrangendo a operação de SOC e Blue Team, Cultura de Cibersegurança, Administração de SIEM, Threat Intelligence, Gestão de Vulnerabilidades e atividades Red Team.

Rio Branco/AC, 18 de Maio de 2026.

PODER JUDICIÁRIO
DO ESTADO DO ACRE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

O Poder Judiciário do Estado do Acre (PJAC) não possui, até o presente momento, uma estrutura técnica, operacional ou contratual que desempenhe as funções atribuídas a um Centro de Operações de Segurança (Security Operations Center – SOC), tais como: monitoramento contínuo de ativos, correlação de eventos de segurança, análise de anomalias, resposta a incidentes cibernéticos, gestão de vulnerabilidades e produção de inteligência proativa contra ameaças.

Essa ausência de um serviço de SOC constitui uma fragilidade crítica no modelo de proteção cibernética da instituição, sobretudo considerando o atual cenário nacional de ameaças avançadas persistentes, ransomware, vazamentos de dados e ataques de negação de serviço (DDoS) direcionados a órgãos públicos, em especial aos Tribunais. O histórico recente de incidentes de grande impacto ocorridos em outros Tribunais reforça a urgência de medidas estruturadas de defesa, resposta e recuperação.

A implementação de um SOC, por meio de contratação especializada, objetiva mitigar significativamente os riscos operacionais, institucionais e legais associados à ausência de monitoramento contínuo e de capacidade de resposta imediata a incidentes de segurança da informação. Este serviço proporcionará ao PJAC a visibilidade centralizada do ambiente tecnológico, permitindo a detecção precoce de comportamentos anômalos, a contenção rápida de ameaças, a coleta de evidências digitais e o registro adequado dos eventos para posterior auditoria, conformidade e lições aprendidas.

Além disso, essa iniciativa alinha-se às diretrizes normativas impostas ao Poder Judiciário brasileiro, notadamente:

- **Resolução CNJ nº 396/2021**, que estabelece a Política de Segurança da Informação no Poder Judiciário e impõe aos tribunais a responsabilidade de implementar medidas de monitoramento, resposta a incidentes, gestão de riscos, controle de acessos e uso seguro dos ativos de informação. O artigo 11, inciso IV, prevê explicitamente a necessidade de "monitorar continuamente os eventos de segurança nos ativos de informação";
- **Recomendação CNJ nº 73/2020**, que orienta os órgãos a instituírem estruturas e práticas de governança de TIC e segurança da informação baseadas em normas técnicas, frameworks reconhecidos (como ISO/IEC 27001 e NIST), e no uso de ferramentas especializadas para controle, auditoria e mitigação de riscos;
- **Lei Geral de Proteção de Dados Pessoais** (LGPD – Lei nº 13.709/2018), que estabelece, no art. 46, que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito.

O não atendimento a esses dispositivos pode implicar responsabilidades administrativas, cíveis e penais, além de comprometer a confiança da sociedade no Poder Judiciário enquanto guardião de dados sensíveis e garantidor de direitos fundamentais. A implementação de um SOC é, portanto, não apenas uma necessidade técnica e institucional, mas também um requisito de conformidade regulatória e de preservação da integridade dos serviços judiciais prestados à população acreana.

Adicionalmente, a ausência de um serviço especializado de monitoramento e resposta coloca o PJAC em desvantagem frente aos riscos cibernéticos modernos, como ataques fileless, engenharia social automatizada, comprometimento de

identidade e exploração de vulnerabilidades zero-day, os quais demandam capacidade de detecção em tempo real, análises automatizadas e respostas coordenadas, atividades tipicamente desempenhadas por um SOC.

Dessa forma, a contratação de um serviço de SOC visa prover resiliência, agilidade e governança à segurança cibernética institucional, fortalecendo as diretrizes de continuidade de serviços e protegendo a missão do PJAC frente às crescentes ameaças do ecossistema digital.

1.2. Identificação da demanda no Plano de Contratações de STIC

A demanda está formalmente identificada e contemplada no Plano de Contratações da área de Tecnologia da Informação e Comunicação (PAC SETIC/2026) do Poder Judiciário do Estado do Acre com registro no ID 6 do referido plano, bem como, constante no Plano Anual de Contratações 2026, o ID PCA no PNCP é 04034872000121-0-000001/2026, publicado em 04/02/2026, com ID do item no PCA 155 e classificado na Categoria/Grupo 648 - 3.3.90.40.24 - SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC.

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

Em um contexto cada vez mais digital e interconectado, a proteção das informações demanda uma estrutura operacional robusta, que vá além da atuação de equipes técnicas internas. Isso torna necessária a adoção de estruturas especializadas, como os Centros de Operações de Segurança — ou Security Operations Center (SOC) —, responsáveis pelo monitoramento contínuo dos ambientes tecnológicos.

O SOC é uma estrutura centralizada que realiza atividades constantes de detecção, análise e resposta a ameaças cibernéticas, com base em técnicas de correlação de eventos, automação de alertas e procedimentos de prevenção e contenção de incidentes de segurança.

Diante do avanço contínuo das técnicas de ataque e das tentativas de acesso não autorizado à informação, os SOCs tornam-se indispensáveis para proteger os dados, os ativos e a reputação das organizações. Em termos práticos, representam a linha de defesa mais crítica contra vazamentos, fraudes, interrupções e outras ameaças que podem comprometer operações essenciais.

Essas estruturas operam de forma ininterrupta, 24 horas por dia, todos os dias do ano, e contam com equipes altamente especializadas, com formação técnica, experiência prática e certificações reconhecidas no mercado. Ao contrário de outras áreas da TI, onde tecnologias podem permanecer estáveis por anos, o cenário de segurança é dinâmico, com vetores de ataque evoluindo constantemente. Por isso, a ausência de uma estrutura dedicada à segurança da informação, como um SOC, aumenta significativamente a exposição a riscos.

Considerando o modelo de Arquitetura de Segurança Adaptativa proposto pelo Gartner, o sucesso das organizações no enfrentamento das ameaças cibernéticas está diretamente atrelado à capacidade do SOC em atuar de forma abrangente nas quatro frentes essenciais: prever, predizer, detectar e responder a incidentes. Essa abordagem integrada é fundamental para antecipar riscos, reduzir impactos e manter a resiliência operacional diante de um cenário de ameaças cada vez mais sofisticadas, conforme ilustrado na figura abaixo.

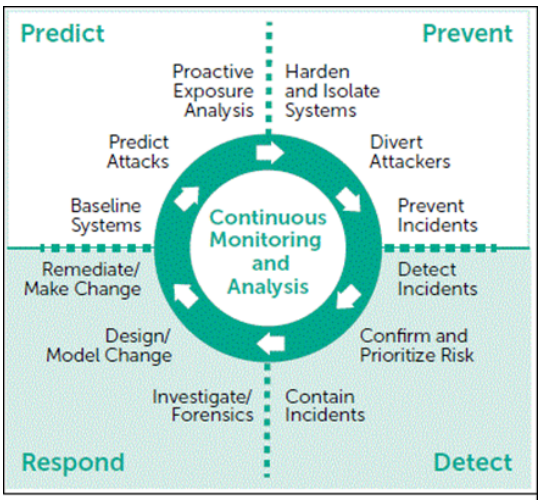


Figura 1: Designing an Adaptive Security Architecture for Protection from Advanced Attacks", publicado em fevereiro de 2014, e referenciado na brochura Kaspersky for Security Operations Center.

Fica evidente, mais uma vez, que a ausência de uma estrutura dedicada exclusivamente à segurança da informação compromete seriamente a capacidade de uma organização em assegurar os quatro eixos fundamentais do modelo adaptativo: predição, prevenção, detecção e resposta eficaz. A tentativa de atingir esses objetivos apenas com recursos internos dispersos exige um esforço desproporcional, altamente oneroso e, na maioria dos casos, insustentável a longo prazo.

Para complementar as atividades desempenhadas por um SOC, outras estruturas e modelos operacionais são comumente adotados, como as equipes Blue Team, Red Team e Purple Team. A seguir, apresentam-se as definições desses times segundo a SANS (System Administration, Networking and Security), reconhecida internacionalmente como referência na área de segurança da informação:

- **Blue Team (Defesa):** “Seu foco é defender a organização de ataques digitais/cibernéticos. Embora qualquer ação que melhore a postura defensiva possa ser considerada parte do Blue Team, há um foco claro na detecção e mitigação de ataques.” (Tradução livre)
- **Red Team (Ataque):** “São aqueles que assumem o papel de adversários. Em essência, o Red Team executa ações ofensivas para testar e desafiar as defesas implementadas pela organização.” (Tradução livre)

Com base nas definições apresentadas pela SANS, pode-se resumir que o Blue Team representa a linha de defesa da organização, o Red Team executa simulações ofensivas com o objetivo de testar essas defesas, e o Purple Team atua de forma colaborativa entre os dois, garantindo que os aprendizados obtidos a partir dos testes se traduzam em melhorias concretas na segurança.

A realização de testes de penetração (Penetration Tests) em consonância com a equipe de defesa caracteriza, na prática, uma atuação em modelo de Purple Team, promovendo um ciclo de melhoria contínua na segurança cibernética da organização.

É importante destacar que esse conceito vai além da atuação de uma equipe técnica específica. O Blue Team se faz presente em todas as etapas da arquitetura adaptativa proposta pelo Gartner (Figura 1), assim como em diversas frentes operacionais do SOC. No entanto, enquanto o Blue Team possui uma atuação mais preventiva e proativa, focada na preparação e fortalecimento das defesas, o SOC se responsabiliza pela monitoração contínua e pela resposta reativa a incidentes, desempenhando papel central na sustentação da segurança operacional da organização.

A atuação integrada do Blue Team com equipes de Pentest eleva o nível de maturidade da organização no eixo de prevenção, permitindo a identificação proativa de vulnerabilidades e possíveis vetores de ataque. Essa abordagem investigativa, realizada antes da concretização de incidentes, fortalece a postura defensiva da organização e antecipa medidas corretivas, reduzindo significativamente o risco de comprometimento.

1.3.2. Definição e Especificação de Requisitos

1.3.2.1. Serviços Gerenciados de Segurança Cibernética

A prestação dos serviços gerenciados de segurança cibernética deverá contemplar os seguintes componentes integrados:

1.3.2.2. Monitoramento, Detecção e Resposta a Incidentes (Blue Team)

Prestação de serviços de análise, correlação, contenção, remediação e documentação de incidentes de segurança da informação, operando de forma contínua (24x7) por meio de um Centro de Operações de Segurança (SOC).

A execução deverá observar os principais frameworks de resposta a incidentes, como NIST SP 800-61 e MITRE ATT&CK, bem como boas práticas amplamente reconhecidas no mercado. A atuação deverá garantir:

- Aumento da visibilidade sobre eventos e atividades críticas;
- Detecção e resposta em tempo real a incidentes de segurança;
- Aplicação de inteligência contra ameaças avançadas, com uso de análises comportamentais e indicadores de comprometimento (IoCs);
- Apoio às equipes internas nas tratativas proativas e reativas a incidentes.

1.3.2.3. Administração da Solução de SIEM

A solução de SIEM (Security Information and Event Management) será fornecida pela Contratante. Caberá à empresa Contratada:

- Operar, gerenciar, atualizar e aprimorar continuamente o SIEM;
- Correlacionar eventos de múltiplas fontes monitoradas;
- Prover ajustes de regras e painéis com foco em reforçar a postura de segurança institucional.

1.3.2.4. Inteligência Cibernética (Threat Intelligence)

Contratação de solução e serviços especializados de inteligência cibernética, com foco em:

- Investigação e monitoramento de fontes abertas (OSINT);
- Análise de redes sociais, fóruns, deep web e dark web;
- Coleta, correlação e disseminação de indicadores relevantes de ameaça;

- Apoio à antecipação de ataques e mitigação de riscos emergentes.

1.3.2.5. Gestão de Vulnerabilidades

Contratação de solução e serviços especializados em gestão de vulnerabilidades, com foco em:

- Descoberta e inventário contínuo de ativos tecnológicos;
- Identificação, análise e priorização de vulnerabilidades em sistemas operacionais, aplicações, serviços e dispositivos de rede;
- Integração com bases de conhecimento atualizadas (CVE, CISA Known Exploited, etc.) para correlação de riscos;
- Apoio à definição de planos de remediação com base em criticidade, risco e impacto institucional;
- Acompanhamento da aplicação de patches e correção de falhas, com geração de relatórios de conformidade;
- Produção de indicadores e métricas de exposição a vulnerabilidades, para apoio à gestão estratégica de riscos cibernéticos.

1.3.2.6. Testes de Invasão (Red Team)

Execução de testes de invasão controlados com o objetivo de:

- Identificar, mapear e explorar vulnerabilidades em sistemas, processos e infraestrutura;
- Avaliar a eficácia dos controles de segurança existentes;
- Simular ataques reais (internos e externos), respeitando os limites acordados contratualmente.

Entregas mínimas:

- Relatórios técnicos e executivos com detalhamento das vulnerabilidades identificadas;
- Evidências documentadas de explorações bem-sucedidas;
- Análise de impacto e criticidade dos achados;
- Recomendações técnicas para correção e mitigação de riscos.

Normas de referência:

- As atividades deverão seguir padrões e boas práticas internacionais, como OWASP, MITRE ATT&CK, NIST e outras aplicáveis.

1.3.2.7. Cultura de Cibersegurança: Ações e Plataforma de treinamento de Cibersegurança

Contratação de serviços especializados em conscientização e educação em segurança da informação, com foco em:

- Elaboração e execução de campanhas educativas, alinhadas ao contexto institucional;
- Desenvolvimento de materiais de apoio (cartilhas, vídeos, infográficos e newsletters) com linguagem acessível e conteúdo técnico validado;
- Realização de simulações práticas de incidentes (ex.: phishing, engenharia social) para avaliação do comportamento dos usuários;
- Promoção de eventos temáticos, como a Semana de Segurança da Informação e atividades de Segurança Cibernética;
- Fornecer ambiente, interface e material didático sobre cibersegurança, integralmente em português (pt-BR).
- Garantir licenças para todos os usuários do CONTRATANTE, até o limite contratado.
- Consolidação de relatórios de efetividade e indicadores de engajamento, subsidiando a melhoria contínua das políticas e práticas de segurança.

1.3.2.8. Gestão e Controle dos Serviços

A empresa Contratada será responsável por:

- Atuar como ponto único de contato junto à Contratante;
- Monitorar o desempenho global dos serviços prestados;
- Assegurar a entrega conforme prazos, metas e padrões acordados;
- Apresentar relatórios e indicadores de desempenho (KPIs) para avaliação objetiva;

Propor ajustes, promover melhorias contínuas e garantir conformidade com os SLAs estabelecidos. A gestão deverá promover a rastreabilidade, transparência e excelência na execução contratual, alinhando-se às diretrizes estratégicas da Contratante.

A gestão deverá promover a rastreabilidade, transparência e excelência na execução contratual, alinhando-se às diretrizes estratégicas da Contratante.

1.3.3. Requisitos Funcionais

1.3.3.1. Requisitos de Arquitetura Tecnológica (Configuração):

Os requisitos gerais dos serviços, define os requisitos obrigatórios para todos os serviços que compõem o objeto .

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA.

A CONTRATANTE deverá possuir acesso a todas as ferramentas com perfil de administração máxima.
Todos os dados coletados, analisados e armazenados são de propriedade do CONTRATANTE.

A CONTRATADA deverá entregar integralmente ao CONTRATANTE todos os dados, evidências, registros, indicadores, painéis, configurações, relatórios técnicos e artefatos produzidos durante a execução do serviço, assegurando a preservação da cadeia de custódia das informações e o atendimento às exigências de integridade e rastreabilidade, em caso de rescisão contratual, término ou não renovação do contrato.

Caberá a CONTRATADA adotar as boas práticas de governança de continuidade, garantindo que toda a infraestrutura, documentação, base de conhecimento e elementos técnicos da solução SIEM estejam plenamente documentados, preservados e sob domínio institucional, viabilizando a continuidade da operação pelo CONTRATANTE ou por outro prestador de serviço, sem impacto operacional ou perda de informações.

Os atendimentos referentes aos Serviços de testes de invasão (Red Team), conforme necessidade e indicação da CONTRATANTE respeitando os volumes descritos.

Todos os serviços e atendimentos serão prestados remotamente, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

Todos os serviços poderão ser prestados em qualquer unidade do CONTRATANTE, quando solicitado, em casos excepcionais.

O horário padrão de trabalho será de segunda a sexta-feira das 07h00 às 14h00 horário do Acre.

Caberá à empresa CONTRATADA a responsabilidade de prestar suporte remoto à equipe da CONTRATANTE durante o expediente do PJAC, com suporte contínuo à operação local.

A empresa CONTRATADA deve disponibilizar três tipos de canais de comunicação, especificamente:

Telefone linha telefônica 0800: Para contato direto e imediato, disponível 24 horas por dia, 7 dias por semana, permitindo comunicação rápida em casos de urgência. Com atendimento em português.
E-mail com domínio registrado e de propriedade da CONTRATADA: Para solicitações formais, documentação de incidentes e comunicação de problemas não imediatos, garantindo um registro escrito das interações.
Portal de Atendimento: Sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI).

Independente do canal de comunicação utilizado pelo CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, imaginando que o CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, assim que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo B: via e-mail.

A solução de ITSM (Information Technology Service Management) adotada pela CONTRATADA deverá possuir capacidade de integração com a solução de ITSM utilizada pela CONTRATANTE, ServiceNow, garantindo a interoperabilidade entre as plataformas a referida integração deverá ser implementada sem qualquer ônus adicional à CONTRATANTE, sendo de inteira responsabilidade da CONTRATADA viabilizar os recursos técnicos necessários para sua realização.

O CONTRATADO deverá utilizar-se de Centros de Operação de Segurança próprios.

A empresa CONTRATADA deverá adotar práticas de governança visando garantir o adequado controle, acompanhamento e qualidade dos serviços prestados. Para isso, deverá:

- Designar um Coordenador Técnico responsável pela interlocução direta com a equipe da CONTRATANTE.
- Realizar reuniões periódicas de acompanhamento dos serviços, com frequência mínima mensal ou sempre que solicitado pela CONTRATANTE.
- Elaborar relatórios gerenciais contendo indicadores, status das atividades, riscos, não conformidades, melhorias implementadas e recomendações.
- Garantir o registro, controle e histórico de todas as solicitações, atividades realizadas e incidentes tratados durante a vigência do contrato.
- Garantir alinhamento das entregas com as boas práticas de mercado (ITIL, ISO 27001, MITRE, OWASP, entre outras, quando aplicável).
- Prover plano de ação e melhoria contínua dos serviços, quando identificado pela CONTRATANTE ou pela própria CONTRATADA.

Atendimento Presencial: Durante o horário regimental de expediente da CONTRATANTE, o atendimento poderá ser realizado presencialmente nas dependências da CONTRATANTE, em casos excepcionais. Remotamente a Contratada deve garantir o apoio às atividades de monitoramento, análise, investigação e resposta a incidentes de segurança.

Atendimento Remoto: Durante e fora do horário regimental de expediente da CONTRATANTE, incluindo períodos noturnos, finais de semana e feriados, o atendimento deverá ocorrer de forma remota, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante toda a vigência do contrato, nas dependências da Contratante.

1.3.3.1.1. CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)
O Centro de Operações de Segurança (SOC) da empresa CONTRATADA deve conter sistemas avançados de vídeo Wall

e painéis com TVs interativas, permitindo que os operadores realizem o monitoramento de incidentes de segurança em tempo real. Este arranjo deve facilitar a rápida identificação e reação a potenciais ameaças, assegurando uma gestão eficaz de incidentes.

O Centro de Operação deve ser situado no Brasil e deve estar plenamente operacional desde a data de abertura da licitação, com operação contínua e eficiente.

A CONTRATADA deverá indicar o local onde possui sua estrutura de central de atendimento, sendo que este deve estar estabelecido no Brasil e estará sujeito à diligência por parte da CONTRATANTE.

Todos os atendimentos devem ser iniciados no Brasil e no idioma português do Brasil.

Sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas.

Filmar toda a área, mantendo as imagens armazenadas pôr no mínimo 60 (sessenta) dias.

Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC.

O perímetro físico do SOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido.

Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

Ter controle de acesso físico com pelo menos 2 (dois) dos seguintes fatores de autenticação, a saber:

- Cartão de identificação magnético;
- Biometria de leitura de digital;
- Identificação facial.

Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

Possuir registro de entrada e saída de pessoas mantidos por pelo menos 60 dias.

Possuir sistemas redundantes para armazenamento de dados.

Possuir sistemas de alimentação de energia redundantes, contendo geradores de energia.

Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados.

Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços.

Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs do inglês Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador;

Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas desautorizadas.

Possuir ambiente, onde seja possível reproduzir os incidentes e problemas do CONTRATANTE, sem que haja impacto na operação do SOC e/ou do próprio CONTRATANTE.

A CONTRATADA deverá possuir plano de contingência de atendimento em caso de impedimento de acesso a Central de Serviços, sendo aceito o atendimento em modo contingência somente em casos de desastre ou previamente justificados e aprovados pela CONTRATANTE.

Para garantir a qualidade e disponibilidade dos serviços remoto, deverá entre o CONTRATANTE e o SOC da CONTRATADA, será de responsabilidade e propriedade da CONTRATADA os equipamentos e/ou soluções para estabelecer as VPNs. Caberá ao CONTRATANTE apenas a disponibilidade de infraestrutura física no seu Data Center, infraestrutura física leia-se: energia elétrica, espaço no rack, climatização adequada, e sistemas de combate a incêndio. Tais equipamentos e/ou soluções devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

Além disso, o termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.

Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

O SOC da CONTRATADA deverá ter a certificação ISO/IEC 27001 vigente ou apresentar uma declaração que ateste estar em fase de implementação do Sistema de Gestão de Segurança da Informação ISO/IEC 27001, com previsão de realização da auditoria de certificação no primeiro ano de vigência do contrato. A declaração deverá ser emitida por uma empresa certificada que siga os padrões ISO 9000, CMMI, MPS.BR, Certics, Scrum e ITIL. Para aceitação da referida declaração, a mesma deve estar acompanhada das certificações da empresa.

1.3.3.1.1.1. SERVIÇO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.

Para a prestação dos serviços de monitoramento e resposta a incidentes dos ativos de segurança da CONTRATANTE, a CONTRATADA deverá disponibilizar, por meio de seu Centro de Operações de Segurança (SOC), todos os recursos necessários, incluindo infraestrutura, ferramentas tecnológicas e equipe técnica especializada, garantindo o atendimento nas seguintes modalidades:

Atendimento Presencial: Durante o horário regimental de expediente da CONTRATANTE, o atendimento poderá ser realizado presencialmente nas dependências da CONTRATANTE, em casos excepcionais. Remotamente a Contratada deve garantir o apoio às atividades de monitoramento, análise, investigação e resposta a incidentes de segurança.

Atendimento Remoto: Durante e fora do horário regimental de expediente da CONTRATANTE, incluindo períodos noturnos, finais de semana e feriados, o atendimento deverá ocorrer de forma remota, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante toda a vigência do contrato, nas dependências da Contratante.

A CONTRATADA deve garantir a continuidade dos serviços de monitoramento e resposta a incidentes, independentemente da modalidade de atendimento, zelando pela segurança dos ativos da CONTRATANTE em tempo integral.

Os atendimentos referentes ao item contratado são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados.

Quanto a resposta a incidentes, ao identificar o incidente a Equipe da contratada fará um plano de ação, o processo de resposta a incidentes seguirá as etapas: Preparação, Detecção e Análise, Contenção, Erradicação, Recuperação e Pós-

Incidente. Ao ser identificado um incidente: A equipe técnica do SOC (níveis N1 a N3) desenvolverá um plano de resposta estruturado.

A Contratante deve ser notificada formalmente e instruída quanto às ações corretivas e mitigatórias recomendadas; A tratativa será registrada conforme os procedimentos internos do SOC, com documentação em playbooks e sistema ITSM; Os Serviços contemplam os seguintes entregáveis:

Os Serviços contemplam os seguintes entregáveis:

- Receber e efetuar a triagem de chamados de segurança cibernética.
- Realizar o primeiro atendimento de reportes de incidentes de segurança cibernética.
- Elaborar o detalhamento dos eventos de alertas, anomalias e incidentes a fim de encaminhar ou escalar para demais níveis de atuação do SOC ou indicados pela CONTRATANTE.
- Notificar e registrar apropriadamente eventos de segurança cibernética conforme a severidade.
- Notificar a(s) área(s) solucionadora(s), sejam elas da CONTRATADA, do CONTRATANTE ou qualquer outro fornecedor autorizado pelo CONTRATANTE, através dos processos apropriados para iniciar a resolução;
- Validar e executar instruções de trabalho relacionadas disponibilizadas pela CONTRATANTE.
- Manter o ambiente alinhado conforme os procedimentos operacionais e padrões de arquitetura definidos pelo CONTRATANTE;
- Analisar o histórico de eventos, utilizando as melhores práticas de gestão da qualidade, identificando relações entre as causas raiz e que possibilitem a aplicação do processo de gestão de problemas para sua eliminação.
- Implementar o modelo de gestão de indicadores de qualidade para facilitar a visibilidade da qualidade e melhoria contínua;
- Utilizar metodologias ágeis para controlar a evolução da gestão de todo o ambiente através
- Deverá avaliar situações em que o ambiente esteja sob ataque ou risco iminente de ataque, provendo o conhecimento e experiência necessários para as medidas de preparação, mitigação, contenção, defesa e resposta apropriadas quando possível executar os pontos listados;
- Deverá propor a criação, alteração, customização, renomeação e/ou remoção de regras, para melhorar os alertas, diminuir a quantidade falsos-positivos, aumentar sua qualidade/efetividade
- Sugerir elaboração, mudanças e manutenção de playbooks para cada caso de uso;
- Atender à eventos de segurança, os quais possuem instruções indicadas em playbooks e runbooks (que serão fornecidos pela CONTRATADA, em conformidade com a CONTRATANTE)
- Disponibilizar pessoal qualificado para o desempenho das atividades e deve oferecer pessoal suficiente para que não haja interrupção na monitoração das atividades;
- Efetuar passagem de turno acompanhando os eventos de segurança em curso e realizar “follow-ups”, de modo que exista acompanhamento integral até sua conclusão.
- Prestar suporte e/ou apoio necessário, sempre que solicitado, a processos de automação das atividades relacionadas ao processo do SOC.
- Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;
- Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;
- Monitorar de forma contínua e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;
- Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;
- Elaborar e propor plano de execução dos serviços de monitoramento, detecção e resposta a incidentes de segurança da informação;
- Elaborar e propor plano de contingência e continuidade de negócios;
- Informar no plano de execução dos serviços os responsáveis pelas ações por parte da CONTRATADA e CONTRATANTE, com os respectivos meios de comunicação;

- Executar outros serviços correlatos à supervisão dos profissionais na execução dos serviços;
- Deverá apoiar e atuar no processo de resposta a Incidentes de Segurança, com os relatórios extraídos da ferramenta e processos como varredura e análise de logs nas soluções de segurança da informação;
- Deverá criar salas de crises e/ou reuniões para tratar incidentes ou quando solicitado pela CONTRATANTE.
- Deverá elaborar o detalhamento dos eventos de alertas, anomalias e incidentes, em formato de dossiê ou relatório detalhado.
- Realizar auditorias na área de segurança da informação, quando necessário.
- Apoiar em respostas a órgãos de controle e fiscalização, quando necessário.
- Utilizar todas as ferramentas deste documento e as ferramentas disponibilizadas pelo

1.3.3.1.2. ADMINISTRAÇÃO DA SOLUÇÃO DE SIEM.

A CONTRATADA será responsável pela sustentação, operação, administração e evolução da solução de SIEM da CONTRATANTE (Wazuh), garantindo a sua correta operação, disponibilidade e evolução contínua, de acordo com as melhores práticas de mercado em segurança da informação e governança de ambientes SIEM.

Entre as atividades previstas neste item, destacam-se:

Administração e operação da solução Wazuh, abrangendo a gestão dos agentes instalados nos ativos de tecnologia da CONTRATANTE, incluindo instalação, atualização, troubleshooting e monitoramento do funcionamento desses agentes.

Criação, customização e manutenção de Decoders e Rules específicos, adequados às necessidades do ambiente da CONTRATANTE, visando ampliar a capacidade de detecção de eventos, anomalias e comportamentos suspeitos.

Aplicação das melhores práticas de segurança para garantir a integridade, desempenho e eficiência da solução, incluindo a realização de ajustes e melhorias constantes na configuração da ferramenta.

Realização de análises periódicas de eficiência das regras e decoders implementados, com proposta de melhorias, ajustes e otimizações, visando maior precisão na detecção de eventos de segurança.

Apoio à investigação e resposta a incidentes, com base nas informações geradas pela solução Wazuh.

Geração de dashboards, relatórios gerenciais e operacionais, sempre que solicitado pela CONTRATANTE.

Apoio na realização de upgrades, atualizações de versão e correções de segurança da solução, em conjunto com a equipe da CONTRATANTE, sempre que necessário.

Realizar integração com serviço de diretório (Active Directory).

Customizar a ferramenta para ser capaz de coletar logs de firewalls, antivírus, IDSs, Proxy, servidores DNS, load balancers e demais dispositivos de segurança.

Deve coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta.

Deve criar integração com as soluções de ITSM de centro de operações de segurança (Security Operations Center - SOC).

Customizar a plataforma de acesso via browser WEB para realizar investigações, gestão de incidentes, gestão de alertas, gestão de relatórios, administração dos componentes e gestão de inteligência externa.

A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados.

Customizar solução de SIEM para possuir funcionalidade de analisar e correlacionar logs, além de trazer contextualização e enriquecimento de dados para análises, podendo ser fornecido através da plataforma especificada de monitoramento.

Configurar procedimentos de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.

Suportar de forma nativa o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento off-line para possível restauração em WARM).

Suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave.

A solução de SIEM deverá ser capaz de analisar e correlacionar logs, além de trazer contextualização e enriquecimento de dados para análises que serão realizadas pelo time de reposta a incidentes;

Sustentar e operar as soluções de SIEM que poderá utilizar agentes para as coletas dos dados;

A coleta de eventos de dispositivos (ativos geradores de eventos) não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como CSV, arquivo texto, XML, SYSLOG, ODBC, JDBC, SNMP Trap v1, v2c e v3, entre outros;

Caso a fonte geradora de eventos não possuía capacidade de gerar eventos com riqueza de detalhes ou úteis para o processamento do SIEM, a CONTRATADA deverá disponibilizar módulos para coleta de eventos em endpoint e em rede;

A Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenados na Solução Integrada de SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças;

O acesso a solução de monitoramento deverá ser realizado apenas pela equipe de segurança da CONTRATANTE e a equipe de serviço de SOC da CONTRATADA;

Customizar e operar a ferramenta para a monitoração de alertas de segurança, a detecção consiste em avaliar os alertas de segurança dos sensores buscando indicadores de comportamentos maliciosos que ultrapassem os limites estabelecidos no baseline. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados. Os alertas devem indicar minimamente:

- Ataques de força bruta com e sem sucesso;
- Falhas de autenticação que indiquem suspeita de roubo de identidade;
- Infecção de equipamentos por vírus;
- Comprometimento de ativos da rede;
- Realização de ações suspeitas por parte de usuários privilegiados;
- Alertas de operação de serviços, como interrupções e falhas;
- Ataques de negação de serviço;
- Ataques comuns em aplicações WEB, como XSS e SQL injection;
- Atividades de botnets;
- Exploração de vulnerabilidades (depende de agente).

A CONTRATADA deve configurar proativamente na solução de SIEM, regras de correlacionamento, baseadas em boas práticas de segurança e bases de conhecimento próprias, customizadas para o ambiente da CONTRATANTE, monitorando minimamente:

- Detecção de rootkits conhecidos;

- Detecção de não conformidades em ativos;
- Detecção de vulnerabilidades em ativos através de agentes; Integridade de arquivos críticos e de configuração através de agentes;
- Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis);
- Detecção de anomalias com base em tendências (Trend Behavior Analisys);
- Detecção de padrões em logs observados e não observados;
- Detecção de padrões baseados em uma sinalização específica (thresholds);
- Detecção de padrões baseados em valores unitários;
- Detecção de ameaças que saem de normas básicas (whitelisting).

A CONTRATADA ficará, durante a vigência contratual do presente objeto, incumbida de realizar parametrizações, customizações e manutenções na plataforma de SIEM.

A CONTRATADA deverá realizar atividades de evolução do SIEM, para atendimento de ajustes, implantação de novas tecnologias, melhorias ou necessidades específicas no ambiente tecnológico do SIEM.

A infraestrutura necessária para a operação da solução Wazuh será disponibilizada pela CONTRATANTE.

Os atendimentos referentes ao item contratado são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados.

1.3.3.1.3. SERVIÇOS DE MONITORAMENTO EM FONTES ABERTAS E INTELIGÊNCIA CIBERNÉTICA (THREAT INTELLIGENCE)

Deverá ser fornecido o serviço de Inteligência em Ameaças Cibernéticas (Threat Intelligence), através de uma Solução que atendam os requisitos abaixo:

- Capacidade para operação de 05 usuários, com acessos simultâneos.
- A operação da ferramenta será realizada pelo time de SOC da empresa CONTRATADA em regime 24x7;
- O funcionamento da plataforma deverá ser em nuvem com acesso realizado via web no modelo SaaS (Software-as-a-Service);
- Deve possuir interface de gerenciamento no idioma português do Brasil, inglês e espanhol;
- Ter interface web via cloud pública;
- Ser compatível com navegadores Mozilla Firefox, versão 60.0 ou superior, Google Chrome versão 65 ou superior;
- Uma vez que os eventos forem coletados pela ferramenta, estes devem permanecer disponíveis por tempo indeterminado, mesmo que haja remoção original do conteúdo;
- Deve possibilitar integração com MISP;
- A plataforma deve ter mecanismo de armazenamento de logs de acesso dos usuários por um período mínimo de 1 ano;
- A solução deverá possuir, pelo menos, 6 bilhões de eventos coletados e indexados;
- A solução deverá possuir, pelo menos, 20 (vinte) milhões de atores maliciosos monitorados;
- Os logs de acesso devem ser armazenados com no mínimo as seguintes informações:
    - Usuário; Atividade executada;
    - IP de acesso;
    - Data e hora de acesso;
    - User Agent e a plataforma deve disponibilizar manual do usuário;
- Possuir análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades:
    - Visualização de perfis relacionados a palavras-chaves;

  - Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;
  - Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das
  - informações relacionadas.
- Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;
- Exportar as informações identificadas em relatórios via XLSX, JSON, CSV e PDF.
- Deve realizar etapa de pós-processamento nos eventos coletados: Realização de OCR (Optical Character Recognition) nas imagens indexadas pela plataforma; Transcrição dos áudios e vídeos indexados na plataforma;
- Detecção automática de linguagem; Extração de metadados relevantes dos eventos para cada fonte passível de coleta;
- Deve realizar detecção automática, com uso de Inteligência Artificial de, pelo menos:
- Credenciais vazadas; Os metadados coletados em cada eventos devem incluir no mínimo:
  - Data original do evento;
  - Hash do conteúdo que permite a desduplicação de informações disponíveis;
  - Data de indexação do evento;
  - Fonte original da informação;
  - Robô responsável pela coleta da informação;
  - Informações pertinentes da fonte que originou o evento;
- Disponibilizar mecanismo para busca das informações permitindo:
  - Busca por intervalo de data; Busca por metadados específicos;
  - Busca por fontes de informação;
  - Busca por palavras chaves.
- Disponibilizar através de interface web, a busca utilizando mecanismos como:
  - Proximidade; Fuzzy (difusa); Lógica binária; Expressões regulares (regex); Operadores lógicos (“AND, “OR” e “NOT”);
  - Permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga;
  - Permitir a escolha da quantidade de resultados por página;
  - Permitir salvar o resultado da pesquisa;
  - Deve possuir mecanismo que permita que buscas criadas possam ser salvas para uso posterior;
  - Deve permitir a identificação de links patrocinados;
  - Deve permitir a identificação de perfis falsos;
  - Deve permitir a identificação de campanhas e ataques “zeroday”;
  - Deve permitir a identificação de campanhas de phishing;
  - Deve permitir a identificação de defacement de páginas;
  - Deve permitir a identificação da comercialização ilegal de vulnerabilidades ou ativos de interesse da CONTRATANTE;
  - Deve permitir o acompanhamento de discussões de assuntos que coloquem em risco os ativos, pessoas ou serviços de interesse da CONTRATANTE;
  - Deve identificar a emissão de certificados de domínios monitorados;
  - Deve identificar a criação de domínios de recursos monitorados;
  - Deve realizar consulta Whois de forma automática nos Bots que realizam coletas de domínios;
  - Deve processar URLs de maneira automática para a detecção de phishings aplicando técnicas de machine-learning;
  - Deve guardar preview dos sites de phishing;
  - Deve fazer o download automático do código fonte de sites detectados como phishing;
  - A ferramenta deve permitir o drill-down das pesquisas utilizando filtros inclusivos e exclusivos;

- Possuir um dashboard para análise dos dados coletados com no mínimo as seguintes informações: Gráfico com a quantidade de informações de acordo com as palavras ou termos buscados; Divisão dos dados por tipo de dado encontrado (imagem, texto, áudio, etc); Principais perfis; Principais fontes de dados; Principais grupos.
- Permitir a busca de perfis específicos, usando nome/apelido, número de telefone ou e-mail, com no mínimo os seguintes campos: Fonte; Nome; Apelido; Telefone; Grupos.
- Possuir um painel de visualização de todas as pesquisas salvas, possibilitando a execução dessas pesquisas salvas;
- Permitir a pesquisa por uma busca salva específica;
- Permitir filtrar as buscas salvas por empresa;
- Permitir a edição e atualização de uma busca salva;
- Deve permitir a criação/alteração/exclusão de variáveis na plataforma, possibilitando gerenciamento de termos ou buscas dentro dessa variável;
- Deve permitir a notificação de eventos relevantes em forma de ocorrências para outros usuários em times dentro da organização;
- Deve permitir a associação de múltiplos eventos a uma mesma ocorrência;
- Deve ser possível visualizar diretamente nos eventos a(s) ocorrência(s) em que o dado evento foi associado;
- As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas;
- O campo de descrição das ocorrências deve permitir a cópia e cola de imagens de forma que possam ser vistas in-line;
- As ocorrências devem permitir o upload de arquivos como anexo;
- Deve ser possível notificar via e-mail e via WebHook a criação e modificação de ocorrências aos times envolvidos;
- Deve permitir a criação de títulos para fácil identificação das ocorrências;
- Deve possuir um painel de gerenciamento das ocorrências, possibilitando a busca com as seguintes opções:
- Busca por palavras-chave;
- Busca por número da ocorrência;
- Deve ser possível buscar nos metadados dos eventos dentro das ocorrências.
- Possuir um filtro para busca de ocorrências com no mínimo as seguintes opções: Categoria; Status; Período; Responsável pela criação; Time responsável.
- No painel de gerenciamento, deve ser possível visualizar a quantidade total de ocorrências e ordenar por data e prioridade;
- Permitir a adição de IOCs dentro das ocorrências;
- Permitir visualizar um histórico com log de alterações das ocorrências;
- Deve permitir a classificação das ocorrências através de categorias;
- Deve permitir a classificação das ocorrências de acordo com a criticidade;
- Deve permitir a definição de times responsáveis por cada ocorrência;
- Deve permitir a adição de comentários ilimitados a cada ocorrência;
- Deve permitir filtrar por organização e empresas;
- Possibilidade de filtrar por períodos e empresas;
- Deve permitir filtrar por organização e empresas
- Além dos eventos, a ferramenta deve contar com relatórios periódicos, desenvolvidos pelo time de inteligência do fabricante, com informações, ameaças, botnets, tendências, campanhas de hacktivismo em andamento, perfis de atores maliciosos, indicadores de comprometimento e aviso informativos gerais;

- Os relatórios devem ser gerados sempre que identificados um assunto pertinente relacionado aos assuntos acima e deve possuir ao menos 7 relatórios publicados por semana;
- Deve permitir a busca desses relatórios por palavras-chave;
- Deve permitir visualizar a quantidade de relatórios encontrados na busca;
- Deve possuir um mínimo de 2 mil relatórios na base de dados;
- Os relatórios devem estar disponíveis, no mínimo, nos seguintes idiomas: português, inglês e espanhol;
- Deve permitir filtrar a busca de relatórios, por no mínimo: Categorias; Período.
- Deve apresentar informações pertinentes de acordo com cada assunto, como IOCs, anexos e IPs que possam ser interessantes ao cliente;
- Deve permitir o download desse relatório no mínimo em formato PDF;
  Para relatórios com classificação confidencial, este deverá ser cifrado com senha individual, com objetivo de evitar compartilhamento acidental de informações sensíveis;
- O sistema deverá possuir mecanismo de captura automatizado de informações em diversas fontes da internet incluindo, no mínimo:
  - **Mídias sociais:**
    - Facebook, Facebook ADS, Twitter, LinkedIn, Instagram, TikTok, YouTube, Koo App, Mastodon, Pinterest, Volo, Twitch.
    - Aplicações de mensageria instantânea:WhatsApp, Telegram, IRC, Discord, Slack.
    - Motores de busca:Google, Yahoo, Bing, DuckDuckGo.
    - Sites de e-commerce: OLX, Mercado Livre.
    - Lojas de aplicativos oficiais e não oficiais: Aptoide, Google Play, APKPure.
    - Chans: 4Chan, Kohlchan, Leftypol, Vhs Chan, Vecchiochan, Mlpol.Net, Chan, Sportschan, 8Kunchan, Endchan, 27Chan, Tvchan, Lainchan, Wired-7, Leftychan, Niuchan, Erischan, Anonima Club, 75Chan, 8Chan, Intern3Ts, 1Chan.Us, 83channel.
    - Fóruns de discussão: Hack Forums, Patched, Club2Crd, Carder Uk, Bleeping Computer, Guia Do Hacker, Leak Base, Xss Is, Sinister, Leaks, Partner It, Sinful, Exploitin, Cryptbb, Verified Carder, Perfect Hackers, Blackbones, Shield, Leakforums, Ramp, Altenen, Forum 1877.
    - Repositórios de código: GitHub, Bitbucket, GitLab.
    - Indexadores de malware: Anyrun, Hybrid Analysis, Malware Bazaar, Ransomware, Virus Total.
    - Serviços de paste: Pastebin, Ghostbin.
    - Feed de domínios: CertStream, Open Phish, Phishtank, Whoxy, Zone Files IO, Fuzzydns, URL Scan, URL Haus.
    - Fontes sobre vulnerabilidades: CVE, Circl.lu, Open Bug Bounty, ExploitDB.
    - Serviços/dispositivos de rede: Binary Edge, Censys, Shodan, Zoom Eye, LeakIX.
    - Defacement: MirrorH, Zone-H.
    - Blogs de grupos de ransomware: Blackcat (Alphvm), Medusa, Clop, Lockbit, Black Basta, Blackbyte Auction, Play, Unsafe, Bianlian, Royal Landing, Dunghill Leak, Ragnar Locker, Trigona, Everest, Money Message, Karakurt, Snatch, Stormous, Lorenz, Ransomware Blog, Vice Society, Ransom House, Abyss, Crosslock, Cryptnet, Cuba, Dark Leak.
    - Outros: External Threats, Grayhatwarfare, ONION, RSS, The Pirate Bay.
    - Deve permitir o direcionamento das coletas realizadas pela plataforma por meio da configuração de robôs de coleta;
    - Quanto a configuração dos robôs, deverá ser realizado através da interface web, sem a necessidade de codificação, da seguinte forma:
      - Deve permitir a configuração de mais de um robô por fonte;

- Deve permitir a configuração do intervalo de execução e coleta de cada robô de forma individual;
- Deve permitir a configuração da visibilidade das informações coletadas por cada robô para times específicos da organização;
- Deve permitir a aplicação de filtros na coleta para direcionamento das informações que entram na plataforma;
- A ferramenta deve permitir a configuração de Google-Dorks para buscas direcionadas ao Google;

- Em relação ao monitoramento de grupos de Ransomware:
  - A solução deverá monitorar e possuir em sua base, pelo menos, 30 mil eventos de Ransomware;
  - Deve possuir um dashboard para apresentação de informações sobre eventos e grupos de ransomware, contendo: eventos com as postagens dos blogs monitorados; principais grupos com mais postagens nos blogs monitorados;
  - Gráfico com a quantidade de eventos publicados por dia; Relatórios relacionados aos ransomwares.
  - A ferramenta deve mapear principais grupos de Ransomware detectados;
  - Deve possuir mecanismo de múltiplo fator de autenticação (MFA);
  - Deverá possuir suporte à Single Sign-on: Azure; OKTA;
  - Permitir, no mínimo, configurar, habilitar e desabilitar múltiplos logins de usuários, complexidade de senhas, troca de senha no primeiro login, troca de senha periodicamente, ativação e desativação de usuários, definição de grupos e times;
  - Disponibilizar usuário(s) com perfil de administrador para acesso aos recursos da ferramenta, bem como acesso aos dados e alertas de outros usuários;
  - Permitir que dentro de uma mesma organização seja possível a criação de grupos distintos, onde seja possível indicar os times com acesso às informações deste grupo;
- Quanto ao permissionamento de usuários:
  - Deverá ser possível dar permissões e papéis diferenciados para os usuários configurados na plataforma;
  - Salve consultas para disponibilizar para outros usuários;
  - Crie, gerencie e exclua alertas;
  - Salve tabelas de dicionários para o uso em pesquisas;
  - Permitir a configuração de organização com no mínimo os seguintes atributos:Times de acesso; Palavras-chave; Ranges IP; Domínios; ASNs; Website; White-list; Palavras-chave; VIPs.
  - Deve possuir perfil de administrador e usuário normal dentro da organização;
  - Deve ser possível criar categorias de perfil com granularidade de acesso por funcionalidade da plataforma (RBAC).
  - Deve permitir configuração de alertas diretamente via interface de gerenciamento;
  - Deve ser possível, através da interface de gerenciamento, realizar testes de funcionamento dos alertas configurados;
  - Deve permitir a configuração de alertas via E-mail, Webhook, SMS, Ocorrências/Tickets e WhatsApp;
  - Deve permitir a configuração de alertas baseados em: consultas/pesquisas salvas; CPF vazado/exposto; citações de pessoas importantes (VIP); Credenciais de domínios cadastrados.

- Deve permitir consultar credenciais de usuários expostas em internet:
  - Credenciais expostas em bases externas;
  - Credenciais expostas por Malware;
  - Credenciais detectadas nos eventos da plataforma.
  - Deve possuir um dashboard com informações gerais sobre as credenciais da organização que foram vazadas;
  - Deve possuir uma tela de pesquisa onde seja possível efetuar a busca por credenciais baseados em domínios, subdomínios, e-mails específicos e urls de acesso.
  - Deverá possuir, no mínimo, 7 bilhões de credenciais expostas na base de dados.
  - Deve permitir filtrar os resultados da busca por data de recebimento da credencial vazada e por tipo de vazamento.
- Disponibilizar através de interface web, a busca de credenciais utilizando mecanismos como:
  - Proximidade; Fuzzy (difusa); Lógica binária; Expressões regulares (regex); Operadores lógicos (“AND, “OR” e “NOT”); Caracteres wildcard;
- Deve possuir um dashboard com informações gerais sobre vulnerabilidades:
  - Deve possuir informações gráficas sobre as principais CVEs identificadas;
  - Deve apresentar relatórios relacionados à vulnerabilidades;
  - Deve apresentar os últimos eventos detectados pela plataforma em relação às vulnerabilidades;
- Deve possuir interface que permita a pesquisa por vulnerabilidades por, no mínimo:
  - Busca textual;
  - Severidade;
  - Data;

1.3.3.1.3.1 TAKEDOWN / SERVIÇO DE REMOÇÃO DE CONTEÚDO MALICIOSO.

Deve possuir uma tela para solicitação de takedowns, com no mínimo as seguintes opções:

- URL para takedown; Empresa; Prioridade; Categoria.
- Deve ser possível adicionar um feedback às ocorrências fechadas, colocando o nível de relevância;
- Deve possuir uma tela para visualização dos takedowns solicitados;
- No painel de gerenciamento, deve ser possível visualizar a quantidade total de takedowns e ordenar por data e prioridade;
- Possuir filtros para a busca de takedowns solicitados com no mínimo as seguintes opções de filtro:
  - Empresa;
  - Status;
  - Categoria;
  - Período;
  - Responsável pela criação;
  - Número da ocorrência;
  - Responsável pelo takedown.
- Quanto ao takedown, a plataforma deve disponibilizar dashboard com pelo menos:
  - Quantidade de takedowns solicitados no período;
  - Status dos takedowns solicitados;
  - Tempo médio de mudança de status do takedown;
  - Lista de takedowns solicitados;
  - Aba de pesquisa de takedowns com filtro por ao menos:

        - Status;
        - Categoria;
        - Período.
    - A plataforma deverá possuir recurso de takedown automatizado onde o processo de remoção do conteúdo malicioso dispensará ação humana para, pelo menos: Perfis de redes sociais, como:
        - Instagram;
        - Facebook;
        - TikTok;
    - Páginas que utilizam serviço de hospedagem, como: Hostigator;
    - Páginas de compartilhamento de documentos, como: Scribd.

1.3.3.1.4 SERVIÇOS DE TESTES DE INVASÃO (RED TEAM)

A CONTRATADA deverá realizar Serviços de Testes de Invasão (Red Team) com o objetivo de identificar, explorar e evidenciar vulnerabilidades técnicas, falhas de configuração, fragilidades em processos e comportamento humano que possam colocar em risco a segurança das informações, sistemas, infraestrutura e serviços da CONTRATANTE.
Os serviços de Pentest poderão ser executados na modalidade híbrida.

A CONTRATADA deverá identificar e explorar vulnerabilidades, simulando ataques reais que serão realizados por profissionais identificados, certificados e capacitados, devendo incluir a elaboração e apresentação de relatórios detalhados contendo os métodos, técnicas e ferramentas utilizadas, bem como avaliação, diagnóstico e recomendações de correção das vulnerabilidades porventura encontradas.

Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem do ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável da CONTRATANTE.

Os testes serão realizados em conjunto com a CONTRATANTE qual será o alvo e o tipo do PENTEST a ser executado, respeitando as definições previamente acordadas.

Caso a CONTRATANTE entenda haver algum risco na execução do Pentest que possa comprometer, em qualquer grau, o funcionamento de sistema, ativo ou processo da CONTRATANTE, poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do horário comercial.

Os testes deverão ser realizados de forma controlada, planejada e autorizada, simulando táticas, técnicas e procedimentos (TTPs) similares aos utilizados por agentes maliciosos reais, respeitando as boas práticas de mercado, normas e metodologias reconhecidas internacionalmente, tais como: MITRE ATT&CK; OWASP (ASVS, Top 10, API Security, etc.); NIST SP 800-115; PTES (Penetration Testing Execution Standard);

Os testes poderão ser dos seguintes tipos: Black Box, onde não há informação prévia; White Box, com acesso total a detalhes internos; e Gray Box, com acesso parcial.

Os testes podem ser focados em componentes específicos, como serviços de rede, aplicações web, redes sem fio e engenharias sociais.

Os retestes deverão ser realizados após correções, efetuadas pelo CONTRATANTE, das vulnerabilidades e com aprovação do CONTRATANTE.

Red Team Engagement Framework.
Escopo dos Serviços:

- Planejamento do exercício Red Team junto à CONTRATANTE, com definição de regras de engajamento (Rules of Engagement – RoE), escopo, horários e limitações.
- Testes de invasão em infraestrutura interna e externa;
- Testes em aplicações web, APIs e dispositivos;
- Engenharia social (simulações de phishing, vishing ou pretextos autorizados);
- Movimentação lateral dentro do ambiente;
- Evasão de controles e simulação de persistência.
- Mapeamento e exploração de vulnerabilidades, com coleta de evidências
- Identificação e validação dos vetores de ataque utilizados.
- Avaliação dos controles de segurança existentes, capacidade de detecção e resposta da equipe defensiva (Blue Team) da CONTRATANTE.
- Relatório técnico detalhado contendo:
    - Descrição de todas as vulnerabilidades exploradas;
    - Evidências coletadas;
    - Riscos associados;
    - Vetores de ataque utilizados;
    - Recomendações de correção.

FASES PRESTAÇÃO DO SERVIÇO

Cada teste de intrusão, necessariamente, deverá seguir as seguintes fases, nesta ordem:

Planejamento - quando serão apresentados e discutidos os itens constantes na OS. Na fase de planejamento serão definidos:

- Objetivo a ser alcançado.
- Processos e atividades permitidas ou proibidas.
- As informações e acessos necessários para a realização do Pentest (especialmente nos casos de Pentests Graybox e Whitebox).
- **Descoberta** - A CONTRATANTE, inicia-se a fase de Descoberta, que tem como objetivo a obtenção de informações relevantes dentro do escopo do teste que possibilitam reconhecer possíveis ameaças/vulnerabilidades. Importante frisar que esta fase não deve se restringir à utilização de ferramentas automatizadas, sendo esperada atuação manual da equipe técnica contratada, aprofundando a análise da superfície de ataque à procura de vulnerabilidades não facilmente identificáveis. Deverão ser realizadas, no mínimo, as seguintes atividades:
    - Coleta passiva, caracterizada pela obtenção de informações utilizando-se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis:
        - **Exploração** - nesta fase, o objetivo é confirmar as vulnerabilidades e identificar os impactos e riscos das ameaças porventura encontradas a partir de simulações de ataques reais. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas na CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável da CONTRATANTE. Além disso, deve-se atender os seguintes itens:
        - A empresa CONTRATADA deverá ser capaz de aplicar, no mínimo, os seguintes tipos de ataques, quando aplicáveis:
        - Ataques baseados em aplicação web:
            - Violações do protocolo HTTP, SQL Injection, LDAP Injection, Cookie Tampering, Cross-Site Scripting (XSS), Directory Traversal, Buffer Overflow, OS Command Execution, Command Injection, Remote Code Inclusion, Server Side Includes (SSI) Injection e File Disclosure.

- Ataques baseados em rede e protocolos:
  - Ataques contra o protocolo TCP, incluindo sequestro de conexões, bem como problemas relacionados ao protocolo SNMP.
  - Ataques avançados a aplicações modernas: Cross-Site Request Forgery (CSRF), Server Side Request Forgery (SSRF) e Insecure Direct Object References (IDOR).
  - Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os testes baseados na publicação OWASP TESTING GUIDE (The Open WebApplication Security Project) em sua versão mais recente.
- Relatório - Após a fase de Exploração, deve ser elaborado pela CONTRATADA um relatório do teste de intrusão. Este relatório deve conter ao menos:
  - Escopo, tipo e modalidade do teste; Metodologias, técnicas, fontes de pesquisa e referências Atividades realizadas, em ordem cronológica; Informações acessadas e detalhes da infraestrutura descoberta (caso aplicável); Confirmação ou refutação da existência das vulnerabilidades.
  - Descrição de todas as vulnerabilidades e ameaças porventura encontradas, informando, no mínimo:
  - nome da vulnerabilidade; nível de risco ou criticidade; indicação se a exploração foi intrusiva (sim ou não); descrição detalhada; documentação do fabricante sobre a vulnerabilidade, se disponível; melhores práticas recomendadas para correção ou mitigação; link para o patch ou correção, se houver; número CVE correspondente, quando aplicável; total de vulnerabilidades detectadas; evidências da exploração das vulnerabilidades eventualmente encontradas; avaliação de riscos e impactos associados à exploração da falha; contramedidas propostas para mitigação ou correção dos riscos; e assinatura do profissional responsável, devidamente certificado.
  - As ferramentas utilizadas nos testes de intrusão são de responsabilidade da CONTRATADA, não devendo ser instaladas no ambiente tecnológico da CONTRATANTE.
  - Os testes de invasão deverão envolver, necessariamente, o uso de técnicas e ferramentas específicas mais atualizadas e comumente utilizadas no mercado de segurança da informação, para tentar obter acesso não autorizado e privilegiado aos ativos e informações, simulando um ataque real.
  - Para a análise de vulnerabilidades, executada durante a fase de descoberta, a CONTRATADA deverá utilizar ferramenta que atenda, no mínimo, as seguintes características:
  - Realize escaneamento utilizando base de dados atualizada com as mais recentes ameaças e vulnerabilidades;
  - Faça avaliação de riscos com apresentação de score utilizando metodologia CVSS (Common Vulnerability Scoring System) – quando aplicável;
  - Apresente formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;
  - Deverá utilizar identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas, quando aplicável.
  - Suportar o armazenamento seguro de credenciais, para uso em varreduras autenticadas, usando as credenciais para se autenticar em sistemas Windows, Linux ou qualquer ativo de infraestrutura, tais como dispositivos de rede, etc, em caso de pentest interno.
  - O processo de varredura deve ter um impacto mínimo sobre a rede.

- Ferramentas de análise de vulnerabilidades e enumeração de sistemas web, deverão possuir minimamente as seguintes características:
  - Ser capaz de detectar, no mínimo, as vulnerabilidades elencadas no guia OWASP TOP 10 em sua versão mais atualizada;
  - Ser capaz de realizar escaneamento ativo ou passivo;
  - Ser capaz de realizar crawling/spidering para descobertas de urls, hiperlinks, páginas, dentre outros.
  - A utilização de ferramentas não deve integrar a atuação do analista quando da realização do Pentest, sendo apenas auxiliar no processo de identificação, análise e posterior exploração de vulnerabilidades.
  - Utilizar profissionais qualificados e certificados em segurança ofensiva, respeitando as boas práticas de segurança.
  - Manter sigilo e confidencialidade sobre todas as informações obtidas durante o teste.
  - Emitir os relatórios em português, de forma clara e objetiva.

1.3.3.1.5 PLATAFORMA DE GESTÃO DE VULNERABILIDADES

A solução deve permitir a descoberta, avaliação, priorização e correção de vulnerabilidades e configurações em toda a infraestrutura da rede, abrangendo estações de trabalho, servidores, dispositivos de rede, telecomunicações, segurança, hipervisores, máquinas virtuais, contêineres e ambientes em nuvem (Azure, GCP, AWS).

A gestão centralizada deverá ser acessível por uma interface web única, sem a necessidade de consoles ou componentes adicionais.

A solução deverá ser licenciada por IP ou HOST, com descoberta e inventário ilimitados, incluindo acesso a agentes, scanners, sensores para contêineres e sensores de descoberta passiva, sem custos adicionais.

A solução deverá fornecer descoberta e inventário contínuos de todos os ativos de TI, incluindo ativos conhecidos e desconhecidos/não gerenciados, em diversos ambientes (on-premises, multi-cloud, contêineres, endpoints remotos, mobile, IoT/OT).

A solução deverá permitir a coleta automatizada e detalhada de informações dos ativos gerenciados, contemplando dados como os serviços em execução, softwares instalados, usuários locais e de domínio, portas abertas, versão do sistema operacional, nome do host (hostname), nome de domínio totalmente qualificado (FQDN), endereços IP nas versões IPv4 e IPv6, endereço MAC, informações do processador, memória instalada, volumes de disco e dados da BIOS. Essas informações deverão estar disponíveis de forma centralizada e estruturada, possibilitando análise, auditoria e correlação com eventos de segurança.

A solução deverá permitir automaticamente classificar os ativos por famílias tecnológicas, tipo de dispositivo, tipo de plataforma e fabricante.

Deverá normalizar automaticamente os nomes dos fabricantes de hardware e software com dados relevantes como nome das aplicações e versões.

A solução deverá permitir etiquetagem de ativos com base em parâmetros como: estática/manual, palavras-chave, endereço IP e intervalos de IPs, segmento de rede, portas abertas, ID de vulnerabilidade específica, Groovy Scriptlet ou Regex.

A solução deverá fornecer avaliação contínua de vulnerabilidades utilizando múltiplos tipos de sensores integrados (agentes, scanners de rede, sensores passivos).

O motor de escaneamento deverá ter taxa de precisão de 99,99966% (nível Six Sigma) para detecção de vulnerabilidades, com base nos últimos 10 anos.

A base de conhecimento deverá ser atualizada semanalmente, incorporando no mínimo 20 CVEs por semana e contendo ao menos 35.000 CVEs históricos e atuais, incluindo tecnologias legadas.

A solução deverá cobrir os seguintes tipos de sistemas e plataformas, como requisito mínimo: sistemas operacionais Microsoft Windows, UNIX, LINUX, MacOS, Cisco, VMware; bancos de dados Microsoft SQL Server, MySQL, Oracle, Sybase; plataformas web como IIS e Apache Tomcat; e serviços e aplicações como TCP, UDP, Adobe, Apple, HP, McAfee, Microsoft (Office, IIS, Exchange), Oracle, Oracle Java e VMware.

A solução deverá permitir escaneamentos de vulnerabilidades baseados em sistemas operacionais, serviços web, portas TCP e UDP, serviços, aplicações e bancos de dados.

Deverá permitir as seguintes alternativas de escaneamento de vulnerabilidades na rede: escaneamento ativo da rede não autenticado, escaneamento ativo da rede autenticado e agente.

A solução deverá incorporar um motor de cálculo de risco multifatorial para ativos e vulnerabilidades.

O cálculo de risco deverá considerar, no mínimo: vulnerabilidades associadas ao ativo, criticidade do ativo, localização, ameaças conhecidas (incluindo CISA Known Exploitable), problemas de configuração, controles compensatórios, certificados associados e obsolescência do software.

A pontuação deverá usar critérios como CVSS, ECM (Exploit Code Maturity), tendência de exploração e atores de ameaça.

O cálculo de risco deverá ser dinâmico, adaptando-se automaticamente às variações nas variáveis e ameaças ao longo do tempo.

Deverá permitir priorizar ações de remediação com base nesse cálculo.

A solução deverá detectar com precisão os patches ausentes nos ativos avaliados e deverá mapear automaticamente patches a CVEs relacionados.

A solução deverá avaliar configurações com base nos benchmarks do Center for Internet Security (CIS), para sistemas operacionais, software de servidores, provedores de nuvem, dispositivos de rede e software de desktop.

O fabricante deverá possuir certificação oficial do CIS para fornecimento desse tipo de controle.

Deverá identificar configurações incorretas que aumentem o risco de segurança.

A solução deverá avaliar certificados digitais (internos e externos) e configurações TLS, identificando emissor, data de expiração, tipo de certificado, robustez do algoritmo e suíte de criptografia.

Deverá permitir renovação de certificados expirados diretamente via interface da ferramenta.

Deverá permitir criação de fluxos de trabalho automatizados, via interface gráfica “drag and drop”, para ações de avaliação e remediação, sem necessidade de código.

Deverá descobrir e inventariar automaticamente aplicações web e APIs, internas e externas, conhecidas e shadow, em ambientes on-prem, nuvem, contêineres, gateways de API.

Deverá integrar com o inventário de ativos unificado.

Deverá realizar crawling automatizado e testes dinâmicos, identificando vulnerabilidades em tempo de execução, incluindo OWASP Top 10 (ex: SQLi, XSS, SSRF).

Deverá suportar varredura autenticada em aplicações com login.

Deverá utilizar técnicas de IA/ML para melhoria da detecção.

Deverá incluir capacidades dedicadas para segurança de API, testando contra o OWASP API Top 10 e validando conformidade com OpenAPI (OAS v3).

Deverá detectar exposição de PII e dados sensíveis em aplicações web e APIs.

Deverá incorporar técnicas avançadas para detectar malware em aplicações web, incluindo ameaças de dia zero.

A solução deverá gerar a avaliação das vulnerabilidades, estabelecendo o nível real de criticidade com base na análise de informações relacionadas à vulnerabilidade. A solução deverá gerar sua própria pontuação de criticidade utilizando critérios como: pontuação CVSS, CISA Known Exploitable, maturidade do código de exploração (ECM), tendência de exploração e atores de ameaça.

A solução deve proporcionar um fluxo de trabalho de remediação baseado em políticas, permitindo a criação, atribuição e reatribuição de tickets conforme condições definidas pelo administrador da solução, seja por meio de políticas automatizadas ou manualmente.

A solução deve permitir a criação de tickets com os estados "aberto", "fechado" ou "ignorado", com base nos seguintes critérios: host(s) a que se aplica a regra, vulnerabilidade(s) associada(s), usuário atribuído, data de criação ou expiração, e mudança de estado do ticket.

A solução deve permitir a criação automática de tickets de remediação com base nos resultados de varreduras de vulnerabilidades, informações específicas de um host ou manualmente por um administrador.

A solução proposta deve permitir a implantação de patches utilizando o mesmo agente responsável pelos escaneamentos de segurança, sem necessidade de agentes de terceiros ou de conectividade via VPN.

A solução deve permitir a gestão de patches para sistemas operacionais Microsoft Windows, Linux e Mac, além de fornecer cobertura para aplicações de uso corporativo frequente, conforme lista de plataformas suportadas para patching.

A solução deve permitir notificações ao usuário final durante o processo de implantação do patch, possibilitando o adiamento da tarefa ou apresentando uma contagem regressiva para a execução.

A solução deve ser capaz de reiniciar automaticamente o host, nos casos em que o patch requer reinicialização para aplicação efetiva.

A solução deve enviar notificações ao usuário sobre a ação de reinício, permitindo ao usuário rejeitar a ação por um número X de vezes, forçar o reinício ou apresentar contagem regressiva para execução.

A solução deve detectar automaticamente se o host está conectado à rede local e, neste caso, realizar o download de patches a partir de um repositório local. Caso contrário, os patches devem ser baixados diretamente da internet.

A solução deve possibilitar a criação de jobs para implementação de patches por meio de módulo integrado à mesma plataforma utilizada na gestão de vulnerabilidades.

O módulo de patch deve possuir a capacidade de configurar ações prévias ou posteriores aos jobs, incluindo reinicialização do sistema, desinstalação de software, instalação de software, execução de scripts e modificações no registro do sistema.

O módulo de patching deve permitir a seleção de um ou múltiplos patches para aplicação em um ou vários ativos, sem que isso implique em custos adicionais de licenciamento do módulo.

O módulo de patching deve suportar a execução de jobs em sistemas operacionais Windows, Linux e Mac.

A solução deve permitir a limitação da janela de tempo em que as tarefas de patching poderão ser executadas.

O módulo de patching deve incluir múltiplos dashboards com visão consolidada sobre o estado dos patches, incluindo, mas não se limitando a: patches não instalados, patches com falha na instalação, ativos que requerem reinicialização e estado geral dos patches aplicados.

1.3.3.1.6. Requisitos de Arquitetura Tecnológica (Configuração):

Para a execução das atividades presenciais previstas neste Termo de Referência, a CONTRATANTE se compromete a disponibilizar ambiente físico adequado nas suas dependências, incluindo os recursos necessários à plena realização dos serviços.

Espaço físico adequado para a acomodação dos profissionais designados pela CONTRATADA;

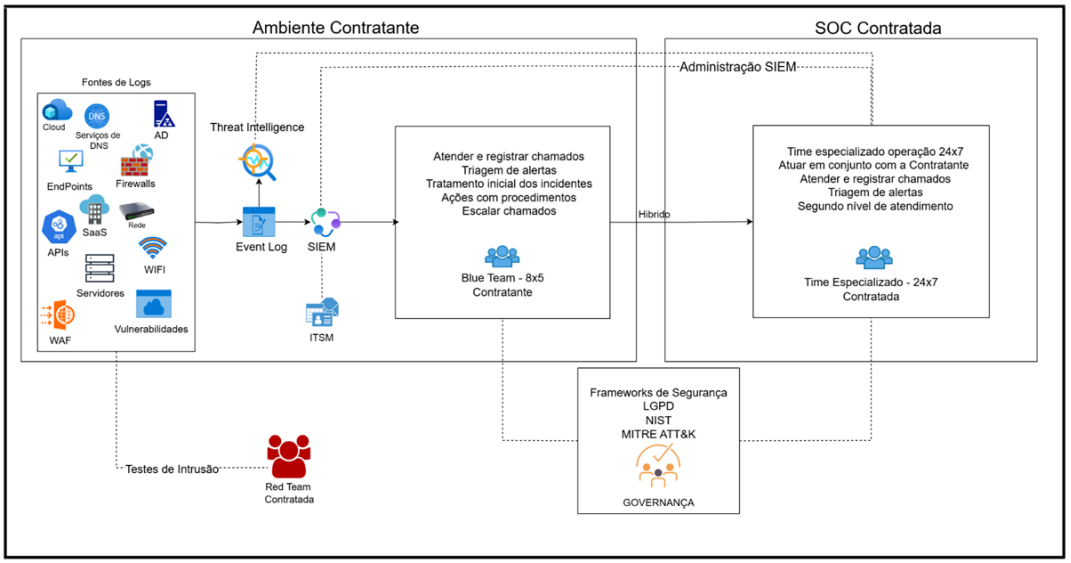
Mobiliário básico como mesas, cadeiras e armários, conforme a necessidade das atividades;

Equipamentos de informática, tais como computadores, monitores, VideWall e periféricos necessários;

Acesso à rede local e à internet, condicionado às políticas internas de segurança da informação;

Credenciais de acesso aos sistemas e ferramentas da CONTRATANTE, conforme perfil e função dos profissionais alocados.

O uso da infraestrutura disponibilizada deverá respeitar as normas internas da CONTRATANTE, especialmente no que se refere à política de uso de ativos, confidencialidade e segurança da informação.



1.3.3.2. Requisitos de Capacitação:

A equipe técnica do PJAC deverá ser capacitada minimamente para operar as ferramentas utilizadas na prestação dos

serviços, de modo a possibilitar a correta interpretação dos alertas, extração de informações relevantes, geração de relatórios e acompanhamento das atividades executadas pela contratada.

A capacitação deverá contemplar, no mínimo, treinamentos de overview sobre o funcionamento do SOC, operação do SIEM, uso da plataforma de Gestão de Vulnerabilidades, consulta a indicadores de Threat Intelligence e interpretação de relatórios técnicos e gerenciais.

A contratada deverá garantir que o processo de capacitação seja contínuo, com atualização periódica em caso de evolução tecnológica ou atualização das ferramentas, bem como disponibilizar materiais de apoio (manuais, tutoriais e guias rápidos) em português.

1.3.3.3. Requisitos de Manutenção:

Elaboração de relatório mensal consolidado com todos os tickets abertos no mês e informações importantes sobre a CONTRATANTE.
A contratada deverá garantir a continuidade dos serviços durante toda a vigência contratual, assegurando operação estável, segura e ininterrupta, inclusive em regime 24x7 quando aplicável.

Deverão ser realizadas atualizações preventivas e corretivas periódicas, tanto em processos, conteúdos e metodologias, quanto em ferramentas tecnológicas associadas, sempre em conformidade com as boas práticas de mercado e normativos aplicáveis.

A contratada será responsável pela substituição imediata de profissionais em caso de desligamento, afastamento ou não conformidade, mantendo o nível de serviço e as qualificações mínimas exigidas.

Relatórios de manutenção e evolução dos serviços deverão ser apresentados trimestralmente, contemplando ajustes realizados, falhas identificadas, medidas preventivas adotadas e propostas de melhoria contínua.

Ambiente a ser analisado e gerenciados:

Ativos	Quantidade
IPs externos	64
Aplicações WEB	200
Domínios	1
Servidores	500
EndPoint	2000
Dispositivos de rede	700
Usuários	2000

1.3.3.3. Requisitos de Manutenção:

1.3.3.3.1 GESTÃO E CONTROLE DE SERVIÇOS

A execução dos serviços deverá ser gerenciada pela Contratada por meio da atuação de uma equipe de Sucesso do cliente, que será responsável por atuar como canal de comunicação entre as partes, além de realizar o acompanhamento contínuo da qualidade dos serviços prestados e dos níveis de serviço acordados.

Essa equipe deverá atuar de forma proativa na identificação de oportunidades de melhoria, ajustes e correções de eventuais desvios, garantindo a aderência dos serviços às necessidades do Cliente e contribuindo para o alcance dos resultados esperados.

Como parte das atividades, deverão ser contempladas, no mínimo, as seguintes responsabilidades:

- Suporte e acompanhamento periódico do contrato referente a todos entregáveis previstos no contrato;
- Acompanhar indicadores da operação;
- Reunião mensal de resultados;
- Análise e acompanhamento referente aos prazos e incidentes;
- Geração de relatório de KPIs;
- Geração de relatório mensal sumarizado com status, ocorrências e ações sugeridas e/ou realizadas;
- Acompanhar os serviços nas revisões dos SLAs.

1.3.3.3.2 ACORDO DE NÍVEL DE SERVIÇOS – SLA PARA SOC E BLUE TEAM/SIEM/THREAT INTELLIGENCE/GESTÃO DE VULNERABILIDADE

A contratada deverá disponibilizar um número único local do tipo 0800, para a execução dos serviços, que demandam contatos telefônicos. O nível de serviço poderá ser definido em função de, no mínimo (SLA): Deverá ser garantido, no mínimo, os seguintes tempos para início de atendimento e tratativas para alertas de criticidade detectada no ambiente:

Indicador	Descrição	Início Previsto	Disponibilidade
TMA Crítica	Tempo Médio de Atendimento (Incidentes que contemplem ambiente parado e/ou indisponibilidade total da solução)	Até 60 minutos após registro do chamado	24x7x365
TMA Alta	Tempo Médio de Atendimento (Incidentes que afetem usuários e aplicações críticas, sem ambiente parado)	Até 2 horas após registro do chamado	24x7x365
TMA Média	Tempo Médio de Atendimento (Incidentes de performance, lentidão ou que afetem usuários e aplicações, permitindo medida de contorno)	Até 8 horas após registro do chamado	24x7x365

TMA Baixa	Tempo Médio de Atendimento (Incidentes de erros e alertas que afetem usuário ou aplicações não críticas; Inclusão e Remoção de Ativo monitorado Dúvidas, orientações e informações sobre qualquer item relacionado a solução)	Até 8 horas comerciais após registro do chamado	10x5 Horário Comercial 08:00hrs às 18:00hrs
SLA	Acordo de Nível de Serviço (Percentual esperado por indicador)	90%	Mensal

Deverá ser garantido, no mínimo, os seguintes tempos para início de atendimento e tratativas para alertas de criticidade detectada no ambiente:

CRITICIDADE	NÍVEIS DE EVENTO	REGIME DE ATENDIMENTO	INÍCIO DE ATENDIMENTO
1 - Crítica	=>12	24 x 7	Em até 30min
2 - Alta	10-11	24 x 7	Em até 1 hora
3 - Média	06-09	24 x 7	Em até 4 horas
4 - Baixa	=<05	24 x 7	Em até 8 horas

1.3.3.3.3. FERRAMENTAS PARA A PRESTAÇÃO DO SERVIÇO

A contratada deverá disponibilizar e/ou operar ferramentas tecnológicas adequadas e compatíveis com o escopo dos serviços contratados, sem custos extras para o CONTRATANTE, observando os seguintes requisitos mínimos:

- **SIEM (Security Information and Event Management):** utilização obrigatória da solução Wazuh já implantada no PJAC, devendo a contratada realizar sua administração, evolução arquitetural, implementação de regras de correlação, geração de dashboards, relatórios automatizados e integração com demais fontes de logs da instituição.
- **Threat Intelligence (Inteligência de Ameaças):** utilização de plataformas e serviços que permitam coleta, análise e correlação de informações provenientes de fontes abertas (OSINT), deep web, dark web, redes sociais, fóruns e grupos de ameaça, incluindo capacidade de takedown de domínios e conteúdos maliciosos.
  Gestão de Vulnerabilidades: adoção de solução integrada de avaliação contínua de vulnerabilidades, gestão de patches e conformidade de configurações, compatível com sistemas operacionais, bancos de dados, aplicações web, APIs e dispositivos de rede.
- **Ferramentas de Red Team:** utilização de ferramentas reconhecidas no mercado para execução de testes de intrusão controlados, simulando ataques a redes, aplicações e infraestrutura, em conformidade com frameworks como MITRE ATT&CK, OWASP e NIST.
- **Plataforma de Conscientização em Segurança da Informação:** disponibilização de ambiente tecnológico que permita a execução de campanhas de treinamento, simulações de phishing, aplicação de quizzes, geração de relatórios de risco humano e acompanhamento de indicadores de engajamento.

- **Integração e Relatórios:** todas as ferramentas utilizadas deverão ser integradas entre si sempre que possível, fornecendo relatórios gerenciais e técnicos centralizados, com indicadores de desempenho (KPIs), métricas de segurança e evidências para auditoria.

1.3.3.4. Requisitos de Implantação:

A empresa contratada deverá apresentar, no prazo máximo de 10 (quinze) dias úteis após a assinatura do contrato e da emissão da primeira Ordem de Serviço, um Plano de Implantação detalhado, contemplando cronograma, atividades, entregas, marcos de acompanhamento, responsáveis e dependências técnicas.

A Contratada deverá iniciar a plena operação dos serviços de SOC (monitoramento 24x7, detecção e resposta a incidentes) em um prazo máximo de 15 (quinze) dias úteis a partir da assinatura do instrumento contratual e da emissão da primeira Ordem de Serviço, mediante comprovação de todas as integrações e configurações necessárias.

A contratada deverá designar um colaborador como ponto focal, responsável pela coordenação das atividades de implantação, pela comunicação oficial com o PJAC e pela entrega dos relatórios de progresso.

Deverá ser realizada uma reunião inicial de kick-off entre a equipe técnica do PJAC e a equipe da contratada, a fim de alinhar expectativas, escopo, metodologia de trabalho, canais de comunicação e indicadores de desempenho, após a assinatura do contrato.

Durante a implantação, a contratada deverá mitigar impactos operacionais, adotando práticas de boas condutas de mudança, de forma a não comprometer a continuidade dos serviços do PJAC.

Todo o processo de implantação deverá ser acompanhado de relatórios de progresso, contendo as atividades concluídas, pendências, riscos identificados e planos de ação.

A solução e os serviços deverão ser implantados em conformidade com a Política de Segurança da Informação do PJAC, com as normas do CNJ e com a legislação vigente aplicável.

1.3.3.5. Requisitos de Experiência e Formação da Equipe

Os recursos humanos disponibilizados pela Contratada deverão conhecer o funcionamento das ferramentas utilizadas pela CONTRATANTE. O quantitativo proposto para pleno atendimento da demanda da CONTRATANTE deve ser dimensionado pela CONTRATADA.

Critérios para definição dos perfis necessários para a operação dos serviços:

1.3.3.5.1 Perfil de monitoramento, detecção e resposta a incidentes de segurança da informação – Blue Team: Grupo 1

Manter equipe experiente na área de monitoramento e resposta a incidentes, capazes de utilizarem técnicas avançadas de detecção, conciliando com as práticas mais adequadas considerando o ambiente e utilizando a ferramenta de SIEM da CONTRATANTE

1.3.3.5.2 Perfil de Analista de segurança da Informação – Sênior - SIEM: Grupo 1

Profissional com experiência em Segurança da Informação, responsável pela operação, administração e sustentação da solução Wazuh — plataforma de SIEM e monitoramento de segurança utilizada pelo CONTRATANTE. Este perfil deve possuir conhecimentos em ferramentas de monitoramento de segurança, análise de logs, correlação de eventos e operação de soluções SIEM. Além das atividades técnicas, espera-se capacidade de análise crítica, visão proativa na identificação de riscos e habilidade em gerar recomendações de melhorias para o ambiente monitorado.

1.3.3.5.2.1. Certificações exigidas: Enterprise Certified Admin.

1.3.3.5.3 Perfil de Gestão de Segurança da Informação - Gestor - Blue Team: Grupo 1
Profissional responsável pela coordenação estratégica das atividades de Segurança da Informação, atuando na definição de políticas, processos, controles e indicadores de desempenho, além de apoiar a alta gestão na tomada de decisões relacionadas à Segurança da informação.

1.3.3.5.3.1. Certificações exigidas desde profissional: ISO/IEC 27001, CISM (Certified Information Security Manager) e CISSP (Certified Information Systems Security Professional).

1.3.3.5.4. Perfil de Gestor e Controlador dos serviços - Blue Team: Grupo 1
A gestão e o controle dos serviços deverão ser conduzidos por profissionais devidamente qualificados, com formação acadêmica de nível superior, preferencialmente nas áreas de Gestão da Qualidade. Além da formação, esses profissionais deverão possuir, no mínimo, 1 (um) ano de experiência profissional.

1.3.3.5.5. Perfil do Analista de Segurança da Informação – Sênior Perfil de Red Team: Item 7
Para este perfil, espera-se que o profissional detenha técnicas de intrusão à sistemas e redes, para poder auxiliar na descoberta de vulnerabilidades que não são, necessariamente, elencadas pelas ferramentas de análise de vulnerabilidades. É essencial que o profissional tenha certificações e experiência na área, para que o risco de qualquer indisponibilidade de serviço ou até mesmo o risco de vazamento de informações por consequência de um teste de penetração sejam mitigados pela experiência do profissional.

1.3.3.5.5.1. Certificações exigidas: Certified Ethical Hacker, CompTIA PenTest+ e Certified in Cybersecurity (CC).

1.3.3.6. Requisitos Temporais:

Esta seção estabelece os parâmetros temporais mandatórios para a contratação, execução e gestão dos serviços especializados de segurança cibernética, englobando desde o prazo de vigência contratual até os marcos de entrega e os tempos de resposta exigidos. A definição precisa desses requisitos é crucial para a previsibilidade da gestão contratual e para a garantia da tempestividade das ações de segurança.

Vigência Contratual e Prazos de Execução:

- **Prazo Inicial:** O prazo de vigência inicial do contrato será de 12 (doze) meses, a contar da data de sua assinatura, conforme preconizado no Documento de Oficialização da Demanda (DOD) nº 15/2025.
- **Prorrogação:** Em conformidade com o disposto no Art. 107 da Lei nº 14.133/2021, o contrato poderá ser prorrogado sucessivamente, mediante apostilamento, observados os limites legais e a justificativa da Administração, por períodos sucessivos até o limite total de 60 (sessenta) meses.

Marcos de Implementação e Entregas Periódicas:

- **Fase de Implementação (Onboarding):** A Contratada deverá apresentar um plano detalhado de implementação (onboarding), contendo cronograma de atividades, responsáveis e prazos para a integração dos sistemas, configuração do SIEM (Wazuh), ativação das fontes de logs, e calibração das regras detecção.

Relatórios e Apresentações:

- **Relatórios Técnicos Detalhados:** A Contratada deverá entregar relatórios técnicos detalhados para cada atividade específica (e.g., conclusões de pentests, resultados de campanhas de conscientização) em até 10 (dez) dias úteis após a conclusão da respectiva atividade.
- **Relatórios Gerenciais Mensais:** Deverá ser entregue um relatório gerencial consolidado, contendo indicadores de desempenho (KPIs), status das atividades, ocorrências e ações realizadas, até o 5º (quinto) dia útil do mês subsequente ao mês de referência.

- **Reuniões Periódicas:** Reuniões de acompanhamento dos serviços com o Fiscal do Contrato deverão ocorrer com frequência mínima mensal, ou sempre que solicitado pelo Contratante, para análise dos relatórios e discussão de melhorias contínuas.

Acordos de Nível de Serviço (SLAs) Temporais:

- Os tempos máximos de resposta e resolução para incidentes de segurança serão regidos pelos Acordos de Nível de Serviço (SLAs) detalhados no subtópico 1.3.3.3.2 deste ETP, os quais deverão ser rigorosamente cumpridos pela Contratada.
- A medição do desempenho em relação a esses SLAs será realizada de forma contínua, com a apuração dos resultados apresentada nos relatórios gerenciais e acompanhada nas reuniões de gestão contratual.

Prazos para Afastamento de Recursos:

- A Contratada deverá promover o afastamento de qualquer recurso técnico que não corresponda aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do PJAC no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação formal.

A inobservância dos prazos e requisitos temporais estabelecidos neste ETP e no Termo de Referência poderá acarretar as sanções contratuais previstas, reforçando a importância do planejamento e da execução diligentemente cronometrados por parte da Contratada.

1.3.3.7. Requisitos de Segurança da Informação:

Considerando a natureza sensível das atividades envolvidas na operação de um Centro de Operações de Segurança (SOC), será exigido da empresa contratada o comprometimento formal com a confidencialidade, a integridade e a proteção dos dados e informações institucionais do Poder Judiciário do Estado do Acre (PJAC).

A prestação dos serviços deverá observar rigorosamente os princípios da confidencialidade, integridade e disponibilidade, conforme preconizado pela Política de Segurança da Informação (PSI) do PJAC e demais normas aplicáveis.

Qualquer incidente relacionado à quebra de sigilo, acesso indevido, vazamento de informação ou uso não autorizado deverá ser comunicado imediatamente ao PJAC, sob pena de responsabilização administrativa, cível e penal.

A Prestadora de Serviços deverá assinar um Termo de Sigilo e Confidencialidade, comprometendo-se a não divulgar, utilizar, compartilhar, promover ou permitir o acesso indevido a quaisquer dados, informações, registros, configurações, documentos ou elementos do ambiente computacional do PJAC, salvo mediante autorização expressa e formal da administração.

Todos os profissionais diretamente envolvidos na execução dos serviços, especialmente aqueles designados nas respectivas Ordens de Serviço, também deverão assinar Termos de Confidencialidade individuais antes do início de suas atividades, assumindo integral responsabilidade pelo sigilo e pela adequada manipulação das informações.

A contratada deverá observar, rigorosamente, os normativos internos do PJAC, a legislação vigente (incluindo a Lei nº 13.709/2018 – LGPD) e as diretrizes específicas de segurança da informação do Poder Judiciário, como previsto na Resolução CNJ nº 396/2021, respeitando todos os protocolos técnicos, administrativos e legais aplicáveis.

O compromisso de sigilo e confidencialidade será irrevogável e permanecerá vigente mesmo após o encerramento do contrato, protegendo o PJAC de eventuais riscos de vazamento, exposição ou uso indevido de informações institucionais ou dados pessoais tratados pela organização.

Além disso, todos os recursos técnicos utilizados na prestação dos serviços deverão estar em conformidade com os regulamentos de segurança e as normas disciplinares instituídas pelo PJAC, inclusive durante acessos presenciais às instalações físicas. Quando houver trabalho remoto, deverão ser utilizados métodos seguros de acesso, como canais criptografados, autenticação multifator e conexão VPN, de modo a proteger a comunicação e garantir a rastreabilidade das ações executadas.

A observância rigorosa desses requisitos é fundamental para garantir a confiança, a legalidade e a proteção dos ativos de informação institucionais, assegurando que a operação do SOC seja realizada em conformidade com os mais elevados padrões de governança e segurança.

1.3.3.8. Requisitos Sociais, Ambientais e Culturais:

A presente contratação, em alinhamento com as diretrizes de governança e sustentabilidade do Poder Judiciário, exige da Contratada a demonstração e o compromisso inequívoco com a observância de preceitos sociais, ambientais e culturais. A solução de Tecnologia da Informação e Comunicação (TIC) e os serviços a serem prestados deverão estar em estrita conformidade com a legislação vigente, os normativos institucionais e as melhores práticas aplicáveis, assegurando uma atuação responsável e alinhada aos valores públicos.

Conformidade com a Política de Sustentabilidade

- A contratada deverá tomar pleno conhecimento do Plano de Logística Sustentável (PLS) do Poder Judiciário do Estado do Acre, das Orientações do Controle Interno e demais procedimentos internos do PJAC pertinentes à sustentabilidade e responsabilidade social e econômica.
- Em estrita observância à Resolução CNJ nº 400/2021, que institui a Política de Sustentabilidade no âmbito do Poder Judiciário, a Contratada deverá integrar os princípios da gestão ambiental, social e econômica em suas operações e na prestação dos serviços.
- Caso a natureza específica dos serviços ou produtos não se enquadre diretamente nas condições exigidas pelos critérios de Sustentabilidade Ambiental, Social e Econômica do PLS ou de outros normativos aplicáveis, a Contratada deverá apresentar justificativa formal e fundamentada para tal inaplicabilidade.

Aspectos Linguísticos e Culturais:

- A solução de TIC e a interação na prestação dos serviços deverão estar em conformidade com os costumes e idiomas do contexto brasileiro, priorizando o idioma Português do Brasil em todas as interfaces, documentações e comunicações operacionais e gerenciais.
- Deverá ser assegurada a adequação da solução e dos serviços à cultura organizacional e funcional do Poder Judiciário, garantindo a interoperabilidade humana e sistêmica sem fricções indevidas ou necessidade de adaptações onerosas por parte do Contratante.

Alinhamento a Normativos de Alta Relevância:
A atuação da Contratada, bem como a solução e os serviços fornecidos, deverão demonstrar alinhamento e conformidade robusta com as seguintes normativas, que permeiam os aspectos sociais (privacidade) e ambientais (gestão de ativos e segurança):

- Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018): Essencial para o tratamento de dados pessoais com segurança e respeito à privacidade.
- ISO/IEC 27001: Padrão internacional para Sistemas de Gestão de Segurança da Informação, fundamental para a proteção do ambiente de TIC.

- Resolução CNJ nº 396/2021: Política de Segurança da Informação do Poder Judiciário, que estabelece diretrizes e responsabilidades para a proteção da informação.
- TPADM TJAC nº 291/2023 (segurança da informação): Normativo interno do Tribunal de Justiça do Estado do Acre que complementa as diretrizes de segurança.

A estrita observância a estes requisitos é imperativa e será objeto de fiscalização durante toda a vigência contratual, visando a garantir que a contratação não apenas atenda às necessidades técnicas de segurança, mas também promova e reforce as políticas de responsabilidade socioambiental e cultural do Poder Judiciário.

1.3.3.9. Requisitos Legais:

A solução e os serviços contratados deverão observar os seguintes instrumentos normativos e legais, nacionais e internacionais:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CNJ nº 396/2021 – Política de Segurança da Informação do Judiciário;
- Resolução PJAC nº 334/2025 – Política de Segurança da Informação do PJAC;
- ISO/IEC 27001: Para manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) formal, com base em políticas, processos e controles voltados à confidencialidade, integridade e disponibilidade da informação;
- NIST Cybersecurity Framework (NIST CSF): Para estruturação de controles voltados à identificação, proteção, detecção, resposta e recuperação frente a incidentes de segurança cibernética;
- CIS Controls (Center for Internet Security): Para implementação de medidas práticas e priorizadas de defesa, voltadas à proteção de sistemas, redes e ativos críticos.

1.3.3.10. Demais Requisitos Aplicáveis (Capacidade Técnica):

Para comprovar a aptidão para execução dos serviços do objeto desta contratação, a empresa CONTRATADA deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste TR.
Os atestados deverão:

- Estar relacionados à atividade econômica principal ou secundária da licitante, conforme contrato social vigente; Conter identificação da empresa emitente e da empresa prestadora (CNPJ e endereço);
- Informar a descrição dos serviços prestados, prazos de execução e grau de satisfação da contratante;
- Poderão ser apresentados em nome da matriz ou filial da licitante;
- Ser acompanhados de documentos que comprovem sua legitimidade, como cópia do contrato que originou os serviços, endereço da contratante e local de execução.
- Os proponentes deverão comprovar experiência prévia em projetos de segurança de porte e complexidade semelhantes ao certame.

1.3.3.10.1. SOC-Blue Team/SIEM/Threat Intelligence/Gestão de vulnerabilidade: Grupo 1

Apresentar atestado que comprove o fornecimento de serviços gerenciados de monitoramento e acionamento contínuo de SOC em escala 24x7 com serviço gerenciado para sustentação, configuração, suporte, operação, monitoramento e acionamento contínuo de SOC, através da plataforma de SIEM utilizada pelo CONTRATANTE, contendo no mínimo:

Volume mínimo de eventos de segurança: 550 GB/Dia; Podem ser efetuadas as somas de atestados para a comprovação dos entregáveis das soluções de SIEM.

Apresentar atestado que comprove o Fornecimento de Serviços gerenciados de governança:

- Gerenciamento de incidentes;
- Melhoria Contínua;
- Gerenciamento de mudanças;
- Gerenciamento de capacidade e Desempenho;
- Gestão de processos.

Apresentar atestado que comprove o Fornecimento de Serviços gerenciados para sustentação e operação de soluções de Gestão de Vulnerabilidades para no mínimo 4000 ativos, os serviços devem minimamente conter:

- Organização de grupos de ativos na console da solução de Gestão de Vulnerabilidades (GV);
- Reportar Vulnerabilidades nos ativos monitorados pela console de GV;
- Reportar status sobre o ambiente de GV; Gerenciar patches.

Apresentar atestado que comprove a capacidade de entrega de Serviços de Inteligência de Ameaças em modelo 24x7, operados a partir do Centro de Operações próprio. Contendo minimamente os seguintes serviços:

- Monitoramento de Deep e Dark web;
- Serviços de Takedown;
- Serviços de Hunting de ameaças;
- Monitoramento de Perfis de usuários.

1.3.3.10.2. Serviços de testes de invasão (Red Team): Item 7

Apresentar atestados que comprovem o fornecimento de Pentest e testes de Phishing, contendo serviços de:

- Redes WIFI;
- Infraestrutura;
- Aplicações WEB;
- API´s.

1.3.3.10.3. Cultura de Cibersegurança: Grupo 3

Apresentar atestado que contemple, no mínimo, a execução de campanhas educativas, treinamentos em segurança da informação, simulações de phishing e vishing, produção de materiais educativos ou programas de conscientização em larga escala.

Apresentar comprovação de disponibilidade de ambiente tecnológico seguro e escalável para execução dos treinamentos, em língua portuguesa (pt-BR), capaz de fornecer relatórios de engajamento, indicadores de risco humano e simulações de ataques

1.3.3.11. Documentos de comprovação dos profissionais

A licitante deverá comprovar experiência prévia em projetos de segurança da informação de porte e complexidade semelhantes, atendendo aos requisitos mínimos estabelecidos neste Termo de Referência, tais como: serviços gerenciados de SOC em regime 24x7, gestão de vulnerabilidades em larga escala, inteligência de ameaças, governança de segurança, pentests e simulações de phishing, conforme detalhado nas especificações técnicas.

Para fins de habilitação técnico-profissional, a licitante deverá indicar os profissionais responsáveis pela execução do objeto contratual, apresentando seus currículos e respectivas certificações, em conformidade com os requisitos deste Termo de Referência.

Será obrigatória a comprovação do vínculo formal destes profissionais com a empresa licitante, admitindo-se como comprovação:

(i) cópia da Carteira de Trabalho e Previdência Social – CTPS assinada pelo empregador;
(ii) contrato de trabalho firmado entre a empresa e o profissional; ou
(iii) contrato de prestação de serviços ou vínculo societário formalmente constituído.

Os documentos apresentados deverão comprovar que o vínculo com a empresa existe há, no mínimo, 03 (três) meses anteriores à data da publicação do edital, sob pena de inabilitação.

1.4. Atendimento da demanda

1.4.1. Portal do Software Público Brasileiro

Solução	Origem/Órgão Responsável	Atende à demanda do PJAC?	Observações
SispMonitoramento	Ministério da Gestão / SISP	Não atende	Foco em monitoramento de links, não em segurança da informação.
SGSI - Sistema de Gestão de Segurança da Informação	Ministério da Economia	Não atende	Focado em governança documental, não em monitoramento técnico.
e-SISP (Solução de automação de TIC)	ME / SISP	Não atende	Focado em gestão administrativa de TIC, não em SOC.
Plataforma ConectaGov	ME / Serpro	Não identificada oferta de SOC	Até o momento, não há serviço de SOC disponível para adesão direta.

1.4.2. Soluções de TIC

Com base na necessidade institucional de implementar um Centro de Operações de Segurança (SOC) com monitoramento contínuo, resposta a incidentes e operação 24x7, foram consideradas três soluções distintas:

1.4.2.1. Solução 1: Contratação de empresa especializada com alocação presencial de profissionais no PJAC

Esta solução prevê a contratação de empresa prestadora de serviços de segurança da informação com alocação de equipe técnica nas dependências do PJAC, para operação presencial do SOC utilizando, preferencialmente, os recursos e ferramentas já existentes na instituição, como a plataforma Wazuh.

A principal vantagem desse modelo reside na presença física dos profissionais, o que permite uma maior proximidade com as equipes internas de TIC, favorece a transferência de conhecimento e viabiliza a atuação imediata sobre os ativos institucionais. Além disso, esse modelo mantém os dados sob custódia direta do PJAC e permite a supervisão presencial das atividades.

Por outro lado, trata-se de uma solução que demanda alto custo, devido à necessidade de manter pessoal altamente especializado em regime de plantão ou sobreaviso, o que tende a encarecer o contrato e não garante, de forma eficiente,

a cobertura plena de eventos em turnos noturnos, fins de semana e feriados.

A operação local também apresenta limitações quanto à escalabilidade e à automação de processos, tornando a resposta a incidentes dependente da capacidade da equipe reduzida presente no local. Ademais, está sujeita a interrupções por fatores externos, como indisponibilidade de transporte, clima ou greves.

Embora seja tecnicamente possível, esta alternativa não atende integralmente aos requisitos de operação contínua 24x7, escalabilidade e resiliência, sendo, portanto, considerada apenas como uma solução intermediária ou complementar, mas não suficiente como abordagem principal.

1.4.2.2. Solução 2: Contratação de empresa especializada para operação remota 24x7 (modelo SOC-as-a-Service)

A segunda alternativa analisada consiste na contratação de empresa especializada para prestação remota do serviço de SOC em regime ininterrupto (24x7x365), operando a partir de sua própria central de segurança, mas utilizando como base a infraestrutura técnica do PJAC, com destaque para a instância do sistema Wazuh já implantada internamente como SIEM.

Nessa abordagem, a contratada será responsável por absorver a operação do Wazuh, promover sua evolução técnica e arquitetural, desenvolver e manter regras de correlação, painéis de monitoramento, relatórios automatizados e respostas coordenadas a incidentes cibernéticos.

- Entre as principais vantagens dessa alternativa, destacam-se:
- Capacidade de prover operação real 24x7, com múltiplos níveis de suporte e especialização técnica, garantida por equipes multidisciplinares e escalonadas por turnos contínuos;
- Escalabilidade e alta disponibilidade, com capacidade de suportar picos de eventos e múltiplos incidentes simultâneos, por meio de arquiteturas robustas, redundantes e com balanceamento de carga;
- Redução significativa de custos com infraestrutura física, pessoal local e encargos trabalhistas;
- Adoção de ferramentas modernas de automação e resposta (SOAR), possibilitando contenção de ameaças em tempo real;
- Cumprimento dos requisitos normativos de segurança, privacidade e transparência, por meio de mecanismos de auditoria, logs imutáveis, geração de evidências e registros históricos;
- Garantia de que toda a infraestrutura lógica e os dados sensíveis permaneçam sob custódia do PJAC, assegurando a soberania institucional e o atendimento à LGPD e à Resolução CNJ nº 396/2021;
- Possibilidade de estabelecimento de indicadores de desempenho (SLAs) claros e objetivos, com aplicação de penalidades em caso de descumprimento.

A alternativa de prestação de serviço remoto, no modelo SOC-as-a-Service, representa a solução mais aderente às exigências institucionais, proporcionando agilidade na implantação, robustez na operação, previsibilidade contratual e alinhamento com as melhores práticas da Administração Pública.

Conclusão

Após análise técnica comparativa das alternativas, conclui-se que a contratação de empresa especializada para prestação remota dos serviços de SOC (Solução 2) representa a abordagem mais eficiente, econômica e segura para atender às necessidades do PJAC.

Essa alternativa possibilita o aproveitamento da infraestrutura já existente, promove a modernização da arquitetura de segurança cibernética, garante operação contínua com expertise técnica e assegura a conformidade com os marcos

normativos aplicáveis ao Poder Judiciário.

1.4.3. Contratações Públicas Similares

1.4.3.1. Prefeitura Municipal de Vila Velha (PMVV)
Processo nº 32524/2024

A Prefeitura de Vila Velha contratou serviços especializados de Centro de Operações de Segurança (SOC) com operação remota em regime 24x7, abrangendo monitoramento de ativos, correlação de eventos, resposta a incidentes e relatórios de segurança, a contratação contempla modelo SOC-as-a-Service, com prestação de serviços contínuos e centralizados por empresa especializada, mantendo a infraestrutura sob controle da Administração Pública.
A experiência da Prefeitura de Vila Velha validou a viabilidade técnica e jurídica do modelo remoto de SOC, com atuação ininterrupta, aderente às boas práticas de segurança e ao perfil de contratação pretendido pelo PJAC.

1.4.3.2. Empresa Brasileira de Hemoderivados e Biotecnologia (HEMOBRÁS)
Processo Administrativo n.º 25800.001168/2023
A HEMOBRÁS contratou serviços de SOC remoto 24x7, com foco em monitoramento contínuo de eventos, gestão de vulnerabilidades, inteligência de ameaças (CTI), relatórios técnicos e resposta a incidentes. A infraestrutura de segurança foi mantida sob controle da contratante, com a prestação realizada remotamente pela empresa especializada.

O modelo adotado é semelhante ao pretendido pelo PJAC, ao integrar serviço especializado com infraestrutura local e garantir conformidade com normas de segurança e proteção de dados. Confirma a viabilidade operacional e contratual do modelo SOC-as-a-Service com base técnica sólida.

1.4.3.3. Poder Judiciário do Estado de Santa Catarina (PJSC)
Pregão Eletrônico N. 90005/2024
O PJSC contratou solução de SOC como serviço (SOC-as-a-Service), com atendimento em regime 24x7, monitoramento remoto, correlação de eventos, gestão de incidentes, e relatórios estratégicos de segurança. O edital exigiu alinhamento à Resolução CNJ nº 396/2021 e à Lei Geral de Proteção de Dados (LGPD).

A contratação é altamente compatível com a proposta do PJAC, tanto em escopo quanto em modelo de operação. Trata-se de referência direta no âmbito do Poder Judiciário, reforçando a adequação técnica e normativa da solução avaliada neste ETP.

1.4.4. Aderência a padrões e modelos

A contratação de soluções de Tecnologia da Informação e Comunicação (TIC) no âmbito do Poder Judiciário requer a verificação da aderência a padrões e modelos de referência que visam a garantir a interoperabilidade, a segurança, a conformidade legal e a sustentabilidade das plataformas e serviços. Embora a aplicabilidade de cada padrão possa variar conforme a natureza e o escopo específico da demanda em estudo, é crucial que a equipe de planejamento e os proponentes analisem a pertinência e demonstrem a conformidade nos aspectos que se conectam ou impactam o objeto da contratação.

Esta seção detalha os modelos a serem considerados, e a Contratada deverá comprovar a compatibilidade da solução ofertada com aqueles que se mostrarem relevantes para o ambiente do Poder Judiciário do Estado do Acre (PJAC) e para

os serviços de SOC.

1.4.4.1. Modelo Nacional de Interoperabilidade - MNI

- **Conceituação:** O MNI, instituído para orientar o desenvolvimento e a aquisição de sistemas de informação do Governo Federal, estabelece um conjunto de princípios e requisitos arquitetônicos para promover a comunicação e o intercâmbio de informações entre diferentes sistemas e órgãos da Administração Pública. Seu objetivo primário é facilitar a integração de dados e processos, eliminando silos e otimizando a prestação de serviços públicos.
- **Requisito de Verificação:** A equipe de planejamento da contratação, bem como a futura Contratada, deverão verificar se a solução de SOC, ou qualquer de seus componentes que envolva troca de informações com outros sistemas governamentais, bases de dados externas ou plataformas de gestão judicial, necessita ser compatível com as diretrizes preconizadas pelo MNI.
- **Justificativa Técnica:** A compatibilidade com o MNI é essencial para assegurar a sinergia dos fluxos de dados, a automação de processos intersetoriais e a conformidade com o ecossistema de TI do Poder Público. Eventuais integrações para ingestão de logs de outras fontes ou exportação de inteligência de ameaças para plataformas compartilhadas devem considerar este modelo.

1.4.4.2. Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil

- **Conceituação:** A ICP-Brasil é a infraestrutura pública brasileira que garante a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais emitidos no âmbito dessa infraestrutura. É a base tecnológica para a segurança de transações eletrônicas e a certificação digital no Brasil.
- **Requisito de Verificação:** A equipe de planejamento da contratação, bem como a futura Contratada, deverão verificar se a demanda requer (ou pode se beneficiar de) a compatibilidade com a ICP-Brasil, especialmente em cenários que envolvam:
  - **Autenticação de Usuários:** Autenticação robusta de usuários (internos e externos) aos sistemas do SOC ou para acesso remoto seguro.
  - **Assinatura Digital:** Assinatura digital de relatórios de incidentes, pareceres técnicos, documentos de auditoria ou evidências forenses produzidas pelo SOC, conferindo-lhes validade jurídica.
  - **Comunicação Segura:** Estabelecimento de canais de comunicação criptografados e autenticados entre o ambiente do PJAC e o SOC da Contratada, utilizando certificados digitais ICP-Brasil.
- **Justificativa Técnica:** A aderência à ICP-Brasil é crucial para garantir a segurança jurídica, o não-repúdio e a confiabilidade das informações e ações executadas no contexto da contratação do SOC, alinhando-se às diretrizes de governo eletrônico e segurança da informação do Estado brasileiro.

1.4.4.3. Modelo de Requisitos MoReq-Jus

- **Conceituação:** MoReq-Jus é uma adaptação brasileira do Modelo de Requisitos para Gestão de Registros Eletrônicos (MoReq2), com foco específico nas necessidades do Poder Judiciário. Este modelo estabelece um conjunto abrangente de requisitos funcionais e não-funcionais para sistemas de gestão de documentos e processos eletrônicos (SGDE) que garantam a autenticidade, a integridade, a confiabilidade e a rastreabilidade dos documentos digitais ao longo de seu ciclo de vida.
- **Requisito de Verificação:** A equipe de planejamento da contratação, juntamente com a futura Contratada, deverão verificar se as entregas do SOC – tais como relatórios de incidentes, dossiês de ameaças, evidências

coletadas em análises forenses e registros de auditoria – necessitam ser gerenciadas como documentos ou registros eletrônicos oficiais do PJAC, e, portanto, demandam conformidade com os requisitos do MoReq-Jus para sua produção, arquivamento e eventual disponibilização.

- **Justificativa Técnica:** A compatibilidade com o MoReq-Jus é vital para assegurar a cadeia de custódia, a validade probatória e a preservação digital das informações geradas pelo SOC que possam vir a compor processos judiciais ou administrativos, conferindo-lhes o devido valor legal e documental no contexto do Poder Judiciário.

1.4.4.4. Contratações correlatas e/ou interdependentes

Após análise técnica e administrativa, não foram identificadas contratações correlatas ou interdependentes ao objeto deste Estudo Técnico Preliminar. A presente demanda trata-se de uma iniciativa autônoma e específica para a contratação de serviços especializados em Segurança Cibernética, não estando vinculada a outras aquisições em curso ou previstas no âmbito do PJAC.

1.5. Análise dos Custos Totais da Demanda

Item	Soluções identificadas	Especificação	CATSER	Qtd	Vantagens e Benefícios	Desvantagens e riscos	Custo(s) envolvido(s)
1	Contratação de empresa especializada com alocação presencial de profissionais no PJAC	Alocação de profissionais técnicos presencialmente no PJAC para operar localmente o SOC, utilizando os recursos próprios do órgão, como o Wazuh, em regime de plantão.	27014	12	Maior proximidade com a equipe interna de TIC. Facilidade na transferência de conhecimento. Supervisão direta das atividades. Maior controle institucional sobre os dados e infraestrutura.	Alto custo mensal. Dificuldade de manter operação contínua 24x7 com equipe presencial. Maior risco de interrupções por ausências físicas (greves, transporte). Menor escalabilidade e automação. Dependência de força de trabalho local especializada e rotatividade.	R$ 237.868,22

2	Contratação de empresa especializada para operação remota 24x7 (modelo SOC-as-a-Service)	Contratação de empresa especializada para operar remotamente o SOC 24x7x365, utilizando a infraestrutura do PJAC, com integração à operação do órgão.	27014	12	Custo significativamente menor. Garantia de cobertura 24x7 com equipes dedicadas em turnos. Alta escalabilidade e disponibilidade. Menor dependência de recursos locais. Acesso a equipes multidisciplinares e indicadores de desempenho (SLAs).	Necessidade de mecanismos de integração e comunicação eficiente. Menor contato presencial com as equipes internas.	R$ 23.719,22

1.6. Escolha e Justificativa da Solução

1.6.1. Descrição da Solução Escolhida

Os serviços gerenciados de segurança cibernética, são compostos pela prestação dos seguintes serviços e soluções de Serviços de Monitoramento, detecção e resposta a incidentes de segurança da informação (Blue Team) através de centro de operação de segurança (SOC), para analisar, correlacionar, remediar, conter e documentar os eventos de segurança da informação. Tal serviço deverá ser executado através de um SOC (Cyber Security Operations Center), obedecendo os principais frameworks de resposta a incidentes de segurança da informação, com Takedown e campanhas de conscientização.

A solução de SIEM (Security Information and Event Management) será fornecida pela Contratante. Compete à empresa Contratada, operar, gerenciar, atualizar, prover melhorias, na solução, realizando a correlação de logs provenientes das diversas fontes de dados monitoradas, com o objetivo de reforçar a postura de segurança da organização.

A atuação deverá garantir: Aumento da visibilidade sobre eventos e atividades críticas; Detecção e resposta em tempo real a incidentes de segurança; Aplicação de inteligência contra ameaças avançadas, por meio de análises comportamentais e indicadores de comprometimento (IoCs); Apoio às equipes de segurança nas tratativas proativas e reativas a incidentes.

Solução de monitoramento de fontes abertas e inteligência Cibernética (Threat Intelligence) e serviços, deve realizar investigação e monitoramento que envolva tanto serviços especializados quanto ferramentas tecnológicas voltadas para a coleta, análise e correlação de informações provenientes de fontes abertas (OSINT), redes sociais, grupos e fóruns em ambientes da Deep e Dark Web, conforme as especificações estabelecidas neste documento.

Serviços de testes de invasão (red team) deverá executar serviços de testes de invasão com o objetivo principal de identificar, mapear, documentar e explorar vulnerabilidades presentes nos sistemas, processos e ativos da infraestrutura

tecnológica da Contratante. Esses testes deverão ser conduzidos de forma controlada e ética, utilizando técnicas, metodologias e ferramentas especializadas, com o intuito de simular ataques reais e avaliar a eficácia dos controles de segurança existentes. As atividades incluirão tentativas deliberadas de obtenção de acesso não autorizado, inclusive com privilégios elevados, aos ativos e informações da Contratante.

As entregas mínimas desse serviço deverão incluir: Relatórios técnicos e executivos com o detalhamento das vulnerabilidades encontradas; Evidências de exploração bem-sucedida, respeitando os limites acordados; Análise de impacto e criticidade dos achados; Recomendações para correção e mitigação dos riscos identificados. Os testes deverão ser realizados em conformidade com normas e boas práticas internacionais, como OWASP, MITRE ATT&CK, NIST e outras aplicáveis, garantindo a segurança, sigilo e integridade dos ambientes analisados.

A gestão de vulnerabilidades deverá ser executada de forma contínua e estruturada, abrangendo a identificação, análise, priorização, tratamento e verificação das vulnerabilidades nos ativos do PJAC. A contratada será responsável por realizar varreduras periódicas, classificando os riscos com base em critérios como CVSS, criticidade do ativo, tendências de exploração e obsolescência. Deverá manter a base de conhecimento atualizada, apoiar a aplicação de correções ou mitigação dos riscos identificados e gerar relatórios periódicos com evidências e indicadores, assegurando rastreabilidade, conformidade e melhoria contínua da postura de segurança da informação do órgão.

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - GRUPOS - Blue Team e Cultura de Cibersegurança			
GRUPO 1 - Blue Team			
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**QTD**
1	Serviço de Monitoramento, detecção e resposta a incidentes de segurança da informação, por meio de um SOC, Blue Team	Mensal	12
2	Administração da solução de SIEM Wazuh, com foco na monitoração e correlação de eventos de segurança	Mensal	12
3	Serviços de Monitoramento em fontes abertas e Inteligência cibernética (Threat Intelligence) com Takedown	Mensal	12
4	Gestão de vulnerabilidades	Mensal	12
GRUPO 2 - Cultura de Cibersegurança			
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**QTD**
5	Ações de Cultura Cibersegurança	Mensal	12
6	Plataforma de treinamento de cibersegurança	Mensal	12

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - ITEM - Red Team			
Red Team			
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**QTD**
7	Serviços de testes de invasão	Unidade	12

O AMBIENTE E QUANTITATIVO A SER MANTIDO E GERENCIADOS PELAS FERRAMENTAS:

Ambiente Computacional a ser monitorado pelo SOC (Security Operations Center):

Quantitativo de IPs externos: 64
Quantitativo de servidores: 500
Quantitativo de endpoints: 2000
Quantitativo de dispositivos de rede: 800

Ambiente Computacional a ser monitorado pela ferramenta de Threat Intelligence (TI):

Domínios a serem monitorados: 1
Aplicações web: 200
Aplicações críticas: 12

Endereços IP ou ranges de interesse relacionados à superfície de ataque exposta: 64
Takedowns Por Ano: 5

Ambiente Computacional a ser monitorado pela solução de Gestão de Vulnerabilidades (GV):
Quantitativo de ativos
Quantitativo de servidores: 500
Quantitativo de endpoints: 2000
Quantitativo de dispositivos de rede: 800
Aplicações web: 200

Itens a serem realizados nos Testes de Intrusão (Pentests):
Ambiente: aplicações web: 200
IPs externos: 64
Aplicações críticas: 12
Quantidade de Pentests: 12 testes em ativos mais retestes após correções

Cultura de Cibersegurança:
Campanhas de phishing: 4 ações para para 2000 pessoas
Phishing: Ilimitados
Campanhas de vishing: 2 ações para 10 pessoas
Campanhas de conscientização: 2 ações para 2000 pessoas, sendo pelo menos 1 presencial
Plataforma de treinamento: Para 2000 pessoas
Plataforma de gamificação: Para 2000 pessoas
Elaboração de cards e material educativo personalizados: Ilimitado

1.6.2. Benefícios Esperados

A contratação de serviços especializados de Centro de Operações de Segurança (SOC), com operação ininterrupta (24x7) e atuação combinada de equipes Blue Team e Purple Team, trará benefícios significativos ao Poder Judiciário do Estado do Acre (PJAC), tanto do ponto de vista técnico quanto gerencial e institucional.

A solução proposta contribuirá diretamente para o aumento da eficácia, eficiência, economicidade e padronização dos processos de segurança da informação, conforme se detalha a seguir:

1.6.2.1. Eficácia

Redução substancial dos riscos cibernéticos relacionados à perda de dados, interrupção de serviços judiciais e comprometimento da imagem institucional do PJAC.

Aumento da resiliência dos ativos de informação e das infraestruturas críticas, por meio da eliminação de pontos cegos e da visibilidade total do ambiente tecnológico.

Detecção precoce e resposta imediata a incidentes, viabilizando contenção de ameaças com menor impacto operacional.

Geração de inteligência cibernética aplicável à governança e à gestão de riscos, por meio de relatórios técnicos, painéis gerenciais e apurações especializadas.

1.6.2.2. Eficiência

Automatização de processos como correlação de eventos, alertas, investigações e contenção de ameaças, reduzindo a dependência de força de trabalho manual.

Diagnóstico contínuo da postura de segurança, com base nas simulações conduzidas pelo Purple Team e nas rotinas de auditoria técnica.

Apoio direto à tomada de decisão, mediante relatórios operacionais e estratégicos disponibilizados para os gestores do PJAC.

Capacitação e transferência de conhecimento para as equipes internas de TIC, promovendo evolução técnica permanente e internalização de boas práticas.

1.6.2.3. Economicidade

Redução de custos operacionais indiretos, ao evitar paralisações, perdas de dados e necessidade de retrabalho após incidentes cibernéticos.

Otimização dos investimentos em segurança, com base em análises técnicas precisas sobre vulnerabilidades, priorização de ativos e medidas corretivas.

Economia potencial com a correção preventiva de irregularidades técnicas antes da entrada em produção de novos sistemas e serviços.

Melhor custo-benefício frente à alternativa de implantação de um SOC interno, que exigiria investimentos elevados em equipe própria e infraestrutura física dedicada.

1.6.2.4. Padronização

Adoção de práticas alinhadas a frameworks consolidados, como ISO/IEC 27001, NIST CSF e MITRE ATT&CK, promovendo padronização dos processos de monitoramento, resposta e auditoria.

Atualização contínua da Política de Segurança da Informação, com base em evidências reais, indicadores técnicos e ameaças emergentes.

Implantação de processos formais de responsabilização e resposta a incidentes, incluindo registro, análise e lições aprendidas.

Engajamento da alta administração institucional, mediante a comunicação regular de riscos e eventos relevantes em formato padronizado.

1.6.2.5. Atendimentos aos aspectos específicos exigidos

Economia potencial com a correção de potenciais irregularidades:

- A atuação proativa do SOC permite identificar falhas de configuração, acessos indevidos e vulnerabilidades antes que gerem incidentes graves ou prejuízos institucionais, evitando custos com contenção emergencial ou prejuízos à imagem do PJAC.

Resolução de irregularidades não associadas a pagamentos:

- A operação do SOC garante a detecção e correção de falhas técnicas, más práticas operacionais e exposições indevidas que, embora não envolvam transações financeiras, afetam a conformidade institucional e a segurança jurídica dos serviços prestados.

Utilização de menor força de trabalho com automação:

- O uso de soluções de SIEM, scripts e playbooks de resposta permite tratar milhares de eventos automaticamente, reduzindo a necessidade de equipes grandes e tornando a operação mais ágil e sustentável.

Agilidade e maior segurança na gestão de pessoas:

- Com mecanismos de auditoria e rastreabilidade, é possível identificar desvios de conduta, acessos indevidos ou violações às normas de uso aceitável de forma rápida e assertiva, promovendo responsabilização e melhoria contínua.

1.6.3. Resultados Esperados

- **Monitoramento contínuo dos ativos de TI:** Garante a supervisão ininterrupta de sistemas e redes, possibilitando a identificação imediata de comportamentos anômalos ou suspeitos, conforme determina a Resolução CNJ nº 396/2021.
- **Detecção precoce e resposta rápida a incidentes de segurança:** Minimiza o tempo entre a ocorrência de um incidente e sua contenção, reduzindo impactos operacionais, jurídicos e reputacionais para o PJAC.
- **Produção de inteligência proativa sobre ameaças:** Permite a antecipação a riscos cibernéticos por meio da análise de indicadores de comprometimento (IoCs) e tendências de ataques, fortalecendo a postura preventiva da instituição.
- **Registro e rastreabilidade dos eventos de segurança:** Garante a coleta e armazenamento adequados de logs e evidências digitais, contribuindo para auditorias, apuração de responsabilidades e cumprimento da LGPD (Lei nº 13.709/2018).
- **Gestão contínua de vulnerabilidades:** Identifica, avalia e prioriza correções em falhas de segurança nos sistemas e ativos do PJAC, reduzindo a superfície de ataque e prevenindo explorações.
- **Alinhamento às normas e boas práticas de segurança:** Atende às exigências da Recomendação CNJ nº 73/2020 e normas técnicas reconhecidas (ISO/IEC 27001, NIST), promovendo conformidade e governança de TIC.
- **Fortalecimento da resiliência institucional:** Aumenta a capacidade do PJAC de suportar, reagir e recuperar-se rapidamente de incidentes cibernéticos, assegurando a continuidade dos serviços essenciais à população.
- **Suporte à conformidade com a LGPD:** O SOC atua na proteção dos dados pessoais tratados pelo PJAC, em conformidade com o artigo 46 da LGPD, mitigando riscos de sanções e danos à imagem institucional.
- **Melhoria da tomada de decisão estratégica em segurança:** A centralização das informações de segurança permite relatórios gerenciais e indicadores que subsidiam a alta gestão na definição de políticas e investimentos.
- **Redução do risco de comprometimento da imagem institucional:** Ao prevenir e mitigar incidentes de alto impacto, como vazamentos ou indisponibilidades, o SOC contribui para a preservação da confiança da sociedade no PJAC como guardião de dados sensíveis e dos direitos fundamentais.

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

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - GRUPOS - Blue Team e Cultura de Cibersegurança
GRUPO 1 - Blue Team

ID	DESCRIÇÃO DO BEM OU SERVIÇO	CATSER	UND	Qtd Unitária	Qtd Total
1	Serviço de Monitoramento, detecção e resposta a incidentes de segurança da informação, por meio de um SOC, Blue Team	27014	Mensal	12	12
2	Administração da solução de SIEM Wazuh, com foco na monitoração e correlação de eventos de segurança	27014	Mensal	12	12
3	Serviços de Monitoramento em fontes abertas e Inteligência cibernética (Threat Intelligence) com Takedown	27014	Mensal	12	12
4	Gestão de vulnerabilidades	27014	Mensal	12	12
GRUPO 2 - Cultura de Cibersegurança					
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**UND**	**UND**	**QTD**
5	Ações de Cultura Cibersegurança	27014	Mensal	12	12
6	Plataforma de treinamento de cibersegurança	27014	Mensal	12	12

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - ITEM - Red Team					
Red Team					
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**UND**	**UND**	**QTD**
7	Serviços de testes de invasão	27014	Unidade	12	12

1.6.5. Estimativa do Custo Total da Solução Escolhida

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - GRUPOS - Blue Team e Cultura de Cibersegurança					
GRUPO 1 - Blue Team					
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**Qtd Unitária**	**Valor Unitário**	**Valor Total**
1	Serviço de Monitoramento, detecção e resposta a incidentes de segurança da informação, por meio de um SOC, Blue Team	Mensal	12	R$ 19.509,79	R$ 234.117,48
2	Administração da solução de SIEM Wazuh, com foco na monitoração e correlação de eventos de segurança	Mensal	12	R$ 26.233,35	R$ 314.800,14
3	Serviços de Monitoramento em fontes abertas e Inteligência cibernética (Threat Intelligence) com Takedown	Mensal	12	R$ 28.500,00	R$ 342.000,00
4	Gestão de vulnerabilidades	Mensal	12	R$ 24.363,00	R$ 292.356,00
GRUPO 2 - Cultura de Cibersegurança					
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**Qtd Unitária**	**Valor Unitário**	**Valor Total**
5	Ações de Cultura Cibersegurança	Mensal	12	R$ 11.475,92	R$ 137.711,04
6	Plataforma de treinamento de cibersegurança	Mensal	12	R$ 10.389,68	R$ 124.676,10

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - ITEM - Red Team					
Red Team					
ID	**DESCRIÇÃO DO BEM OU SERVIÇO**	**UND**	**Qtd Unitária**	**Valor Unitário**	**Valor Total**
7	Serviços de testes de invasão	Unidade	12	R$ 32.899,50	R$ 394.794,00

A estimativa total da contratação e de **R$ 1.840.454,76 (Um milhão, oitocentos e quarenta mil, quatrocentos e cinquenta e quatro reais e setenta e seis cenvatos)**.

1.7. Declaração de viabilidade da contratação

1.7.1. Declaração de Viabilidade:

(x) Viável;
( ) Viável com restrições;
( ) Inviável.

1.7.2. Justificativa:

A deliberação pela **Viabilidade** da contratação dos serviços de Centro de Operações de Segurança (SOC), conforme declaração no subtópico 1.7.1, é o resultado de uma análise pormenorizada e multidimensional, que perpassou a contextualização da demanda, o alinhamento estratégico, a caracterização técnica e a prospecção de mercado, culminando na avaliação econômica das alternativas.

Com base nas informações consolidadas neste Estudo Técnico Preliminar (ETP), observam-se os seguintes fundamentos para a viabilidade da contratação:

- **Necessidade e Alinhamento Estratégico:** A contextualização da demanda revelou a imperativa lacuna na estrutura de segurança cibernética do PJAC, expondo-o a riscos operacionais e regulatórios crescentes. A contratação do SOC alinha-se diretamente com os macrodesafios e objetivos estratégicos definidos no Plano Estratégico Institucional (PEI) e no Plano Diretor Institucional (PDTIC), bem como com a previsão do Plano Anual de Contratação de TIC (PSTIC) de 2025, garantindo que o investimento seja direcionado a uma prioridade institucional de alta relevância.
- **Aderência aos Requisitos Técnicos e Operacionais:** A caracterização detalhada das necessidades e a especificação dos requisitos técnicos (incluindo *Blue Team*, administração de SIEM, *Threat Intelligence*, *Red Team* e Gestão de Vulnerabilidades) demonstram a clareza e a profundidade da demanda. A solução de **contratação de empresa especializada para operação remota 24x7 (modelo SOC-as-a-Service)** foi identificada como a mais apta a atender a esses requisitos de forma integral, promovendo monitoramento contínuo, detecção precoce e resposta estruturada a incidentes.
- **Validação de Mercado e Experiência Comprovada:** A análise das soluções de mercado e a prospecção de contratações públicas similares (conforme detalhado no subtópico 1.4.3) validaram a exequibilidade e a maturidade do modelo SOC-as-a-Service, evidenciando sua aplicação exitosa em outros órgãos da Administração Pública com desafios análogos, incluindo outras Cortes do Poder Judiciário.
- **Análise de Custos Totais da Demanda e Vantajosidade Econômica (TCO):** A rigorosa **Análise dos Custos Totais da Demanda (TCO)**, detalhada no subtópico 1.5, demonstrou que a solução de **SOC-as-a-Service** apresenta o **custo total de propriedade mais vantajoso** para o PJAC. Comparativamente à alternativa de alocação presencial de profissionais, o modelo gerenciado resultou em uma **redução significativa dos custos envolvidos**, minimizando o investimento inicial em infraestrutura própria e mitigando os desafios inerentes à manutenção de equipes altamente especializadas em regime 24x7. A memória de cálculo confirmou que, além dos benefícios técnicos e operacionais, a escolha do modelo gerenciado otimiza a alocação dos recursos orçamentários, evidenciando uma decisão economicamente racional e eficiente.

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

A execução da contratação principal dos serviços de Centro de Operações de Segurança (SOC) exige uma análise prospectiva das necessidades de recursos materiais e humanos complementares que deverão ser providos pelo Poder Judiciário do Estado do Acre (PJAC) para assegurar a plena funcionalidade e a efetiva fiscalização do contrato.

- **Identificação de Contratações Imprescindíveis:** Deverá ser realizada uma avaliação para identificar e documentar quaisquer outras contratações, sejam elas de bens ou serviços, que se configurem como imprescindíveis e interdependentes para o êxito da execução da contratação principal do SOC. Isso pode incluir, mas não se limita a, licenças de software adicionais, equipamentos de rede específicos para integração, ou serviços de consultoria para auditoria independente.
- **Gestão de Recursos Humanos Internos:**
    - **Dimensionamento da Equipe de Fiscalização e Gestão Contratual:** Será necessário identificar a demanda por recursos humanos internos do PJAC para atuar na fiscalização técnica, administrativa e setorial do contrato do SOC. Isso envolve a definição de perfis, quantitativos e, se necessário, a terceirização de parte dessas atividades, sempre em conformidade com a legislação aplicável.
    - **Requisitos de Habilidades e Capacitação:** Deverão ser estabelecidas as habilidades técnicas mínimas esperadas dos servidores ou empregados que integrarão a equipe de gestão e fiscalização contratual. Adicionalmente, será prioritária a identificação da necessidade de programas de treinamento e capacitação específicos, visando a aprimorar o conhecimento sobre as tecnologias, metodologias e processos envolvidos na operação de um SOC, capacitando-os para uma fiscalização efetiva e para a absorção de conhecimento.

2.3. Continuidade do Fornecimento

O planejamento para a continuidade do fornecimento dos serviços de SOC é um elemento crítico de mitigação de riscos, visando a preservar a operacionalidade do Poder Judiciário em cenários de interrupção contratual. Esta seção deve delinear as estratégias e ações proativas a serem implementadas pelo PJAC.

- **Planejamento para Interrupção Contratual:** Deverá ser elaborado um plano de continuidade que aborde as ações e estratégias a serem adotadas pelo PJAC em caso de interrupção abrupta ou programada do fornecimento dos serviços pela Contratada.
- **Identificação de Hipóteses de Descontinuidade Técnica:** Serão levantadas e analisadas as hipóteses que podem motivar a descontinuidade do fornecimento da Solução de TIC por motivos estritamente técnicos (e.g., falência do fornecedor, incapacidade tecnológica, incidentes de segurança de grande escala afetando a Contratada, greves ou eventos de força maior). Para cada hipótese, deverão ser detalhadas as ações de contingência a serem adotadas pelo PJAC para minimizar o impacto.
- **Impacto nas Atividades Institucionais:** É mandatório que este item explicite, de forma inequívoca, os efeitos potenciais de uma eventual descontinuidade dos serviços de SOC sobre as atividades essenciais do PJAC. Isso

inclui a avaliação do impacto na integridade e disponibilidade dos dados, na continuidade dos serviços judiciais e na capacidade de resposta a novas ameaças cibernéticas.

- **Natureza do Objeto:** Deverá ser formalmente classificado se a necessidade do objeto de SOC é **permanente** (caráter essencial e contínuo para a missão institucional) ou **pontual** (associada a um projeto específico e com prazo definido). Para um SOC, a natureza é, por essência, permanente e continuada, o que reforça a criticidade do plano de continuidade.
- **Integração com a Matriz de Riscos:** Todas as hipóteses de descontinuidade do fornecimento e seus respectivos efeitos deverão ser formalmente incorporadas e tratadas na Matriz de Gerenciamento de Riscos do processo de contratação, com a definição de probabilidades, impactos e estratégias de tratamento (prevenção, mitigação e contingência).

2.4. Transição Contratual e Encerramento do Contrato

A fase de transição contratual e o encerramento do contrato são momentos críticos que exigem um planejamento detalhado para garantir a continuidade dos serviços e a segurança da informação, mesmo em cenários de substituição de fornecedor ou finalização do vínculo contratual.

- **Hipóteses de Descontinuidade Administrativa:** Serão levantadas as hipóteses que podem motivar a descontinuidade do fornecimento da Solução de TIC por motivos de ordem administrativa (e.g., término da vigência sem prorrogação, rescisão contratual por inadimplemento, decisão de não renovação).
- **Plano de Transição e Encerramento:** Deverá ser descrito um plano abrangente de atividades técnicas mandatórias a serem realizadas pela Contratada para a transição e encerramento formal do contrato, assegurando a mínima interrupção e a completa recuperação do controle por parte do PJAC. Este plano deverá incluir, no mínimo, as seguintes regras:
    - **a. Entrega de Versões Finais:** Formalização da entrega de todas as versões finais de produtos, artefatos, documentações (incluindo diagramas de arquitetura, configurações de ferramentas, playbooks de resposta a incidentes) e relatórios técnicos resultantes da prestação dos serviços.
    - **b. Transferência de Conhecimento:** Realização de sessões formais de transferência de conhecimento (*knowledge transfer*) sobre a execução e a manutenção da Solução de TIC, incluindo treinamentos para a equipe interna do PJAC sobre a operação das ferramentas e processos utilizados pela Contratada.
    - **c. Devolução de Recursos Materiais:** Processo claro para a devolução de quaisquer recursos materiais (equipamentos, dispositivos, credenciais físicas) disponibilizados pelo PJAC à Contratada.
    - **d. Revogação de Perfis de Acesso:** Procedimento para a imediata revogação de todos os perfis de acesso (lógicos e físicos) concedidos aos profissionais da Contratada no ambiente do PJAC ao final do contrato.
    - **e. Eliminação de Caixas Postais e Contas:** Eliminação segura de caixas postais, contas de usuário e demais acessos virtuais criados para a Contratada no ambiente do PJAC, garantindo a desvinculação completa.
    - **f. Garantia da Cadeia de Custódia de Dados:** Assegurar a integridade e a disponibilidade de todos os dados e logs coletados e processados durante a vigência do contrato, garantindo que o PJAC mantenha a propriedade e o controle sobre essas informações, que são cruciais para auditorias futuras e investigações.

2.5. Estratégia de Independência Tecnológica

A elaboração de uma estratégia robusta de independência tecnológica é fundamental para proteger o Poder Judiciário do aprisionamento tecnológico (*vendor lock-in*), garantindo a flexibilidade e a liberdade de escolha futuras na gestão de suas

soluções de TIC.

- **Critérios de Independência:** Serão estabelecidos critérios claros e vinculantes para assegurar a independência tecnológica do PJAC em relação à Contratada. Esses critérios devem abranger:
  - **Transferência de Conhecimento:** A Contratada deverá promover a transferência efetiva e completa de conhecimento sobre a arquitetura, configuração, operação e manutenção de todos os componentes da solução de SOC, capacitando a equipe interna do PJAC a assumir a gestão ou a transitar para outro provedor, se necessário.
  - **Direito à Propriedade Intelectual:** Deverá ser formalmente definido e garantido o direito do PJAC sobre a propriedade intelectual de todo e qualquer software, código-fonte, configurações, customizações, modelos de dados, documentação e demais produtos ou ativos intelectuais que venham a ser desenvolvidos ou adaptados especificamente para o Contratante durante a execução do contrato. Caso haja elementos com direitos exclusivos da Contratada, estes deverão ser devidamente justificados e não poderão comprometer a operacionalidade do SOC ou a transição para outra solução.
  - **Abertura e Interoperabilidade:** A solução contratada deverá ser baseada em padrões abertos e amplamente aceitos no mercado, facilitando a interoperabilidade com sistemas existentes e futuros do PJAC, e minimizando a dependência de tecnologias proprietárias que restrinjam a portabilidade de dados ou a substituição de componentes.
  - **Documentação e Acesso a Configurações:** A Contratada deverá manter documentação completa e atualizada de todas as configurações, políticas, regras e procedimentos implementados, garantindo que o PJAC tenha pleno acesso a essas informações para fins de auditoria, manutenção e eventual transição.

2.6. Sanções contratuais

2.6.1. Das sanções administrativas

Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

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

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

f) praticar ato fraudulento na execução do contrato;

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

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

2.6.2. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

- Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;
- Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

- Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

2.6.2.1. Multa:

- Moratória, para as infrações descritas no item “d”, de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias.
- Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;
- O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
- Compensatória, para as infrações descritas acima alíneas “e” a “h” de 5% (cinco por cento) a 10% (dez por cento) do valor da contratação.
- Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 5% (cinco por cento) a 10% (dez por cento) do valor da contratação.
- Compensatória, para a infração descrita acima na alínea “b”, de 5% (cinco por cento) a 10% (dez por cento) do valor da contratação.
- Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 5% (cinco por cento) a 10 (dez por cento) do valor da contratação.
- Compensatória, para a infração descrita acima na alínea “a”, de 5% (cinco por cento) a 10% (dez por cento) do valor da contratação.

2.6.3. São, também, situações passíveis de aplicação de multas por inexecução total ou parcial do objeto do Contrato ou pelo descumprimento de obrigações contratuais:

- Deixar de realizar o pagamento dos salários, inclusive férias e 13º salário, vale transporte e vale refeição;
- Deixar de registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal;
- Deixar de cumprir quaisquer dos itens do Contrato e seus anexos não previstos nesta tabela de multas, por item e por ocorrência;
- Deixar de apresentar, quando solicitado, documentação fiscal, trabalhista, previdenciária e outros documentos necessários à comprovação do cumprimento dos demais encargos trabalhistas;
- Permitir a presença de empregado sem asseio pessoal, mal apresentado e/ou sem crachá e/ou sem uniforme;
- Recusar-se a executar serviço previsto no Edital e determinado pela fiscalização, sem motivo justificado;
- Deixar de cumprir determinação formal ou instrução complementar da fiscalização, sem motivo justificado;
- Deixar de indicar e manter durante a execução do Contrato os prepostos previstos no Edital/Contrato;
- Deixar posto de trabalho desocupado, sem motivo justificado e/ou sem anuência da fiscalização;
- Na apuração mensal do Nível Mínimo de Serviço (NMS) o mesmo indicador ficar abaixo da meta por três meses consecutivos;
- Utilizar as dependências do PJAC para fins diversos do objeto do Contrato;
- Deixar de efetuar os pagamentos de salários ou benefícios, conforme previsto no presente Termo de Referência;
- Manter empregado sem qualificação para executar os serviços contratados;
- Deixar de efetuar os recolhimentos das contribuições sociais da Previdência Social ou do FGTS, ou arcar com quaisquer despesas diretas/ou indiretas relacionadas à execução do Contrato nas datas avençadas;
- Deixar de realizar o treinamento dos colaboradores a cada 6 (seis) meses, conforme previsto no Plano de Capacitação homologado;

- Deixar de afastar e/ou substituir, após notificação, empregado que se conduza de modo inconveniente ou incompatível com suas atribuições;
- Destruir ou danificar propriedade, material ou imaterial, do PJAC por culpa ou dolo de seus agentes;
- Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais;
- Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais nas dependências do PJAC.
- Atrasar a disponibilização dos relatórios gerenciais;
- Atrasar o fornecimento de itens do uniforme;
- Atrasar na apresentação do Plano de Capacitação e/ou Plano de Transferência de Conhecimento;
- Atrasar prazo descrito nas ações de início, de transição e de encerramento contratual;
- Atrasar na apresentação de resposta às notificações/questionamentos recebidos do órgão fiscalizador;
- Atrasar na correção dos serviços;
- Atrasar na abertura da conta vinculada;
- Atrasar na apresentação da garantia contratual.

2.6.4. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

2.6.5. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

2.6.6. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

2.6.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

2.6.8. A multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

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

2.6.10. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

2.6.11. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicaf serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

2.6.12. Na aplicação das sanções serão considerados:

- A natureza e a gravidade da infração cometida;
- As peculiaridades do caso concreto;
- As circunstâncias agravantes ou atenuantes;
- Os danos que dela provierem para o Contratante; e
- A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013,

serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

- A personalidade jurídica da Contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.
- O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.
- As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.
- Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

3. ESTRATÉGIA PARA A CONTRATAÇÃO

3.1. Natureza do Objeto

Este subtópico tem como objetivo a precisa classificação da natureza jurídica e econômica do objeto da contratação, que consiste na prestação de serviços de Centro de Operações de Segurança (SOC). A correta caracterização é imperativa para a conformidade com a legislação orçamentária e de contratações públicas.

- **Classificação Contábil: Despesas Correntes e/ou Despesas de Capital:**
  - **Despesas Correntes:** O objeto da presente contratação, que envolve o monitoramento contínuo de segurança, detecção e resposta a incidentes, administração de SIEM, inteligência cibernética, testes de invasão e gestão de vulnerabilidades, configura-se predominantemente como **Despesa Corrente**. Tais serviços, por sua natureza, não resultam na aquisição de bens de capital que incorporem o patrimônio do PJAC de forma duradoura, mas sim na manutenção de suas operações e na proteção de ativos existentes.
  - **Despesas de Capital:** Apenas se a contratação envolver a aquisição de equipamentos ou softwares que incorporem o patrimônio do PJAC e possuam vida útil superior a um ano e valor significativo, seria classificada, em parte, como Despesa de Capital. Contudo, no modelo de SOC-as-a-Service proposto, a infraestrutura e as ferramentas são de responsabilidade da Contratada, caracterizando a contratação como serviço e não como aquisição de ativo permanente.
- **Classificação Quanto à Continuidade: Serviços Contínuos ou Não Contínuos:**
  - **Critério de Continuidade:** A caracterização do serviço como contínuo ou não contínuo é balizada pela essencialidade da atividade para a Administração e pela habitualidade de sua prestação. Serviços contínuos são aqueles cuja interrupção possa comprometer a continuidade das atividades essenciais do órgão ou gerar prejuízos significativos à sua operação.
  - **Natureza dos Serviços de SOC:** Os serviços de SOC, por sua intrínseca finalidade de proteção e monitoramento ininterrupto de um ambiente cibernético em constante ameaça, são inequivocamente classificados como **Serviços Contínuos**. A ausência de um SOC ou a interrupção de seus serviços implica

a exposição imediata do PJAC a incidentes de segurança, vazamentos de dados e indisponibilidade de sistemas, impactando diretamente a prestação de serviços judiciais e a imagem institucional. A essencialidade e a habitualidade da necessidade de proteção cibernética justificam plenamente esta classificação.

- **Direitos de Propriedade Intelectual e Autoria:** A definição dos direitos de propriedade intelectual e autoria sobre os produtos gerados durante a execução do contrato é um aspecto crítico para a salvaguarda dos interesses do PJAC, prevenindo o aprisionamento tecnológico (*vendor lock-in*) e garantindo a soberania sobre os dados e o conhecimento produzido.
    - **Princípio Geral:** Salvo justificativa técnica excepcional, todos os produtos gerados ou desenvolvidos especificamente para o PJAC no âmbito da contratação, incluindo, mas não se limitando a:
        - **Documentação:** Relatórios de incidentes, planos de resposta, manuais operacionais, documentação de configurações e arquiteturas customizadas.
        - **Código-Fonte:** Quaisquer scripts, ferramentas auxiliares ou componentes de software desenvolvidos *ad hoc* para a integração ou otimização do SOC com o ambiente do PJAC.
        - **Modelos de Dados e Bases de Dados:** Estruturas de dados, repositórios de *logs*, bases de conhecimento de ameaças e *playbooks* customizados.
    - **Titularidade:** A propriedade intelectual e os direitos autorais sobre os itens mencionados acima deverão ser integralmente do **Poder Judiciário do Estado do Acre**. Isso assegura que o PJAC possa, a qualquer tempo, utilizar, modificar, adaptar ou licenciar esses produtos independentemente da Contratada.
    - **Exceções e Justificativa:** Caso a Contratada alegue direitos exclusivos sobre determinados componentes (e.g., plataformas proprietárias base, tecnologias de SIEM que não sejam Wazuh se usadas como base, ou ferramentas de *Threat Intelligence* de sua titularidade), esta exceção deverá ser **cabalmente justificada** e não poderá, sob nenhuma hipótese, comprometer a capacidade do PJAC de operar, fiscalizar, auditar e, futuramente, transicionar para outra solução ou internalizar a gestão do SOC. A justificativa deverá demonstrar que a exclusividade é inerente à natureza do produto e não impede a plena utilização e o acesso à informação gerada para o PJAC.

3.2. Parcelamento do Objeto e Adjudicação

O objeto da presente contratação foi estruturado em três Grupos distintos, de forma a garantir a especialização das empresas contratadas e assegurar a segregação de funções entre atividades de defesa, ataque controlado e conscientização em segurança da informação.

O parcelamento foi definido considerando os seguintes aspectos:

- **Grupo 1 (Itens 1 a 4) –** Serviços de Monitoramento e Defesa Cibernética (SOC, Blue Team, SIEM, Threat Intelligence e Gestão de Vulnerabilidades): atividades contínuas e integradas de monitoramento, detecção e resposta a incidentes, correlacionadas à gestão proativa de vulnerabilidades e inteligência de ameaças.
- **Grupo 2 (Itens 5 e 6) –** Cultura de Cibersegurança: campanhas educativas, simulações e treinamentos voltados à conscientização dos usuários.
- **Item 7 –** Serviços de Red Team: execução de testes de invasão controlados e independentes, garantindo imparcialidade na validação da eficácia dos controles de segurança.

A opção pelo parcelamento fundamenta-se na necessidade de evitar conflitos de interesse e ineficácia operacional, promovendo a segregação de funções entre as equipes responsáveis pelo Red Team e aquelas dedicadas ao SOC, conforme as melhores práticas de frameworks internacionais de cibersegurança, tais como o NIST Cybersecurity

Framework (CSF) e a ISO/IEC 27001. Essa separação assegura a imparcialidade, eficácia e conformidade legal das atividades de segurança cibernética, além de favorecer maior transparência e robustez na gestão de riscos.

Portanto, o parcelamento em Grupos distintos se mostra tecnicamente viável e economicamente vantajoso, atendendo ao disposto no art. 40, §§ 2º e 3º, e no art. 47, §1º, da Lei nº 14.133/2021.

3.2.1. Cláusula de Segregação de Funções e Conflito de Interesses

Com o objetivo de assegurar a independência técnica, a imparcialidade dos resultados e a conformidade com as boas práticas de segurança da informação preconizadas por frameworks internacionais (tais como NIST CSF e ABNT NBR ISO/IEC 27001), fica vedada a adjudicação simultânea do Grupo 1 (itens de 1 a 4) e Item 7 à mesma empresa ou grupo econômico.

O Grupo 1 refere-se à prestação de serviços de Gerenciamento de Segurança Cibernética (SOC, Blue Team, SIEM, Threat Intelligence e Gestão de Vulnerabilidades), enquanto o Item 7 compreende os Serviços de Testes de Invasão (Red Team).

A execução simultânea dessas atividades por uma mesma empresa configuraria conflito de interesses e risco de ineficácia operacional, uma vez que comprometeria a independência das avaliações e a confiabilidade dos resultados dos testes de segurança.

Essa vedação tem por finalidade garantir a segregação de funções entre as equipes de defesa e ataque controlado, promovendo maior transparência, segurança e conformidade com os princípios da gestão de riscos e com os regulamentos de segurança da informação aplicáveis ao Poder Judiciário.

3.2.2. Adjudicação do Objeto

Cada Grupo e o Item 7 será adjudicado de forma individual, permitindo a contratação de empresas distintas para cada especialidade. Essa medida tem como objetivo assegurar a efetiva segregação de funções, aumentar a competitividade e ampliar a participação de empresas com expertises específicas.

Será vedada a subcontratação dos serviços previstos em cada Grupo, exceto no caso de suporte técnico oficial de fabricantes, quando estritamente necessário. Também não será permitida a participação em consórcio, em conformidade com os arts. 15 e 122 da Lei nº 14.133/2021.

3.3. Modalidade e Tipo de Licitação

A seleção da modalidade e do tipo de licitação é determinada pela natureza do objeto a ser contratado, visando a assegurar a máxima eficiência e a obtenção da proposta mais vantajosa para a Administração Pública, em conformidade com o arcabouço legal vigente.

- **Modalidade:** Para a contratação de serviços de Centro de Operações de Segurança (SOC), que se caracterizam como **serviços comuns**, por possuírem padrões de desempenho e qualidade objetivamente definíveis por meio de especificações usuais de mercado (e.g., Acordos de Nível de Serviço - SLAs, indicadores de desempenho - KPIs, certificações técnicas), a utilização da modalidade **Pregão** é **obrigatória**. Esta imposição está alicerçada no Art. 29 da Lei Federal nº 14.133/2021, que estabelece que o pregão deve ser empregado para a aquisição de bens e contratação de serviços comuns, independentemente do valor estimado. A adoção do Pregão, preferencialmente na forma eletrônica, otimiza o procedimento, garante a ampla competitividade e a celeridade.

- **Tipo de Licitação:** O critério de julgamento para o Pregão será o de **Menor Preço por Grupo e Item**. Esta escolha se justifica pela padronização e objetividade dos serviços de SOC definidos neste ETP, o que permite a comparação direta das propostas com base no valor final ofertado pela solução completa. A definição do menor preço como critério garante que a Administração obtenha o serviço demandado com o menor ônus financeiro, sem comprometer os requisitos de qualidade e desempenho previamente estabelecidos.

3.4. Vigência do contrato

A definição da vigência contratual é um elemento mandatório que estabelece o período de efetiva prestação dos serviços e a duração do vínculo jurídico entre o Contratante e a Contratada. É crucial distinguir a vigência do contrato da duração de eventuais garantias associadas a bens ou serviços específicos.

- **Estabelecimento da Vigência:** A vigência inicial do contrato será de 12 (doze) meses, conforme identificado no Documento de Oficialização da Demanda (DOD) e nos estudos preliminares. Este prazo inicial será estabelecido de forma abrangente para a totalidade dos serviços de SOC.
- **Contrato de Natureza Continuada:** Dada a classificação dos serviços de SOC como de **natureza continuada**, conforme detalhado no subtópico 3.1, o contrato poderá ser prorrogado por períodos sucessivos, até o limite máximo de 60 (sessenta) meses, conforme Art. 107 da Lei Federal nº 14.133/2021, desde que demonstrada a vantajosidade e o interesse da Administração Pública, e mediante apostilamento. Eventuais necessidades de prorrogação além deste limite legal deverão ser devidamente justificadas com base nas exceções previstas na legislação (e.g., serviços de defesa nacional).
- **Distinção Crucial:** Ressalta-se que a **vigência do contrato ou instrumento contratual** não deve ser confundida, nem substituída, pela **vigência da garantia dos bens e serviços** (se houver). Enquanto a vigência do contrato define o período de execução e remuneração dos serviços, a garantia refere-se ao período de responsabilidade da Contratada pela qualidade, desempenho e conformidade dos bens entregues ou dos serviços prestados, podendo estender-se para além do término da vigência contratual.

3.5. Equipe de Apoio à Contratação

Nome	Cargo	Matrícula	Setor
Elielcio Canedo da Silva	Subscretário	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
Amilar Sales Alves	Gestor Substituto	7000980	SUSEG

3.7. Equipe de Fiscalização do Contrato

Nome	Cargo	Matrícula	Setor
Gerson Oliveira da Silva Junior	Fiscal Titular	7002070	DISEG

Jader Sousa Santos	Fiscal Substituto	7001721	DIMEV

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

PODER JUDICIÁRIO
DO ESTADO DO ACRE

R01	**Risco:**	Escopo Mal Definido ou Incompleto no Termo de Referência/Edital (Ausência da descrição da solução como um todo no TR)	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Dificuldade na execução contratual, desalinhamento com as expectativas da área requisitante, necessidade de aditivos onerosos ou, em casos extremos, anulação do processo ou rescisão contratual.	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Equipe de planejamento da contratação inclui no TR ou PB seção destinada a descrever a solução como um todo, explicitando que o objeto da licitação é uma parte desta solução.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Negociar aditivos contratuais para ajustar o escopo e prazos, dentro dos limites legais e com devida justificativa técnica e jurídica.	Gestor do Contrato / Área Jurídica
	2	Em situações de inviabilidade de ajuste, proceder com a anulação do processo ou rescisão contratual, iniciando um novo planejamento se necessário.	Autoridade Competente / Área Jurídica

R02	**Risco:**	Acesso Indevido por Invasor Interno (Falha nas políticas de acesso de funcionários do provedor de nuvem aos ativos)	
	Probab.:	Baixa	
	Impacto:	Muito Baixa	
	Dano 1:	Vazamento de dados sensíveis, comprometimento da segurança e integridade de sistemas, danos reputacionais e sanções regulatórias	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Definir no contrato as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso de seus funcionários aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Equipe de Contratação / Área Jurídica
	Id	**Ação de Contingência**	**Responsável**
	1	Acionar cláusulas contratuais de responsabilidade, aplicar multas e iniciar investigação de segurança/auditoria forense.	Gestor do Contrato / Segurança da Informação

R03	**Risco:**	Acesso Indevido por Invasor Interno (Inadequação na contratação e monitoramento de pessoal do provedor)	
	Probab.:	Baixa	
	Impacto:	Muito Baixa	
	Dano 1:	Exposição a ameaças internas, falhas na proteção de informações críticas e comprometimento da confiança na prestação do serviço	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Definir no contrato as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Equipe de Contratação / Área Jurídica
	Id	**Ação de Contingência**	**Responsável**
	1	Exigir a substituição imediata de pessoal, suspender acessos e aplicar as sanções contratuais cabíveis	Gestor do Contrato

R04	**Risco:**	Discrepância Salarial em Acordos Coletivos (Sem motivação entre salários fixados no edital e CCTs)
	Probab.:	Média

	Impacto:	Médio	
	Dano 1:	Impugnações e questionamentos jurídicos ao edital, risco de futuras ações trabalhistas contra a Administração, e possível desqualificação de propostas.	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Revisar e alinhar os salários fixados no edital com as convenções coletivas de trabalho aplicáveis ou justificar tecnicamente eventuais discrepâncias	Equipe de Planejamento / Área Jurídica
	Id	**Ação de Contingência**	**Responsável**
	1	Publicar errata ou retificação do edital, reabrindo os prazos se necessário para garantir a isonomia.	Pregoeiro / Comissão de Licitação

R05	**Risco:**	Ausência de Informações sobre Situação das Contratações Planejadas	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Desalinhamento orçamentário, atrasos na execução de projetos, interrupção de serviços essenciais devido à falta de recursos ou planejamento inadequado.	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Responsabilizar o gestor pelas aquisições por manter informações atualizadas sobre a disponibilidade orçamentária e financeira, e a situação de cada contratação.	Gestor de Aquisições / Área Financeira
	2	Adotar providências para que grande parte das contratações se inicie no primeiro semestre do exercício corrente, otimizando o fluxo de informações	Gestor de Aquisições / Autoridade Competente
	Id	**Ação de Contingência**	**Responsável**
	1	Negociar aditivos contratuais para ajustar o escopo e prazos, dentro dos limites legais e com devida justificativa técnica e jurídica.	Gestor do Contrato / Área Jurídica
	2	Em situações de inviabilidade de ajuste, proceder com a anulação do processo ou rescisão contratual, iniciando um novo planejamento se necessário.	Autoridade Competente / Área Jurídica

R06	**Risco:**	Emissão de Autorização para Adesões de Não Participantes em Atas Acima do Limite Legal	
	Probab.:	Alta	
	Impacto:	Médio	
	Dano 1:	Ilegalidade na gestão da Ata de Registro de Preços, questionamentos de órgãos de controle e possíveis sanções administrativas ou judiciais	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Garantir o cumprimento rigoroso dos limites individual e global previstos em decreto para adesões ("caronas") em atas de registro de preços	Equipe de Planejamento / Gestor da Ata
	Id	**Ação de Contingência**	**Responsável**
	1	Suspender novas adesões e revisar as já autorizadas, buscando correção ou anulação das que excedem os limites	Gestor da Ata / Área Jurídica
	2	Aplicar medidas corretivas e sanções administrativas aos responsáveis, se houver dolo ou má-fé	Corregedoria / Autoridade Competente

PODER JUDICIÁRIO
DO ESTADO DO ACRE

R07	**Risco:**	Inexistência de Análise de Risco no Planejamento	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Desconsideração de riscos inerentes à contratação e à gestão do contrato, levando a problemas na execução, atrasos, custos extras e falha na obtenção dos resultados esperados	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Obrigatoriedade da equipe de planejamento da contratação em realizar e documentar a análise de risco para a contratação e para a gestão contratual	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Interromper o processo de contratação e realizar imediatamente a análise de risco retrospectiva, identificando e tratando as vulnerabilidades	Autoridade Competente / Equipe de Planejamento
	2	Ajustar o planejamento e o Termo de Referência com base nos riscos identificados	Equipe de Planejamento

R08	**Risco:**	Análise de Risco Deficiente no Planejamento	
	Probab.:	Alta	
	Impacto:	Médio	
	Dano 1:	Desconsideração de riscos relevantes, resultando em falhas operacionais, segurança comprometida ou custos imprevistos durante a execução do contrato	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Implementar um processo de revisão dos artefatos de planejamento, incluindo a análise de riscos, por um servidor sênior ou comitê especializado	Gestor da Área / Unidade de Governança
	Id	**Ação de Contingência**	**Responsável**
	1	Realizar uma reanálise de risco aprofundada, com foco nos pontos críticos e cenários não devidamente explorados	Equipe de Planejamento / Especialistas em Risco
	2	Atualizar o plano de gestão de riscos com as novas medidas preventivas e de contingência	Equipe de Planejamento

R09	**Risco:**	Recebimento de Produtos que Não Atendem aos Requisitos de Qualidade/Desempenho	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Inoperabilidade, baixa qualidade do serviço final, necessidade de retrabalho, prejuízos financeiros e comprometimento da prestação de serviços públicos	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Prever no instrumento convocatório critérios de qualidade e procedimentos de aceitação do produto detalhados e mensuráveis	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Autorizar a especificação de solução paliativa de menor custo para mitigar o impacto imediato	Fiscal do Contrato / Gestor
	2	Aplicar sanções contratuais (multas, advertências) e exigir a substituição ou correção dos produtos não conformes	Fiscal do Contrato / Gestor

R10	**Risco:**	Pessoal em Quantidade ou com Qualificação Inadequada (Para apoio às aquisições e gestão contratual)	
	Probab.:	Alta	
	Impacto:	Alto	
	Dano 1:	Falhas no planejamento e gestão de contratos, sobrecarga de trabalho, erros, descumprimento de prazos e potencial prejuízo à Administração Pública	
	Tratament:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	A alta administração deve prover os papéis que atuam nos processos de contratação e gestão contratual com servidores em quantidade e com qualificação adequadas.	Alta Administração / Gestão de Pessoas
	2	A alta administração pode autorizar a contratação de empresas para apoiar as atividades de gestão (planejamento, coordenação, controle e supervisão), em especial o planejamento e a gestão contratual.	Alta Administração
	Id	**Ação de Contingência**	**Responsável**
	1	Realocar servidores com as qualificações necessárias, priorizando as contratações mais críticas	Gestão de Pessoas / Gestores de Área
	2	Investir emergencialmente em treinamentos e capacitação para suprir as lacunas de conhecimento	Gestão de Pessoas / Área de Capacitação

5. APROVAÇÃO E ASSINATURA

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

Allexandra Macedo de Souza Oliveira
Equipe de Apoio
Integrante Administrativo - Portaria nº 3847/2025/TJAC

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

Documento assinado eletronicamente por **AMILAR SALES ALVES**, **Gerente de Segurança da Informação** em 02/06/2026 às 11:40:29.

Documento assinado eletronicamente por **ELIELCIO CANEDO DA SILVA**, **Técnico Judiciário** em 02/06/2026 às 13:26:57.

Documento assinado eletronicamente por **ALLEXANDRA MACEDO DE SOUZA OLIVEIRA**, **Chefe de Divisão** em 02/06/2026 às 14:56:56.

Documento assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Secretário(a)** em 02/06/2026 às 13:45:15.

Documento assinado eletronicamente por **ANGELO MAXIMO DE MELO SILVA**, em 02/06/2026 às 13:30:29.

PODER JUDICIÁRIO
DO ESTADO DO ACRE

Para conferir a autenticidade do documento, utilize um leitor de QRCode ou acesse o endereço **http://appgrp.tjac.jus.br/grp/acessoexterno/programaAcessoExterno.faces?codigo=670270** e informe a chancela **NUN0.GHJ8.SF2V.ALA8**