PODER JUDICIÁRIO
DO ESTADO DO ACRE

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

TERMO DE REFERÊNCIA Nº 39/2025

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

Processo nº **2025-415**

Fornecer ao Poder Judiciário do Estado do Acre (PJAC) Serviços Especializados de Segurança Cibernética, abrangendo a operação de SOC, Blue e Red 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

TERMO DE REFERÊNCIA Nº 39/2025

1. DO OBJETO:

1.1. Definição do Objeto

1.1.1. A presente contratação tem por objeto 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. Tais serviços, por sua natureza essencial e continuada para a missão institucional do PJAC, serão fornecidos em regime ininterrupto, conforme as especificações e quantitativos detalhados abaixo, com um prazo de vigência inicial de 12 (doze) meses, passível de prorrogação nos termos da legislação aplicável.

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

SERVIÇOS GERENCIADOS DE SEGURANÇA CIBERNÉTICA - ITEM - Red Team						
Red Team						
Item	**DESCRIÇÃO DO BEM OU SERVIÇO**	**CATSER***	**UND**	**Qtd Unitária**	**Valor Unitário**	**Valor Total**
7	Serviços de testes de invasão	27014	Unidade	12		

* Caso haja divergência entre o CATSER e o item apresentando, será considerada a descrição do item.

2. MOTIVAÇÃO:

2.1. O Poder Judiciário do Estado do Acre (PJAC) não dispõe, até o momento, de uma estrutura técnica, operacional ou contratual capaz de desempenhar as funções atribuídas a um Centro de Operações de Segurança (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. Esta ausência representa uma fragilidade crítica no modelo de proteção cibernética da instituição, especialmente considerando o cenário atual de ameaças avançadas, ransomware, vazamentos de dados e ataques de negação de

serviço (DDoS) direcionados a órgãos públicos, em particular 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, tornando a implementação de um SOC, por meio de contratação especializada, essencial para mitigar significativamente os riscos operacionais, institucionais e legais.

2.2. Alinhamento Estratégico

2.2.1. O objeto da contratação está formalmente identificado e contemplado no Plano de Contratações da área de Tecnologia da Informação e Comunicação (PAC SETIC/2026) do Poder Judiciário do Estado do Acre, 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 173 e classificado na Categoria/Grupo 648 - 3.3.90.40.24-SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC.

2.2.2. O objeto da contratação também está alinhado com o Planejamento Estratégico do Poder Judiciário do Estado do Acre, com especial consonância à Perspectiva do Aprendizado e Crescimento, que visa fortalecer a Gestão de TIC, e ao objetivo de definir e executar projetos estratégicos de TIC no TJ, conforme resoluções do CNJ, com a meta de modernizar a estrutura de TI em 70% até 2026. Além disso, encontra consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), que tem o objetivo de detalhar e acompanhar as principais ações e o alcance das metas previstas para os indicadores de TIC do Poder Judiciário do Estado do Acre. Esta contratação atinge o ID da Ação 1, "Ferramentas e soluções que visam fomentar a segurança da informação", da Área Responsável SETIC, conforme Plano de Ações do PDTIC.

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

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

2.2.5. No que tange ao Planejamento Estratégico do Poder Judiciário do Estado do Acre, depreende-se alinhamento quanto ao macro desafio 11. FORTALECER A GESTÃO DE TIC, tendo como meta "-Implantar programas eletrônicos conforme orientações do CNJ", pertinentes ao objeto a ser contratado, especificamente aqueles que endereçam o fortalecimento da gestão de TIC e a modernização da infraestrutura tecnológica.

No que concerne ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), para os anos de 2021/2026, que tem o objetivo de detalhar e acompanhar as principais ações e o alcance das metas previstas para os indicadores de TIC do Poder Judiciário do Estado do Acre esta contratação atinge a ID 5, do Plano de Ações que apresenta a lista de indicadores e metas de TIC previsto para o período de vigência do PDTIC, como:

ID da Ação	Identificação do Dispositivo da Resolução	Descrição da Ação	Procedimentos	Área Responsável no Órgão (Coordenação)
1	Modernização do sistema de segurança da informação (software, ferramentas)	Ferramentas e soluções que visam fomentar a segurança da informação, com vistas a dar cumprimento a Res. 396/2021 e fomentar a maturidade em segurança.	-	SETIC

2.2.6. A solução indicada está alinhada às necessidades de negócio, uma vez que permite a implementação dos controles estabelecidos na Instrução Normativa n° 51/2013 e alterações, que dispõe sobre o uso dos recursos de tecnologia da informação e comunicação do Poder Judiciário do Estado do Acre.

2.2.7. Esta contratação também será orientada, no que couber, pelas orientações e disposições contidas na Lei Geral de Proteção de Dados Pessoais, Lei Federal n° 13.709/2018, de 14 de agosto de 2018.

2.3. Objetivos

2.3.1. A contratação do Centro de Operações de Segurança (SOC) visa alcançar os seguintes objetivos táticos e operacionais:

- Aumentar a visibilidade sobre eventos e atividades críticas no ambiente de TI do PJAC.
- Promover a detecção e resposta em tempo real a incidentes de segurança cibernética, minimizando o tempo de exposição e os impactos.
- Aplicar inteligência contra ameaças avançadas, por meio de análises comportamentais e indicadores de comprometimento (IoCs).
- Apoiar as equipes internas nas tratativas proativas e reativas a incidentes, capacitando e transferindo conhecimento.
- Reduzir os riscos operacionais, institucionais e legais associados à ausência de monitoramento contínuo e capacidade de resposta imediata a incidentes de segurança da informação.
- Fortalecer a conformidade com as diretrizes normativas do Conselho Nacional de Justiça (CNJ) e a Lei Geral de Proteção de Dados (LGPD).

2.4. Referência aos Estudos Técnicos Preliminares

2.4.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) encaminhado pela Subsecretaria de Contratações de TIC (SUCTI) e os Estudos Técnicos Preliminares constantes do Processo Administrativo Eletrônico GRP nº 2025-415.

2.5. Análise de Mercado de TIC

2.5.1. A análise de mercado de TIC foi conduzida com o objetivo de identificar as soluções técnica e funcionalmente viáveis para atender à demanda do PJAC. Esta análise incluiu o cálculo dos custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento.

2.5.2. A memória de cálculo que referencia os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados, está devidamente documentada no Estudo Técnico Preliminar e seus anexos, garantindo a rastreabilidade e auditabilidade dos valores estimados.

2.5.3. Considerando as necessidades e requisitos da demanda, visualizou-se no mercado de TIC diversas alternativas de solução. Dentre elas, destacaram-se:

a) Solução 1: Contratação de empresa especializada com alocação presencial de profissionais no PJAC para operação local do SOC.

b) Solução 2: Contratação de empresa especializada para operação remota 24x7 (modelo SOC-as-a-Service), utilizando a infraestrutura técnica do PJAC e integrando-se à operação.

2.5.4. Para cada solução identificada, foram descritos a aderência técnica à necessidade da demanda, a ponderação econômica, os serviços acessórios necessários, se for o caso, e as contratações em outros entes públicos. A análise comparativa revelou que o modelo SOC-as-a-Service, com prestação remota, oferece a abordagem mais eficiente, econômica e segura para atender às necessidades do PJAC, proporcionando agilidade na implantação, robustez na operação, previsibilidade contratual e alinhamento com as melhores práticas da Administração Pública, aproveitando a infraestrutura de SIEM (Wazuh) já existente no PJAC.

2.5.5. Considerando o modelo de contratação remota do SOC (SOC-as-a-Service) como a solução mais vantajosa, foi efetuada pesquisa de preços fundamentada com o objetivo de identificar contratações similares efetuadas por órgãos públicos federais ou instituições públicas. Assim, foram encontrados os seguintes exemplos cujos extratos estão incluídos no Anexo "Contratações Públicas Similares" dos Estudos Preliminares:

a) Prefeitura Municipal de Vila Velha (PMVV): Processo nº 32524/2024, contratação de serviços de SOC remoto 24x7, modelo SOC-as-a-Service.

b) Empresa Brasileira de Hemoderivados e Biotecnologia (HEMOBRÁS): Processo Administrativo n.º 25800.001168/2023, contratação de SOC remoto 24x7, com infraestrutura local.

c) Poder Judiciário do Estado de Santa Catarina (PJSC): Pregão Eletrônico N. 90005/2024, contratação de SOC como serviço (SOC-as-a-Service), com atendimento 24x7 e alinhamento à Resolução CNJ nº 396/2021 e LGPD.

2.6. Benefícios e Resultados

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:

2.6.1. 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.

2.6.2. 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.

2.6.3. 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.

2.6.4. 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.

2.7. Relação entre a Demanda Prevista e a Contratada

2.7.1. A relação entre a necessidade da contratação da solução de TIC e os respectivos volumes e características está estabelecida na seguinte tabela, que demonstra a demanda prevista em termos de itens de serviço e suas quantidades para o período contratual.

Grupo / Item	Descrição	CATSER	Und	Qtd Unit	Qtd Total
1 / 1	Serviço de Monitoramento, detecção e resposta a incidentes de segurança da informação, por meio de um SOC, Blue Team	27014	Mês	12	12
1 / 2	Administração da solução de SIEM Wazuh, com foco na monitoração e correlação de eventos de segurança	27014	Mês	12	12
1 / 3	Serviços de Monitoramento em fontes abertas e Inteligência cibernética (Threat Intelligence) com Takedown	27014	Mês	12	12
1 / 4	Gestão de vulnerabilidades	27014	Mês	12	12
2 / 5	Ações de Cultura Cibersegurança	27014	Mês	12	12
2 / 6	Plataforma de treinamento de cibersegurança	27014	Mês	12	12
Item 7	Serviços de testes de invasão (Red Team)	27014	Mês	12	12

A forma de cálculo utilizada para a definição do quantitativo baseia-se na necessidade de prestação contínua e mensal dos serviços pelo período de vigência contratual inicial de 12 meses, conforme estimativa do Estudo Técnico Preliminar e a caracterização da demanda.

2.8. Impacto ambiental

2.8.1. Deverá ser informado o impacto ambiental, à luz do Plano de Logística Sustentável (PLS) do Poder Judiciário do Estado do Acre e arcabouço normativo estabelecido no Poder Judiciário, observando-se, inclusive, no que couber, outros normativos vigentes. A Contratada deverá demonstrar compromisso com práticas sustentáveis e apresentar justificativa formal para qualquer inaplicabilidade dos critérios ambientais do PLS.

2.9. Impacto social e cultural

2.9.1. Definir os requisitos em conformidade com costumes, idiomas, práticas para acessibilidade e sustentabilidade, nos termos da Resolução CNJ nº 400/2021, que trata da política de sustentabilidade no âmbito do Poder Judiciário. 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. Além disso, a contratação deverá observar a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) em todos os seus aspectos, dada a natureza sensível dos dados tratados.

2.10. Conformidade Legal

2.10.1. Os procedimentos de segurança da informação e o processamento da informação devem estar em conformidade com as políticas e normas de segurança adotadas pelo Poder Judiciário do Estado do Acre e pelo Poder Judiciário, em destaque:

- Lei Federal n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).
- Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação).
- Resolução CNJ nº 396/2021 (Política de Segurança da Informação do Judiciário).
- Resolução PJAC nº 334/2025 (Política de Segurança da Informação do PJAC).
- ABNT NBR 11515:2007 – Guia de práticas para segurança física no armazenamento de dados.
- ABNT NBR ISO/IEC 27002:2013 – Código de práticas para controles de segurança da informação.
- ABNT NBR ISO/IEC 27017:2016 – Segurança da informação para serviços em nuvem.
- ABNT NBR ISO/IEC 27037:2012 – Preservação de evidências digitais.
- ABNT NBR ISO 27340:2013 – Governança de segurança da informação.
- ABNT NBR 16167:2013 – Classificação e rotulação da informação.
- ABNT NBR ISO 22301:2013 – Gestão de continuidade de negócios.
- ABNT NBR ISO 22313:2015 – Diretrizes para uso da NBR ISO 22301.
- ABNT NBR ISO 27031:2015 – Continuidade da TIC e prontidão para incidentes.
- ABNT NBR ISO 23081-1:2019 – Metadados para documentos de arquivo.

Deverá ser mantida a conformidade com o Processo de Desenvolvimento e Sustentação de Sistemas (PDS), utilizado no Departamento de Tecnologia da Informação e Comunicação (DTI) deste Poder Judiciário do Estado do Acre.

3. DA LICITAÇÃO:

3.1. Da Prestação da Contratação

3.1.1. Contratação de serviços especializados de um Centro de Operações de Segurança (SOC), abrangendo monitoramento contínuo, detecção, análise e resposta a incidentes de segurança da informação, bem como a administração da solução de SIEM (Security Information and Event Management), inteligência cibernética (Threat Intelligence), testes de invasão (Red Team) e gestão de vulnerabilidades. Os serviços serão fornecidos para o Poder Judiciário do Estado do Acre (PJAC) em regime contínuo, conforme as especificações e quantitativos detalhados abaixo, com um prazo de vigência inicial de 12 (doze) meses.

3.2. Da Natureza do Objeto da Contratação

3.2.1. O objeto desta contratação, a prestação de serviços de Centro de Operações de Segurança (SOC), caracteriza-se como **despesa corrente** e, precipuamente, como **serviço contínuo**. A natureza de despesa corrente decorre do fato de que os serviços não resultam na aquisição de bens de capital que se incorporem ao patrimônio do PJAC de forma duradoura. A classificação como serviço contínuo se justifica pela essencialidade e

habitualidade da atividade para a Administração, cuja interrupção comprometeria a segurança da informação, a proteção de dados e a continuidade das atividades essenciais do órgão.

3.3. Do Parcelamento e Adjudicação

O objeto da presente contratação foi estruturado em dois GRUPOS distintos (Grupo 1 - Itens 1 a 4 e Grupo 2 - Itens 5 e 6) e um Item (Item 7), 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 – 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 – 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 e o Item 7 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.

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, **fica vedada a adjudicação simultânea do GRUPO 1 e Item 7 à mesma empresa ou grupo econômico**. 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.

Cada GRUPO e o Item 7 serão adjudicados de forma individual, permitindo a contratação de empresas distintas para cada especialidade. 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.

3.4. Modalidade e Tipo de Licitação

3.4.1. 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 pelo parcelamento do objeto em GRUPOS distintos (Grupo 1 - Itens 1 a 4 e Grupo 2 - Itens 5 e 6) e o Item (Item 7), especialmente pela padronização e objetividade dos serviços de SOC definidos no ETP, o que permite a comparação direta das propostas com base no valor final ofertado por cada GRUPO e o Item 7. A definição do menor preço por GRUPO e Item como critério garante que a Administração obtenha o serviço demandado com o menor ônus financeiro por especialidade, sem comprometer os requisitos de qualidade e desempenho previamente estabelecidos.

3.5. Critérios de Habilitação

3.5.1. Quanto à regularidade e capacidade

a) regularidade perante a Fazenda federal, estadual do domicílio ou sede da licitante, ou outra equivalente e municipal, na forma da lei;

b) regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

c) regularidade perante a Justiça do Trabalho;

d) certidão negativa de feitos sobre falência expedida pelo distribuidor da sede da licitante; e

e) balanço patrimonial e demonstração de resultado de exercício do último exercício social, comprovação de índices relativos à boa situação financeira da licitante (Liquidez Geral, Liquidez Corrente e Solvência Geral) iguais ou maiores que 1 (um). Caso qualquer dos índices esteja inferior a 1(um), será verificada a comprovação de Patrimônio Líquido não inferior a 10% (dez por cento) do valor estimado da contratação;

f) atestado de capacidade técnica, emitido em seu nome, expedido por pessoa jurídica de direito público ou privado, comprovando experiência anterior na execução de serviço semelhante e/ou compatível com o objeto deste termo de referência, qual seja:

f.1) Para o Grupo 1 - comprovação de experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 2000 (dois mil) ativos;

f.2) Para o Grupo 1 - comprovação de experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas em ambientes com, no mínimo, 200 (duzentos) ativos;

f.3) Para o Grupo 1 - comprovação de experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação SIEM, em ambientes com, no mínimo, 200 (duzentos) ativos, 1000 (mil) eventos por segundo (EPS) ou no mínimo volume de eventos de segurança: 100 GB/Dia (podendo ser efetuadas somas de atestados);

f.4) Para o Grupo 2 - comprovação de experiência na prestação de serviços de campanhas educativas, treinamentos em segurança da informação, simulações de phishing, produção de materiais educativos ou programas de conscientização em larga escala.

f.5) Para o Item 7 - comprovação de experiência na prestação de serviço de teste de invasão (PENTEST) para exploração de vulnerabilidades de segurança da informação.

3.5.2. Os documentos exigidos nas alíneas "a", "b", "c" e "d" do item 3.5.1 deste Termo de Referência serão verificados, pelo(a) Pregoeiro(a), em consulta ao Sistema de Cadastramento Unificado de Fornecedores SICAF e/ou em sítios oficiais de órgãos e entidades emissoras de certidões que constituirá meio legal de prova.

3.5.3. O documento exigido na alínea "e" do item 3.5.1 deste Termo de Referência será verificado, pelo(a) Pregoeiro(a), em consulta ao Sistema de Cadastramento Unificado de Fornecedores SICAF que constituirá meio legal de prova.

3.5.4. Os documentos exigidos n a alínea "f" do item 3.5.1 deste Termo de Referencia deverão ser apresentados pela licitante quando solicitados pelo(a) Pregoeiro(a).

3.5.5. Caso os documentos exigidos para atendimento das alíneas "d" e "e" do item 3.5.1 deste Termo de Referência estejam com prazo de validade vencidos e/ou não estejam disponíveis no Sistema de Cadastramento Unificado de Fornecedores SICAF, deverão ser apresentados pela licitante quando solicitados pelo(a) Pregoeiro(a).

3.5.6. O marco temporal para apresentação das demonstrações do último exercício social exigível será a data limite definida pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital ECD ao Sped.

3.5.7. As demonstrações contábeis exigidas limitar-se-ão ao último exercício no caso de a licitante ter sido constituída há menos de 2 (dois) anos.

3.5.7.1. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

3.5.8. A licitante poderá apresentar quantos atestados forem necessários para a comprovação do atendimento quanto à exigência contida na alínea “f” do item 3.5.1 deste Termo de Referência.

3.5.8.1. O(s) atestado(s) apresentado(s) deverá(ão) conter informações que identifique o emitente e a qualidade da execução do objeto contratado.

3.5.9. A comprovação de capacidade técnica estará sujeita à confirmação da veracidade de suas informações por meio de possíveis diligências, conforme prescreve o art. 64, inciso I, da Lei n. 14.133/2021.

3.5.10. Após a apresentação dos documentos de habilitação, fica vedada a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

a) complementação de informações acerca dos documentos já apresentados pelas licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

b) atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

3.5.11. A documentação exigida deverá ter validade mínima até a data prevista para a sessão pública. Se o prazo de validade das certidões não estiver expresso, será considerado o prazo de 90 (noventa) dias corridos, excluindo se nesta contagem o dia da emissão/expedição.

3.5.12. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte, é assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que for declarada vencedora desta licitação, prorrogável por igual período, a critério do Tribunal, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

3.5.12.1. A não regularização da documentação no prazo previsto no subitem anterior implicará na decadência do direito à contratação da microempresa ou empresa de pequeno porte, sem prejuízo das sanções previstas neste Edital e na legislação, sendo facultado ao Tribunal convocar as licitantes remanescentes, na ordem de classificação ou, ainda, revogar esta licitação.

3.5.13. Cópias autenticadas, caso sejam solicitados, deverão ser digitalizados e enviados à Comissão Permanente de Licitações 1, dentro do prazo e e-mail assinalado pelo(a) Pregoeiro(a).

3.5.13.1. Caso o(a) licitante escolha apresentar em meio físico, as cópias poderão ser autenticadas por tabelião de notas, Pregoeiro(a) ou membro da equipe de apoio, mediante apresentação do original ou publicação em órgão da imprensa oficial e ainda por declaração de autenticidade por advogado, junto à Comissão Permanente de Licitações 1, dentro do prazo e local assinalado pelo(a) Pregoeiro(a).

3.5.14. As certidões apresentadas pela licitante, conforme disposição do subitem 3.5.1 deste Termo de Referência, estarão sujeitas à verificação de sua validade e autenticidade pelo(a) Pregoeiro(a) ou membro da equipe de apoio. A verificação pelo Tribunal nos sites oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

3.5.15. A licitante deverá manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

3.5.16. Sob pena de inabilitação, todos os documentos deverão ser apresentados da seguinte forma:

a) se a licitante for a matriz, todos os documentos deverão estar em nome da matriz;

b) em se tratando de filial, os documentos de habilitação jurídica, regularidade fiscal e trabalhista deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos som ente em nome da matriz; e

c) se a licitante for a matriz e a fornecedora do objeto deste Edital ou a emissora da nota fiscal ou documento de cobrança equivalente for a filial, os documentos deverão ser apresentados em nome da matriz e da filial, simultaneamente.

3.5.17. Se a proposta não for aceitável ou se a licitante não atender às exigências habilitatórias, o(a) Pregoeiro(a) examinará a proposta subsequente e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda a este instrumento, quando então poderá negociar diretamente com a proponente para que seja obtido preço melhor.

3.5.18. Se a documentação exigida para habilitação não estiver completa e correta, ou contrariar qualquer dispositivo deste Edital e seus Anexos, ou s e a licitante estiver em suspensão temporária de participação em licitação e impedimento de contratar com a Administração, ou se for identificada como inidônea para licitar ou contratar com a Administração Pública, tal licitante será inabilitada, sem prejuízo das sanções legais cabíveis.

4. DA EXECUÇÃO E GESTÃO DO CONTRATO

4.1. Papéis Desempenhados na contratação

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

a) **Autoridade competente:** Titular da unidade/setor do órgão ou autoridade delegada, responsável pela assinatura do Contrato, Termo de compromisso de manutenção de Sigilo e pela publicação da equipe de fiscalização;

b) **Gestor do Contrato:** servidor com atribuições gerenciais, preferencialmente da Área Demandante da Solução de TIC (STIC), designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

c) **Fiscal Técnico do Contrato:** servidor representante da Área de Tecnologia da Informação e Comunicação, designado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

d) **Fiscal Demandante:** servidor representante da Área Demandante da solução, designado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

e) **Fiscal Administrativo:** servidor representante da Área Administrativa do órgão, designado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes, obrigações. fiscais, previdenciárias e trabalhistas e demais obrigações contratuais. O fiscal administrativo deverá ser designado pela autoridade competente e não poderá ser servidor da área de TIC, salvo em situações excepcionais, devidamente justificada, Resolução CNJ nº 468/2022, artigo 24, §3;

f) **Preposto:** funcionário representante da empresa Contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual; e

g) **Representante da Contratada:** Responsável legal da Contratada para assinatura do contrato, caso tal poder não tenha sido delegado para o preposto.

4.2. Formas de comunicação e acompanhamento da execução do contrato

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

a) Ata de Reunião;
b) Correio eletrônico (e-mail);

c) Ofício;
d) Ordem de Serviço;
e) Sistema de abertura de chamados;
f) Processo administrativo eletrônico do órgão;
g) poderão ser acrescidos outros meios de acompanhamento.>

4.3. Principais marcos e eventos da Execução do contrato

4.3.1. A tabela abaixo foi elaborada com os principais marcos e eventos relevantes que ocorrerão durante a execução do contrato:

Etapa	Descrição	Prazo	Atores	Artefato	Canal
1	Assinatura do contrato	Até o 5º (quinto) dia útil da convocação para a assinatura do contrato	Diretor Geral/Preposto ou Representante da Contratada	Contrato assinado	GRP
	Assinatura do Termo de compromisso de manutenção de Sigilo			Termo de compromisso de manutenção de Sigilo assinado	
2	Publicação da Equipe de Fiscalização	Após a assinatura do contrato	Diretor Geral	Portaria de designação	GRP
3	Reunião de alinhamento	Até o 5º (quinto) dia útil após a assinatura do contrato.	Gestor do Contrato/ Preposto	Ata de reunião de alinhamento	GRP
4	Início da Operação Plena do SOC	Prazo máximo de 15 (quinze) dias úteis a partir da assinatura do instrumento contratual e da emissão da primeira Ordem de Serviço.	Contratada / Gestor do Contrato	Relatório de Implantação e Comprovação de Operação	GRP / Sistema de Chamados
5	Ciclos de Testes de Invasão (Red Team)	A cada 4 (quatro) meses	Contratada / Fiscal Técnico / Equipe de	Relatório Técnico de Pentest	GRP / Sistema de Chamados
6	Entrega de Relatórios Gerenciais Mensais	Até o 5º (quinto) dia útil do mês subsequente ao mês de referência	Contratada / Gestor do Contrato	Relatório Gerencial Consolidado	GRP / E-mail

4.4. Dinâmica da execução

As rotinas de execução, envolvendo prazos, horários, local, documentação mínima exigida, observarão modelos adotados pelo Poder Judiciário do Estado do Acre.

4.4.1. O local de execução do contrato, por se tratar de um modelo SOC-as-a-Service, será prioritariamente **remoto**, a partir da própria central de segurança da Contratada, com acesso e integração à infraestrutura do PJAC. Atendimentos presenciais serão exceções, realizados nas dependências do PJAC, mediante solicitação e em casos específicos que demandem a presença física da equipe.

4.4.2. A execução dos serviços associados ao objeto (Grupo 1) deverá ser prestada em regime **24x7x365 (vinte e quatro horas por dia, sete dias por semana e trezentos e sessenta e cinco dias por ano)** para o monitoramento, detecção e resposta a incidentes de segurança. O horário padrão de trabalho para atendimentos não críticos, quando aplicável, será de segunda a sexta-feira das 07h00 às 14h00, horário do Acre.

4.4.3. A rotina de execução do contrato deverá observar os guias, normativos técnicos, metodologias e melhores práticas internacionais de segurança da informação, como NIST SP 800-61, MITRE ATT&CK, OWASP, ISO/IEC 27001 e ITIL, conforme detalhado nos requisitos técnicos.

4.4.4. O contrato terá vigência de 12 (doze) meses a partir da assinatura do contrato, podendo 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, conforme Art. 107 da Lei nº 14.133/2021.

4.4.5. Capacitação necessária, quando couber, para os servidores do órgão: A Contratada deverá prever a realização de treinamentos e campanhas de conscientização em segurança da informação para os servidores do PJAC, com carga horária e materiais didáticos definidos em conjunto com a Fiscalização do Contrato.

4.4.6. Os procedimentos de segurança da informação e o processamento da informação devem estar em conformidade com as políticas e normas de segurança adotadas pelo Poder Judiciário do Estado do Acre e pelo Poder Judiciário, em destaque: Lei Federal n° 13.709/2018 (LGPD), com a redação dada pela Lei Federal n° 13.853/2019, sobre a proteção de dados pessoais, que altera a Lei Federal n° 12.965/2014 (Marco Civil da Internet); Resolução CNJ nº 396/2021 e o ato normativo do órgão que trata da Política de Segurança da Informação.

4.5. Instrumentos formais de solicitação do objeto

4.5.1. Serão utilizados os seguintes instrumentos formais de solicitação de serviços e acompanhamento de parcelas relevantes do objeto, a exemplo:

a) Ordem de serviço;
b) Chamado eletrônico via sistema ITSM com integração à plataforma do Contratante (ServiceNow);
c) Chamado telefônico via linha 0800;
d) E-mail com domínio registrado e de propriedade da Contratada.

4.6. Instrumentos formais de solicitação do objeto

4.6.1. A produtividade e capacidade mínima de fornecimento da solução de TIC por parte da Contratada serão definidas com base nos Acordos de Nível de Serviço (SLAs) estabelecidos, que quantificam a performance esperada para cada componente do serviço, com base em pesquisas de mercado e as necessidades específicas do PJAC.

4.6.2. Fixam-se os critérios de aceitação dos serviços prestados abrangendo métricas, indicadores e níveis mínimos de serviços com os valores aceitáveis para os principais elementos que compõem a solução de TIC, conforme tabela de SLAs abaixo e demais requisitos técnicos.

4.6.3. Os níveis de serviço exigidos deverão ser propostos conforme preconiza a Instrução Normativa SLTI/MPOG n° 5 de 26/05/2017, e suas atualizações.

N° 01 Índice de atendimento de chamados técnicos de criticidade alta	
Item	**Descrição**
Finalidade	Minimizar os efeitos de indisponibilidade dos equipamentos

Metas a cumprir	Solução definitiva em até 4h para cada chamado técnico
Instrumento de medição	Chamados Técnicos.
Forma de acompanhamento	Relatório Gerencial de Serviço – RGS.
Periodicidade	Mensal.
Mecanismo de Cálculo	Porcentagem de chamados técnicos com solução definitiva em até 4 (quatro) horas.
Início da Vigência	Data de assinatura do contrato.
Faixas de ajustes no pagamento	Igual ou Maior que 98% - 100% da parcela mensal. Entre 95% e menor que 98% - 97,5% da parcela mensal. Entre 90% e menor que 95% - 90% da parcela mensal. Entre 85% e menor que 90% - 70% da parcela mensal. Entre 80% e menor que 85% - 50% da parcela mensal. Menor que 80% - 25% da parcela mensal.
Sanções	Menor que 50% - Multa de 2,5% do valor do contrato para o grupo 1.

Tabela de Níveis de Serviço exigidos para chamados de criticidade alta

Indicador	Descrição	Início Previsto	Disponibilidade	SLA	Periodicidade
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	90%	Mensal
TMA Alta	Tempo Médio de Atendimento (Incidentes que afetem usuários e aplicações críticas, sem ambiente parado)	Até 2 horas após registro do chamado	24x7x365	90%	Mensal
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	90%	Mensal
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 à solução)	Até 8 horas comerciais após registro do chamado	10x5 Horário Comercial (08:00h às 18:00h)	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

4.7. Qualificação Técnica

4.7.1. GRUPO 01 - (Serviços de SOC – Blue Team, SIEM, Threat Intelligence e Gestão de Vulnerabilidades)

4.7.1.1. Para fins de comprovação de capacidade técnica da LICITANTE no âmbito do Grupo 01, considerando a elevada complexidade tecnológica, criticidade operacional e relevância estratégica dos serviços de monitoramento, detecção, resposta a incidentes e gestão contínua de segurança cibernética, a LICITANTE deverá apresentar os seguintes documentos e comprovações:

4.7.1.1.1. Entende-se por pertinente e compatível em características o atestado de capacidade técnica que contemple a execução satisfatória de serviços compatíveis com o objeto do Grupo 01 desta contratação, especialmente relacionados à:

a. operação de Centro de Operações de Segurança (SOC – Security Operations Center);
b. serviços de monitoramento, detecção e resposta a incidentes de segurança da informação;
c. administração e operação de soluções SIEM (Security Information and Event Management);
d. correlação e análise de eventos de segurança;
e. serviços de Threat Intelligence;
f. monitoramento de fontes abertas e análise de ameaças cibernéticas;
g. gestão de vulnerabilidades;
h. análise, tratamento e mitigação de riscos cibernéticos;
i. atividades de Blue Team.

4.7.1.1.2. Entende-se por pertinente e compatível em quantidade o atestado que comprove que a LICITANTE executou ou executa satisfatoriamente serviços compatíveis com o objeto desta contratação, em quantitativo correspondente a, no mínimo, 50% (cinquenta por cento) do quantitativo previsto para cada item do Grupo 01.

4.7.1.1.3. A LICITANTE deverá apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a execução satisfatória de serviços compatíveis com o objeto licitado, contendo, sempre que possível:

a. identificação da contratante;
b. período de execução contratual;
c. descrição detalhada dos serviços executados;
d. quantitativos executados;
e. manifestação expressa quanto à boa execução dos serviços.

4.7.1.1.4. A LICITANTE deverá possuir em sua equipe técnica, na data da apresentação da proposta, no mínimo, 02 (dois) profissionais devidamente certificados nas tecnologias e serviços relacionados ao Grupo 01 com, no

mínimo, 01 (uma) certificação válida para cada profissional.

4.7.1.1.5. Serão aceitas, dentre outras equivalentes e compatíveis com o objeto, certificações reconhecidas pelo mercado nas áreas de:

a. SOC (Security Operations Center);
b. SIEM;
c. Resposta a Incidentes;
d. Threat Intelligence;
e. Gestão de Vulnerabilidades;
f. Segurança da Informação;
g. Cyber Defense;
h. Blue Team.

4.7.1.1.6. Poderão ser aceitas certificações técnicas tais como:

a. Certified Information Systems Security Professional (CISSP);
b. Certified Ethical Hacker (CEH);
c. CompTIA Security+;
d. CompTIA CySA+;
e. GIAC Certified Incident Handler (GCIH);
f. GIAC Security Operations Certified (GSOC);
g. Certified SOC Analyst (CSA);
h. EC-Council Certified Incident Handler (ECIH);
i. ISO/IEC 27001 Lead Implementer ou Lead Auditor;
j. Certificações oficiais do fabricante da solução SIEM ofertada;
k. Certificações oficiais relacionadas às plataformas de monitoramento, correlação de eventos ou gestão de vulnerabilidades ofertadas.

4.7.1.1.7. O vínculo profissional dos integrantes da equipe técnica com a LICITANTE deverá ser comprovado mediante apresentação de um dos seguintes documentos:

a. Cópia da Carteira de Trabalho e Previdência Social (CTPS), acompanhada do registro de empregado;
b. Contrato de prestação de serviços celebrado nos termos da legislação civil;
c. Contrato social, em caso de sócio ou dirigente;
d. Documento equivalente juridicamente válido que demonstre vínculo profissional com a LICITANTE.

4.7.1.1.8. A ausência de documentos comprobatórios das exigências previstas neste instrumento poderá implicar a inabilitação da LICITANTE, observado o disposto na Lei nº 14.133/2021 e nas disposições previstas no edital.

4.7.1.1.9. Durante a análise das propostas, as soluções ofertadas deverão possuir todas as características técnicas obrigatórias constantes no Termo de Referência, não sendo aceitas funcionalidades em desenvolvimento, previstas para versões futuras, roadmap do fabricante ou implementações ainda indisponíveis em ambiente produtivo.

4.7.1.1.10. A Administração, por intermédio do Pregoeiro ou da equipe de apoio, poderá realizar diligências para verificação da autenticidade, veracidade e compatibilidade dos documentos apresentados, inclusive mediante consultas a sítios oficiais, contatos com emitentes dos atestados ou solicitações complementares de esclarecimentos, nos termos da legislação vigente.

4.7.1.1.11. Considerando a natureza crítica dos serviços de cibersegurança envolvidos no Grupo 01, especialmente aqueles relacionados ao monitoramento contínuo de eventos, resposta a incidentes, proteção de ativos institucionais e mitigação de ameaças cibernéticas, a exigência de qualificação técnica e profissional mostra-se necessária e proporcional à complexidade do objeto, nos termos do art. 67 da Lei nº 14.133/2021.

4.7.1.2. Centro de Operações de Segurança (SOC)

4.7.1.2.1. 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.

4.7.1.2.2. Este arranjo deve facilitar a rápida identificação e reação a potenciais ameaças, assegurando uma gestão eficaz de incidentes.

4.7.1.2.3. 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.

4.7.1.2.4. 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.

4.7.1.2.5. 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.

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

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

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

4.7.1.2.9. 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.

4.7.1.2.10. 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.

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

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

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

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

4.7.1.2.15. 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;

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

4.7.1.2.17. 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.

4.7.1.2.18. 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.

4.7.1.2.19. 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.

4.7.1.2.20. 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.

4.7.1.2.21. 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.

4.7.1.2.22. 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.

4.7.1.2.23. 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.

4.7.1.2.24. 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 6 meses de vigência do contrato.

4.7.1.2.25. 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

4.7.2. GRUPO 02 - (Ações de Cultura de Cibersegurança e Plataforma de Treinamento de Cibersegurança)

4.7.2.1. Para fins de comprovação de capacidade técnica da LICITANTE no âmbito do Grupo 02, considerando a natureza especializada, continuada e estratégica dos serviços de cultura de cibersegurança e plataforma de treinamento, a LICITANTE deverá apresentar os seguintes documentos e comprovações:

4.7.2.1.1. Entende-se por pertinente e compatível em características o atestado de capacidade técnica que contemple a execução satisfatória de serviços compatíveis com o objeto do Grupo 02 desta contratação, especialmente relacionados à:

a. execução de ações de cultura de cibersegurança;
b. campanhas de conscientização em segurança da informação;
c. programas de capacitação e treinamento em cibersegurança;
d. fornecimento, implantação, gerenciamento ou subscrição de plataforma de treinamento de cibersegurança;
e. soluções de treinamento com trilhas de aprendizagem, simulações, avaliações ou métricas de conscientização em segurança digital.

4.7.2.1.2. Entende-se por pertinente e compatível em quantidade o atestado que comprove que a LICITANTE executou ou executa satisfatoriamente serviços compatíveis com o objeto desta contratação, em quantitativo correspondente a, no mínimo, 50% (cinquenta por cento) do quantitativo previsto para cada item do Grupo 02.

4.7.2.1.3. A LICITANTE deverá apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a prestação satisfatória dos serviços compatíveis com o objeto licitado, contendo, sempre que possível:

a. identificação da contratante;
b. período de execução;
c. descrição detalhada dos serviços executados;
d. quantitativos executados;
e. manifestação expressa acerca da boa execução contratual.

4.7.2.1.4. A LICITANTE deverá possuir em sua equipe técnica, na data da apresentação da proposta, no mínimo, 01 (um) profissional com, no mínimo, 01 (uma) certificação válida e compatível com as soluções e serviços ofertados no Grupo 02, admitindo-se certificações relacionadas às áreas de:

a. Segurança e Cyber Segurança da Informação;
b. Security Awareness;
c. Gestão de Segurança da Informação;
d. Treinamento e Conscientização em Cibersegurança;
e. Administração ou operação da plataforma ofertada.

4.7.2.1.5. Serão aceitas, dentre outras equivalentes, certificações reconhecidas pelo mercado e aderentes ao objeto, tais como:

a. Certified Information Systems Security Professional (CISSP);
b. Certified Ethical Hacker (CEH);
c. CompTIA Security+;
d. ISO/IEC 27001 Lead Implementer ou Lead Auditor;
e. Information Security Foundation based on ISO IEC 27001
f. Certificações oficiais da área Segurança de TIC;
g. Certificações em plataformas de treinamento e conscientização de usuários em cibersegurança.

4.7.2.1.6. O vínculo profissional dos integrantes da equipe técnica com a LICITANTE deverá ser comprovado mediante apresentação de um dos seguintes documentos:

a. Cópia da Carteira de Trabalho e Previdência Social (CTPS), acompanhada do registro de empregado;
b. Contrato de prestação de serviços celebrado nos termos da legislação civil;
c. Contrato social, em caso de sócio ou dirigente;
d. Documento equivalente juridicamente válido que demonstre vínculo profissional com a LICITANTE.

4.7.2.1.7. A ausência de documentos comprobatórios das exigências previstas neste instrumento poderá implicar a inabilitação da LICITANTE, observado o disposto na Lei nº 14.133/2021 e nas regras de diligência previstas no edital.

4.7.2.1.8. Durante a análise das propostas, a solução ofertada deverá possuir todas as características técnicas obrigatórias constantes no Termo de Referência, não sendo aceitas funcionalidades em desenvolvimento, previstas para versões futuras, roadmap de fabricante ou implementações não disponíveis em ambiente produtivo.

4.7.2.1.9. A Administração, por intermédio do Pregoeiro ou da equipe de apoio, poderá realizar diligências para verificação da autenticidade, veracidade e compatibilidade dos documentos apresentados, inclusive mediante consultas a sítios oficiais, contatos com emitentes dos atestados ou solicitações complementares de esclarecimentos, nos termos da legislação vigente.

4.7.2.1.10. Considerando a criticidade do objeto para a promoção da cultura de segurança institucional e mitigação de riscos cibernéticos, a comprovação de experiência anterior e de qualificação profissional mostra-se indispensável para assegurar a adequada execução contratual, nos termos do art. 67 da Lei nº 14.133/2021.

4.7.3. ITEM 07 - (Serviços de Testes de Invasão – Red Team)

4.7.3.1. Para fins de comprovação de capacidade técnica da LICITANTE quanto à execução dos serviços especializados de testes de invasão (Red Team), considerando a elevada complexidade técnica, criticidade operacional e sensibilidade das atividades relacionadas à identificação controlada de vulnerabilidades e simulação de ataques cibernéticos, a LICITANTE deverá apresentar os seguintes documentos e comprovações:

4.7.3.1.1. Entende-se por pertinente e compatível em características o atestado de capacidade técnica que contemple a execução satisfatória de serviços compatíveis com o objeto deste item, especialmente relacionados à:

a. testes de invasão (Pentest);
b. serviços de Red Team;
c. avaliação de vulnerabilidades;
d. exploração controlada de falhas de segurança;
e. simulação de ataques cibernéticos;
f. testes em aplicações web, redes, APIs, infraestrutura, ambientes híbridos ou em nuvem;
g. análise de segurança ofensiva;
h. elaboração de relatórios técnicos de vulnerabilidades e recomendações de mitigação.

4.7.3.1.2. Entende-se por pertinente e compatível em quantidade o atestado que comprove que a LICITANTE executou ou executa satisfatoriamente serviços compatíveis com o objeto desta contratação, em quantitativo correspondente a, no mínimo, 50% (cinquenta por cento) do quantitativo previsto para o item.

4.7.3.1.3. A LICITANTE deverá apresentar, no mínimo, 01 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando a execução satisfatória de serviços compatíveis com o objeto

licitado, contendo, sempre que possível:

a. identificação da contratante;
b. período de execução contratual;
c. descrição detalhada dos serviços executados;
d. escopo dos testes realizados;
e. quantitativos executados;
f. manifestação expressa quanto à boa execução dos serviços.

4.7.3.1.4. A LICITANTE deverá possuir em sua equipe técnica, na data da apresentação da proposta, no mínimo, 02 (dois) profissionais devidamente certificados em segurança ofensiva, testes de invasão ou Red Team, com certificações válidas e compatíveis com os serviços ofertados.

4.7.3.1.5. Serão aceitas, dentre outras equivalentes e compatíveis com o objeto, certificações reconhecidas pelo mercado nas áreas de:

a. Ethical Hacking;
b. Penetration Testing;
c. Red Team Operations;
d. Offensive Security;
e. Exploração de Vulnerabilidades;
f. Segurança Ofensiva;
g. Application Security;
h. Cybersecurity Offensive Operations.

4.7.3.1.6. Poderão ser aceitas certificações técnicas tais como:

a. Offensive Security Certified Professional (OSCP);
b. Offensive Security Experienced Penetration Tester (OSEP);
c. Certified Ethical Hacker (CEH);
d. GIAC Penetration Tester (GPEN);
e. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);
f. Certified Red Team Professional (CRTP);
g. Certified Red Team Expert (CRTE);
h. eLearnSecurity Junior Penetration Tester (eJPT);
i. eLearnSecurity Certified Professional Penetration Tester (eCPPT);
j. CompTIA PenTest+;
k. Certificações oficiais dos fabricantes das soluções utilizadas, quando aplicável.

4.7.3.1.7. O vínculo profissional dos integrantes da equipe técnica com a LICITANTE deverá ser comprovado mediante apresentação de um dos seguintes documentos:

a. Cópia da Carteira de Trabalho e Previdência Social (CTPS), acompanhada do registro de empregado;
b. Contrato de prestação de serviços celebrado nos termos da legislação civil;
c. Contrato social, em caso de sócio ou dirigente;
d. Documento equivalente juridicamente válido que demonstre vínculo profissional com a LICITANTE.

4.7.3.1.8. A LICITANTE deverá declarar que executará os serviços observando metodologia formal de testes de invasão, boas práticas internacionais e princípios éticos de segurança ofensiva, contemplando, no mínimo:

a. planejamento e definição de escopo;
b. regras de engajamento;
c. execução controlada dos testes;
d. registro de evidências;
e. classificação de criticidade;
f. emissão de relatório técnico conclusivo;
g. recomendações de mitigação das vulnerabilidades identificadas.

4.7.3.1.9. Durante a análise das propostas, as soluções, ferramentas e metodologias ofertadas deverão possuir aderência às melhores práticas de mercado e compatibilidade com os requisitos técnicos previstos no Termo de Referência, não sendo aceitas funcionalidades não implementadas, experimentais ou previstas apenas em versões futuras.

4.7.3.1.10. A ausência de documentos comprobatórios das exigências previstas neste instrumento poderá implicar a inabilitação da LICITANTE, observado o disposto na Lei nº 14.133/2021 e nas disposições previstas no edital.

4.7.3.1.11. A Administração, por intermédio do Pregoeiro ou da equipe de apoio, poderá realizar diligências para verificação da autenticidade, veracidade e compatibilidade dos documentos apresentados, inclusive mediante consultas a sítios oficiais, contatos com emitentes dos atestados ou solicitações complementares de esclarecimentos, nos termos da legislação vigente.

4.7.3.1.12. Considerando a natureza crítica e altamente especializada dos serviços de segurança ofensiva, bem como os riscos inerentes à execução de testes controlados de invasão em ambientes corporativos, a exigência de qualificação técnica e profissional mostra-se necessária e proporcional à complexidade do objeto, nos termos do art. 67 da Lei nº 14.133/2021.

4.8. Forma de recebimento provisório/definitivo e qualidade

4.8.1. O recebimento provisório e definitivo, serão feitos:

a) Estabelecimento de critérios claros para recebimento provisório/definitivo, seguindo a dinâmica da execução contratual e os requisitos técnicos do objeto/parcela do bem/serviço recebido. A aceitação será formalizada após a verificação do cumprimento das entregas e níveis de serviço

4.8.2. A avaliação de qualidade dos serviços será realizada:

a) Por meio de critérios técnicos qualitativos e quantitativos, documentais e padrões de mercado, incluindo a análise dos relatórios gerenciais, indicadores de desempenho (KPIs) e o cumprimento dos SLAs estabelecidos.

4.9. Forma de pagamento

4.9.1. A forma de pagamento será efetuada em função dos resultados obtidos e do cumprimento dos Acordos de Nível de Serviço (SLAs). Será fixado os valores e procedimentos para retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, e serão previstos procedimentos para o pagamento, descontados os valores oriundos da aplicação de eventuais glosas ou sanções.

4.9.2. Cronograma Físico Financeiro

O pagamento será realizado de acordo com a Tabela a seguir:

Grupo	Item	Descrição	Prazo	Custo
1	01	Serviço de Monitoramento, detecção e resposta a incidentes de segurança da informação, por meio de um SOC, Blue Team	Mensal	
	02	Administração da solução de SIEM Wazuh, com foco na monitoração e correlação de eventos de segurança	Mensal	
	03	Serviços de Monitoramento em fontes abertas e Inteligência cibernética (Threat Intelligence) com Takedown	Mensal	
	04	Gestão de vulnerabilidades	Mensal	
2	05	Ações de Cultura Cibersegurança	Mensal	
	06	Plataforma de treinamento de cibersegurança	Mensal	
Item	07	Serviços de testes de invasão (Red Team)	Mensal	
Custo Total Mensal Estimado				
Custo Total Anual Estimado				

4.9.3. Será fixado os valores e procedimentos para retenção ou glosa no pagamento, conforme o desempenho da Contratada em relação aos SLAs e às entregas contratadas.

4.9.4. Estão previstos procedimentos para o pagamento, descontados os valores oriundos da aplicação de eventuais glosas ou sanções.

4.9.5. O pagamento está condicionado ao atendimento das seguintes exigências, a exemplo:

a) Apresentação de nota fiscal, acompanhada de: Certidão Negativa de Débito – CND, comprovando regularidade com o INSS, Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS, Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal, e Certidão Negativa de Débitos Trabalhista – CNDT, expedida pela justiça do Trabalho;
b) Inexistência de fato impeditivo para o qual tenha concorrido.

4.10. Manutenção e Garantia

4.10.1. Serão fixadas as premissas de manutenção, que definem a necessidade de serviços de manutenção preventiva, corretiva, adaptativa e evolutiva (melhoria funcional) da solução de SOC e dos componentes sob responsabilidade da Contratada, especialmente em relação à administração da solução SIEM (Wazuh).

4.10.2. Será estabelecido, para cada item de serviço, considerando as informações previstas, os efeitos no tempo que a contratação deverá ter garantia dos serviços prestados ou dos bens adquiridos, garantindo a continuidade e a qualidade da operação.

4.11. Transferência de Conhecimento

4.11.1. Será prevista a transferência final de conhecimentos sobre a execução e a manutenção da solução de TIC, capacitando a equipe interna do PJAC a assumir a gestão ou a transitar para outro provedor, se necessário. Esta transferência abrangerá a arquitetura, configuração, operação e manutenção de todos os componentes da solução de SOC, e deverá incluir sessões formais de transferência de conhecimento (knowledge transfer) sobre a execução e a manutenção da Solução de TIC, bem como a 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 produzidos.

4.12. Direitos de Propriedade Intelectual e direitos autorais

4.12.1. Deverão ser previstas garantias dos direitos de propriedade intelectual e direitos autorais da Solução de TIC em favor do órgão contratante. A Contratada deve ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre todos os produtos gerados ou desenvolvidos especificamente para o PJAC no âmbito da contratação, incluindo, mas não se limitando a: relatórios de incidentes, planos de resposta, manuais operacionais, documentação de configurações e arquiteturas customizadas, quaisquer scripts, ferramentas auxiliares ou componentes de software desenvolvidos ad hoc, estruturas de dados, repositórios de logs, bases de conhecimento de ameaças e playbooks customizados. Salvo justificativa técnica excepcional e comprovada, todos os direitos sobre esses itens deverão ser integralmente do Poder Judiciário do Estado do Acre. A conformidade com os direitos de propriedade intelectual deve ser assegurada, de acordo com a Lei Federal nº 9.609/1998 e demais legislações aplicáveis.

4.13. Obrigações do Contratante

4.13.1. Prestar, por meio do Gestor do Contrato, as informações e os esclarecimentos pertinentes ao objeta Contratada que venham a ser solicitados pela Contratada, utilizando-se das formas de comunicação estabelecidas neste termo de referência.

4.13.2. Liquidar o empenho e efetuar o pagamento devido nos prazos estipulados em cada etapa da execução e gestão do contrato, desde que cumpridas todas as formalidades e exigências contratuais, bem com as deste Termo de Referência.

4.13.3. Proporcionar os recursos técnicos e logísticos necessários para que a Contratada possa executar os serviços conforme as especificações estabelecidas neste Termo de Referência.

4.13.4. Exercer permanente fiscalização na execução do objeto, registrando ocorrências relacionadas a falhas no cumprimento do contrato, determinando ao preposto ou ao representante da Contratada as medidas necessárias à sua regularização.

4.13.5. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir acesso aos profissionais ou representantes da Contratada às suas dependências com controle e supervisão das áreas técnicas do Poder Judiciário do Estado do Acre.

4.13.6. Aplicar as penalidades previstas no contrato, de acordo com as regras estabelecidas no Termo de Referência, assegurando à contratada o contraditório e a ampla defesa.

4.14. Obrigações do Contratada

4.14.1. Aceitar todos os termos e condições previstas no edital de licitação e seus anexos.

4.14.2. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

4.14.3. Não está prevista subcontratação parcial de outra empresa para a execução do objeto desta contratação, devido características técnicas de agrupamento dos itens que o compõe.

4.14.4. Indicar preposto, e cuidar para que esse mantenha permanente contato com o gestor do contrato na coordenação dos trabalhos concernentes a execução do objeto.

4.14.5. O preposto indicado pela Contratada deverá reportar formal e imediatamente ao gestor do contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do objeto, utilizando-se das formas de comunicação estabelecidas neste termo de referência.

4.14.6. Manter seus profissionais nas dependências do Poder Judiciário do Estado do Acre adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível, de acordo com as regras estabelecidas no ato normativo do órgão.

4.14.7. Seguir as instruções e observações efetuadas pelo gestor do contrato, bem como reparar, corrigir ou substituir às suas expensas, no todo ou em parte, os itens que constituem o objeto quando se verificarem vícios, defeitos ou incorreções.

4.14.8. Responder integralmente por quaisquer perdas ou danos causados ao Poder Judiciário do Estado do Acre ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução do objeto, independentemente de outras cominações contratuais ou legais a que estiver sujeito, conforme preconiza a Lei Federal n° 14.133/2021.

4.14.9. O Representante legal da Contratada deverá assinar Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto do contrato, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, além de outros termos em conformidade com resoluções do CNJ e TJAC.

4.14.10. Todos os profissionais da Contratada diretamente envolvidos na execução contratual deverão assinar Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes.

4.14.11. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados

prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público, sempre que exigido pelo Gestor do Contrato do Poder Judiciário do Estado do Acre.

4.14.12. Caso ocorra a inexecução total do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá restituir integralmente o valor pago antecipadamente pelo contratante. O valor a ser restituído deverá ser atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 201829, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela Equipe de Planejamento da Contratação durante a elaboração deste Termo de Referência). A atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição.

4.14.13. Caso ocorra a inexecução parcial do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá realizar a restituição proporcional dos valores pagos antecipadamente pelo contratante. A restituição proporcional será calculada com base na porcentagem de execução dos serviços previstos no contrato. O valor a ser restituído será atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 2018, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela Equipe de Planejamento da Contratação durante a elaboração deste Termo de Referência). A atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição.

4.14.14. Poderão constar nas contratações de execução continuada ou fornecimento contínuo de bens e serviços deverá ser exigido a prestação de garantia poderá ser de até 5% (cinco por cento) do valor inicial do contrato, autorizada a majoração desse percentual para até 10% (dez por cento), desde que justificada mediante análise da complexidade técnica e dos riscos envolvidos. As modalidades de garantia serão aquelas previstas no art. 96 da Lei Federal n° 14.133/2021.

4.14.15. A Contratada, nas alterações unilaterais a que se refere o inciso I do caput do art. 124 da Lei Federal n° 14.133/2021, fica obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras.

4.15. Estimativa de preços

4.15.1. Com base nas informações de parcelamento do objeto, a estimativa de preços para a contratação dos serviços de SOC é de **R$ 1.840.454,76 (Um milhão, oitocentos e quarenta mil, quatrocentos e cinquenta e quatro reais e setenta e seis centavos),** para o período inicial de 12 (doze) meses. As fontes da pesquisa fundamentada de preços e as palavras-chave usadas para encontrar o valor do orçamento estimado constam detalhadamente no Estudo Técnico Preliminar e seus anexos.

4.16. Adequação orçamentária

4.16.1. A estimativa do impacto no orçamento do órgão foi devidamente realizada, com indicação das fontes de recurso, e a classificação orçamentária será feita com base no manual de classificação orçamentária do SIAFI, conforme abaixo:

I) Programa de Trabalho: 203.617.02.061.2293.2296.0000 - APRIMORAMENTO DAS SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO RES. 396/CNJ/2021 ENSEC-PJ;

II) Fonte de Recursos: 1.760.0700;

III) Elemento de Despesa: 3.3.90.40.21 - SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO.

4.16.2. O orçamento estimado está compatível com as conclusões qualitativas verificadas na análise de custos totais da solução, evidenciando a vantajosidade do modelo SOC-as-a-Service.

4.16.3. Não será permitido pagamento antecipado, parcial ou total, relativo a parcelas contratuais vinculadas ao fornecimento de bens, à execução de obras ou à prestação de serviços, salvo as ressalvas expressas na Lei Federal nº 14.133/2021, Art. 145, as quais indicam que a antecipação de pagamento somente será permitida se propiciar sensível economia de recursos ou se representar condição indispensável para a obtenção do bem ou para a prestação do serviço, hipótese que deverá ser previamente justificada no processo licitatório e expressamente prevista no edital de licitação ou instrumento formal de contratação direta.

4.17. Do Reajuste e da Repactuação

4.17.1. Repactuação

4.17.1.1. Considerando que a execução contratual envolve a prestação de serviços com predominância de mão de obra, os custos referentes a salários, encargos sociais, trabalhistas e previdenciários poderão ser repactuados, observados:

(i) o transcurso do prazo mínimo de 12 (doze) meses contados da data limite para apresentação das propostas ou da última repactuação concedida;
(ii) a comprovação da variação dos custos efetivamente ocorrida, mediante apresentação de documentação pertinente, como convenções ou acordos coletivos de trabalho, dissídios da categoria ou legislações supervenientes;
(iii) a análise e aprovação da Administração quanto à adequação dos novos custos à planilha de custos e formação de preços do contrato.

4.17.2. Reajuste

4.17.2.1. Para os demais itens da planilha de custos que não correspondam a mão de obra direta (tais como insumos, materiais, softwares, equipamentos, despesas administrativas e de infraestrutura), será aplicado o reajuste anual pela variação do Índice de Custo da Tecnologia da Informação – ICTI, calculado e divulgado pela Fundação Getúlio Vargas – FGV.

4.17.2.2. O reajuste será devido após o transcurso de 12 (doze) meses contados da data limite para apresentação da proposta ou da última aplicação do índice, em conformidade com o art. 92, § 4º, da Lei nº 14.133/2021.

4.17.3. Convivência entre os institutos

4.17.13.1. A repactuação e o reajuste poderão coexistir no âmbito deste contrato, aplicando-se cada mecanismo ao respectivo componente de custos, de modo a assegurar a preservação do equilíbrio econômico-financeiro previsto

no art. 37, inciso XXI, da Constituição Federal e nos arts. 89 a 92 da Lei nº 14.133/2021.

4.18. Sanções Administrativas

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

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

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

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

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

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

4.18.5. Na aplicação das sanções serão considerados:

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

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

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

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

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

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

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

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

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

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

4.18.15. A aplicação das sanções previstas nas alíneas "c" e "d" do item 4.18.4 requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará a Licitante ou a Contratada para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

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

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

5. REQUISITOS TÉCNICOS

5.1.1. Detalhamento das características técnicas do objeto

Os requisitos e as características técnicas do objeto, essenciais para a prestação dos serviços de Centro de Operações de Segurança (SOC) para o PJAC, são detalhados a seguir, abordando, no mínimo, aspectos funcionais, arquitetura tecnológica, projeto e implementação, implantação, manutenção e garantia, e procedimentos de recebimento dos objetos contratados.

5.1.1.1. Serviços Gerenciados de Segurança Cibernética (Gerais):

A prestação dos serviços gerenciados de segurança cibernética deverá contemplar componentes integrados, sendo que 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 à CONTRATADA adotar 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. Os atendimentos referentes ao objeto contratado são ilimitados durante o período de vigência, e os atendimentos referentes aos Serviços de Testes de Invasão (Red Team) serão realizados conforme necessidade e indicação da Contratante, respeitando os volumes descritos. Todos os serviços e atendimentos serão prestados remotamente, em regime 24x7. A Contratada deve disponibilizar três tipos de canais de comunicação: Telefone linha telefônica 0800, E-mail com domínio registrado e Portal de Atendimento ITSM. A solução de ITSM da Contratada deverá possuir capacidade de integração com o ServiceNow do Contratante sem ônus adicionais. O CONTRATADO deverá utilizar Centros de Operação de Segurança próprios e designar um Coordenador Técnico.

5.1.1.1.1. Ambiente Computacional a ser Monitorado e Gerenciado: A prestação dos serviços gerenciados de segurança cibernética deverá ser dimensionada para o seguinte ambiente computacional do PJAC:

- **IPs Externos:** 64
- **Aplicações WEB:** 200
- **Domínios:** 1
- **Servidores:** 500
- **Endpoints:** 2000
- **Dispositivos de Rede:** 800
- **Usuários (para Cultura de Cibersegurança e Plataforma de Treinamento):** 2000

5.1.1.2. Para o Grupo 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 o monitoramento de incidentes de segurança em tempo real. O Centro de Operação deve ser situado no Brasil e estar plenamente operacional desde a data de abertura da licitação, com operação contínua. Todos os atendimentos devem ser iniciados no Brasil e no idioma português do Brasil. O SOC deve possuir sistema de

gerenciamento de CFTV com armazenamento de imagens por no mínimo 60 dias, registro de entrada e saída de visitantes, sensor de intrusão e alarmes, vigilância física ininterrupta 24x7x365, controle de acesso físico com pelo menos 2 fatores de autenticação (cartão magnético, biometria, identificação facial), registro de entrada e saída de pessoas por 60 dias, sistemas redundantes para armazenamento de dados e energia (geradores e UPSs), componentes de segurança contra incêndio e plano de recuperação de catástrofes. Não deve possuir campo físico visual externo. Deve possuir ambiente para reproduzir incidentes sem impacto operacional e plano de contingência de atendimento. A CONTRATADA será responsável pelos equipamentos/soluções para estabelecer VPNs entre as partes. O SOC da Contratada deverá ter a certificação ISO/IEC 27001 vigente ou apresentar declaração de estar em fase de implementação com previsão de certificação no primeiro ano de vigência, emitida por empresa certificada.

5.1.1.3. Para o Grupo 1 - Serviço de Monitoramento, Detecção e Resposta a Incidentes de Segurança da Informação (Blue Team): A Contratada deverá disponibilizar, por meio de seu SOC, infraestrutura, ferramentas e equipe especializada para o monitoramento e resposta a incidentes dos ativos de segurança do Contratante, em regime 24x7x365, com atendimento remoto e presencial em casos excepcionais. Os serviços contemplam: triagem e primeiro atendimento de chamados, detalhamento e encaminhamento de eventos, notificação e registro de incidentes, validação e execução de instruções de trabalho, alinhamento do ambiente aos procedimentos operacionais do Contratante, análise de histórico de eventos, implementação de gestão de indicadores de qualidade, utilização de metodologias ágeis, apoio em ataques (preparação, mitigação, contenção, defesa, resposta), proposição de regras para SIEM, sugestão de *playbooks* e *runbooks*, pessoal qualificado e suficiente, passagem de turno com *follow-ups*, suporte à automação de atividades, acompanhamento de SLAs, priorização de atendimentos críticos, monitoramento contínuo de produtos de segurança do Contratante, provimento de relatórios técnicos/gerenciais, elaboração de plano de execução, elaboração de plano de contingência e continuidade de negócios, apoio em processos de resposta a incidentes, criação de salas de crise, elaboração de dossiês detalhados, realização de auditorias, apoio a órgãos de controle e utilização de ferramentas.

5.1.1.4. Para o Grupo 1 - Takedown / Serviço de Remoção de Conteúdo Malicioso: O serviço deverá possuir funcionalidade de 5 *Takedowns* por ano, com tela para solicitação (URL, Empresa, Prioridade, Categoria), feedback para ocorrências fechadas, visualização de *takedowns* solicitados, painel de gerenciamento com total e ordenação por data/prioridade, filtros de busca (Empresa, Status, Categoria, Período, Responsável), e dashboard com quantidade, status, tempo médio de mudança de status. A plataforma deve possuir recurso de *takedown* automatizado para perfis de redes sociais (Instagram, Facebook, TikTok), páginas de hospedagem (Hostgator) e compartilhamento de documentos (Scribd).

5.1.1.5. Para o Grupo 1 - Administração da Solução de SIEM (Wazuh): A Contratada será responsável pela sustentação, operação, administração e evolução da solução de SIEM da Contratante (Wazuh), garantindo sua correta operação, disponibilidade e evolução contínua, de acordo com as melhores práticas de mercado. Destacam-se: gestão dos agentes (instalação, atualização, *troubleshooting*, monitoramento), criação, customização e manutenção de *Decoders* e *Rules*, aplicação de melhores práticas, análises periódicas de eficiência das regras, apoio à investigação e resposta a incidentes, geração de *dashboards* e relatórios, apoio em *upgrades* e atualizações, integração com serviço de diretório (Active Directory), customização para coleta de *logs* de firewalls, antivírus, IDSs, Proxy, DNS, etc., coleta e armazenamento sem normalização no momento da coleta, integração com ITSM, customização de plataforma de acesso web, ajuste e desenvolvimento da lógica de detecção, contextualização e enriquecimento de dados, configuração de Backup & Restore, suporte a armazenamento em camadas (HOT, WARM, COLD), suporte a filtros na camada de rede e aplicação, análise e correlação de *logs*, utilização de agentes para coleta de dados, módulos para coleta em *endpoint* e rede, detecção por análise de *logs*, acesso restrito à equipe de segurança do Contratante e equipe do SOC da Contratada, configuração proativa de regras de correlacionamento (rootkits, não conformidades, vulnerabilidades, integridade de arquivos, análise

comportamental, padrões de *logs*, *whitelisting*), parametrizações, customizações e manutenções na plataforma, e atividades de evolução do SIEM. A infraestrutura necessária para a operação do Wazuh será disponibilizada pelo Contratante.

5.1.1.6. Para o Grupo 1 - 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 atenda: operação para 5 usuários simultâneos, operação 24x7 pela Contratada, plataforma em nuvem (SaaS) com acesso web, interface em português, inglês e espanhol, compatibilidade com navegadores web modernos, eventos coletados permanecem disponíveis por tempo indeterminado, integração com MISP, armazenamento de logs de acesso de usuários por no mínimo 1 ano, base de pelo menos 6 bilhões de eventos e 20 milhões de atores maliciosos monitorados, logs de acesso detalhados, painel de visualização com perfis por palavras-chave, buscas avançadas, navegação por clicks, apresentação de dados por fontes, exportação de relatórios (XLSX, JSON, CSV, DOCX, PDF), pós-processamento de eventos (OCR, transcrição, detecção de linguagem, extração de metadados), detecção automática com IA (credenciais vazadas), busca por intervalo de data, metadados, fontes, palavras-chave, interface web com proximidade, fuzzy, lógica binária, regex, operadores lógicos, ordenação de resultados, salvar e gerenciar buscas, identificação de links patrocinados, perfis falsos, campanhas *zeroday*, phishing, *defacement*, comercialização ilegal de vulnerabilidades, acompanhamento de discussões de risco, identificação de certificados/domínios monitorados, consulta Whois automática, processamento de URLs para phishing com IA, guardar preview de sites de phishing e download de código fonte, *drill-down* de pesquisas, dashboard de análise (quantidade por termo, tipo de dado, perfis, fontes, grupos), busca de perfis por nome/apelido/telefone/e-mail, painel de buscas salvas, criação/alteração/exclusão de variáveis, notificação de eventos para outros usuários, associação de múltiplos eventos a ocorrências, campo de descrição em ocorrências (com imagens), upload de anexos, notificação de ocorrências via e-mail e WebHook, painel de gerenciamento de ocorrências, adição de IOCs, histórico de alterações, classificação por categorias/criticidade/times, comentários ilimitados, filtros por organização/empresa/período, relatórios periódicos do fabricante (7/semana, 2 mil na base), relatórios em português, inglês, espanhol, informações pertinentes (IOCs, anexos, IPs), download em PDF (cifrado para confidencial), captura automatizada de informações de diversas fontes da internet (mídias sociais, mensageria, buscadores, e-commerce, apps, chans, fóruns, repositórios, indexadores de malware, paste services, feed de domínios, vulnerabilidades, rede, defacement, blogs de *ransomware*, outros), direcionamento de coletas com robôs configuráveis, configuração de Google-Dorks, monitoramento de grupos de Ransomware (30 mil eventos, dashboard), autenticação multifator (MFA), suporte a SSO (Azure, OKTA), gerenciamento de usuários (login, senha, ativação/desativação, grupos, times), permissões granulares (RBAC), configuração de alertas (email, Webhook, SMS, Tickets, WhatsApp) baseados em consultas, CPF vazado, VIPs, credenciais de domínios, pesquisa de credenciais de usuários expostas (7 bilhões na base), dashboard de vulnerabilidades (CVEs, relatórios, eventos, pesquisa textual, severidade, data).

5.1.1.7. Plataforma de Gestão de Vulnerabilidades: A solução deve permitir a descoberta, avaliação, priorização e correção de vulnerabilidades em toda a infraestrutura (estações, servidores, dispositivos de rede, telecomunicações, segurança, hipervisores, VMs, contêineres, nuvem). Gestão centralizada via interface web única. Licenciada por IP ou HOST, com descoberta e inventário ilimitados (agentes, scanners, sensores passivos) sem custos adicionais. Inventário contínuo (ativos conhecidos e desconhecidos), coleta automatizada e detalhada de informações (serviços, softwares, usuários, portas, SO, hostname, IP, MAC, processador, memória, disco, BIOS). Classificação automática por família tecnológica, tipo, plataforma e fabricante. Normalização automática de nomes de fabricantes. Etiquetagem de ativos (estática/manual, palavras-chave, IP, segmento de rede, portas, CVE, scriptlet, Regex). Avaliação contínua de vulnerabilidades com múltiplos sensores. Motor de escaneamento com 99,99966% de precisão. Base de conhecimento atualizada semanalmente (mínimo 20 CVEs/semana), com 35.000 CVEs históricos/atuais. Cobertura para Windows, UNIX, LINUX, MacOS, Cisco, VMware, bancos de dados (MS SQL, MySQL, Oracle), plataformas web (IIS, Apache), serviços/aplicações (TCP, UDP, Adobe, Apple, HP, McAfee,

Microsoft, Oracle). Escaneamentos de vulnerabilidades (SO, serviços web, portas TCP/UDP, serviços, aplicações, bancos). Alternativas de escaneamento: ativo não autenticado, autenticado, agente. Motor de cálculo de risco multifatorial (CVSS, ECM, tendência de exploração, atores, CISA Known Exploitable, configuração, controles compensatórios, certificados, obsolescência). Cálculo dinâmico. Priorização de remediação. Detecção de patches ausentes e mapeamento CVE. Avaliação de configurações baseada em CIS Benchmarks (fabricante com certificação oficial). Identificação de configurações incorretas. Avaliação de certificados digitais e configurações TLS. Renovação de certificados. Fluxos de trabalho automatizados (drag and drop). Descoberta e inventário automático de aplicações web e APIs (crawling, testes dinâmicos, OWASP Top 10, varredura autenticada, IA/ML, OWASP API Top 10, detecção PII, detecção malware). Geração de score de criticidade (CVSS, CISA Known Exploitable, ECM). Fluxo de trabalho de remediação baseado em políticas (criação, atribuição, estados: aberto/fechado/ignorado). Criação automática de tickets. Implantação de patches via agente (Windows, Linux, Mac, aplicações corporativas). Notificações ao usuário final (adiamento, contagem regressiva). Reinício automático de host. Download de patches (repositório local ou internet). Criação de jobs para patching. Ações prévias/posteriores a jobs. Seleção de múltiplos patches sem custos adicionais. Limitação da janela de tempo. Dashboards de estado de patches.

5.1.1.8. Para o Grupo 2 - Conscientização, Educação e Treinamento em Segurança da Informação: Deve promover a conscientização contínua dos usuários internos do PJAC quanto às boas práticas de segurança da informação, proteção de dados pessoais, prevenção a incidentes e conformidade normativa. Todo o conteúdo deverá ser previamente revisado e validado pelo PJAC e ser compatível com diversos canais de distribuição. Os direitos de uso e propriedade intelectual de todo o material produzido deverão ser integralmente cedidos ao PJAC. A Contratada deverá apresentar relatórios das atividades (alcance, participação, efetividade), com registro de *feedbacks*, lições aprendidas e sugestões de melhorias. Deverá propor atualizações de políticas. Realizar e propor no mínimo 4 (quatro) vezes ao ano, palestras remotas de 4 horas sobre engenharia social, e no mínimo 4 (quatro) vezes ao ano, treinamentos e conscientização. O escopo inclui elaboração e execução de campanhas educativas, produção de materiais educativos (cartilhas, vídeos, infográficos, banners, *newsletters*), realização de eventos temáticos, *webinars* ou oficinas práticas trimestrais, e condução de simulações práticas de incidentes e testes de comportamento (phishing, análise de resposta, relatórios comportamentais, *quizzes* e avaliações de aprendizado com *dashboards* de engajamento).

5.1.1.9. Para o Item 7 - 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. Os testes poderão ser executados na modalidade híbrida por profissionais identificados, certificados e capacitados. Deverão incluir elaboração e apresentação de relatórios detalhados contendo métodos, técnicas, ferramentas, avaliação, diagnóstico e recomendações. Os testes não poderão impactar o funcionamento dos recursos testados sem autorização prévia. Serão realizados a cada 4 meses, com alvo e tipo de Pentest acordados. Caso a Contratante entenda risco, poderá solicitar mudança de metodologia e/ou cronograma. Os testes seguirão padrões internacionais (MITRE ATT&CK, OWASP, NIST SP 800-115, PTES, Red Team Engagement Framework). O escopo inclui: planejamento (RoE, escopo, horários), testes de invasão em infraestrutura interna/externa, aplicações web/APIs/dispositivos, engenharia social simulada, movimentação lateral, evasão de controles, mapeamento/exploração de vulnerabilidades, avaliação de controles de segurança (capacidade de detecção Blue Team), relatório técnico detalhado (descrição, evidências, riscos, vetores, recomendações). Obrigações da Contratada: profissionais qualificados e certificados, testes em ambiente seguro, sigilo/confidencialidade, relatórios em português.

5.1.1.10. Requisitos de Arquitetura Tecnológica (Configuração - Ambiente Contratante): Para a execução das atividades presenciais previstas, a CONTRATANTE se compromete a disponibilizar ambiente físico adequado em suas dependências, incluindo mobiliário básico, equipamentos de informática (computadores, monitores,

Videowall, periféricos), acesso à rede local e à internet (condicionado às políticas internas), e credenciais de acesso aos sistemas e ferramentas do Contratante (conforme perfil e função). O uso da infraestrutura disponibilizada deverá respeitar as normas internas do Contratante, especialmente no que se refere à política de uso de ativos, confidencialidade e segurança da informação.

5.1.1.11. Requisitos de Manutenção (Serviços): A empresa contratada deverá prestar serviços de monitoramento e acionamento do CONTRATANTE em caso de vazamento de dados. Exemplos de atividades: elaboração de relatórios de inteligência sobre ameaças de interesse, criação de alertas na plataforma, criação de buscas pré-configuradas para potenciais ameaças, realização de suporte técnico em conjunto com o fabricante, elaboração de relatório mensal consolidado de tickets. O ambiente computacional a ser analisado abrange: 64 IPs externos, 200 Aplicações WEB, 1 Domínio, 500 Servidores, 2000 EndPoints, 800 Dispositivos de rede.

5.1.1.12. 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, responsável por atuar como canal de comunicação, acompanhamento contínuo da qualidade e dos SLAs. A equipe deverá atuar proativamente na identificação de oportunidades de melhoria. As responsabilidades incluem: suporte e acompanhamento periódico do contrato, acompanhamento de indicadores da operação, reunião mensal de resultados, análise e acompanhamento de prazos e incidentes, geração de relatório de KPIs, geração de relatório mensal sumarizado (status, ocorrências, ações) e acompanhamento dos serviços nas revisões dos SLAs. Os profissionais deverão ter formação acadêmica de nível superior, preferencialmente em Gestão da Qualidade, e no mínimo 1 (um) ano de experiência profissional.

5.1.1.13. Acordo de Nível de Serviços – SLA: Conforme tabela apresentada no item 4.6.

5.1.1.14. Ferramentas para a Prestação do Serviço: 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 o uso de técnicas e ferramentas mais atualizadas, simulando ataque real. Para análise de vulnerabilidades, a Contratada deverá utilizar ferramenta que atenda: base de dados atualizada, avaliação de riscos com CVSS, apresentação de formas de resolução/mitigação, utilização de identificadores CVE. As ferramentas devem suportar armazenamento seguro de credenciais para varreduras autenticadas. O processo de varredura deve ter impacto mínimo sobre a rede. Ferramentas de análise de vulnerabilidades web deverão: detectar OWASP TOP 10, realizar escaneamento ativo/passivo, realizar *crawling/spidering*. A utilização de ferramentas não deve integralizar a atuação do analista, sendo apenas auxiliares.

5.1.1.15. Requisitos de Projeto e de Implementação:

Este subtópico define as metodologias, processos e artefatos esperados para o desenvolvimento, execução e entrega dos serviços, garantindo uma abordagem sistemática e auditável. As fases e os requisitos são mandatórios:

- **Fase de Planejamento (Planejamento do Exercício):** Definição clara e mensurável de objetivos, processos e atividades permitidas/proibidas, informações e acessos necessários (especialmente Graybox e Whitebox).
- **Fase de Descoberta (Reconhecimento e Levantamento):** Coleta abrangente de informações (incluindo atuação manual), técnicas e ferramentas de coleta passiva.
- **Fase de Exploração (Simulação de Ataques):** Validação e confirmação de vulnerabilidades, avaliação de impactos, simulações de ataques reais e controlados, utilização de metodologias reconhecidas (OWASP Testing Guide), preservação da operação, aplicação de ataques baseados em Aplicação Web (SQL Injection, XSS, etc.), Rede e Protocolos (TCP, SNMP), e Aplicações Modernas (CSRF, SSRF, IDOR).

- **Fase de Relatório (Documentação e Recomendações):** Elaboração de relatório técnico detalhado contendo: identificação do projeto (escopo, tipo, modalidade), referências metodológicas, cronologia das atividades, visibilidade do ambiente, confirmação de vulnerabilidades, descrição abrangente das vulnerabilidades (nome, nível de risco/criticidade, indicação de exploração intrusiva, descrição detalhada, documentação do fabricante, melhores práticas, link para patch, CVE, total detectado, evidências, avaliação de riscos/impactos, contramedidas), e assinatura técnica do profissional responsável.

5.1.1.16. Requisitos de Experiência e Formação da Equipe: Conforme detalhado no item 4.7. A Contratada deverá comprovar que seus profissionais possuem conhecimento aprofundado e proficiência no manuseio das ferramentas e tecnologias utilizadas pelo Contratante, em particular a plataforma SIEM em uso (Wazuh).

5.1.1.17. Requisitos de Segurança da Informação: A Contratada deverá formalizar seu comprometimento com a confidencialidade, integridade e proteção dos dados e informações institucionais do PJAC. Qualquer incidente de segurança deverá ser comunicado imediatamente. A Prestadora de Serviços deverá assinar um Termo de Sigilo e Confidencialidade, e todos os profissionais envolvidos assinarão Termos de Confidencialidade individuais. A Contratada observará rigorosamente os normativos internos do PJAC, a LGPD (Lei nº 13.709/2018) e a Resolução CNJ nº 396/2021. O compromisso de sigilo será irrevogável e permanecerá vigente mesmo após o encerramento do contrato. Recursos técnicos utilizados na prestação dos serviços deverão estar em conformidade com os regulamentos de segurança do PJAC, incluindo uso de métodos seguros de acesso remoto (canais criptografados, MFA, VPN).

5.1.1.18. Requisitos Sociais, Ambientais e Culturais: A Contratada deverá demonstrar compromisso com a observância de preceitos sociais, ambientais e culturais. A solução e os serviços deverão estar em estrita conformidade com a legislação vigente, os normativos institucionais (PLS do PJAC, Resolução CNJ nº 400/2021) e as melhores práticas aplicáveis. A adequação da solução e dos serviços à cultura organizacional e funcional do Poder Judiciário, garantindo a interoperabilidade humana e sistêmica sem fricções indevidas, priorizando o idioma Português do Brasil. Além disso, a solução ou seus componentes que envolvam troca de informações com outros sistemas governamentais, bases de dados externas ou plataformas de gestão judicial, deverão ser compatíveis com as diretrizes do Modelo Nacional de Interoperabilidade (MNI), Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) para autenticação e assinatura digital, e Modelo de Requisitos MoReq-Jus para a gestão de documentos e registros eletrônicos gerados pelo SOC. A atuação deverá estar alinhada com LGPD, ISO/IEC 27001, Resolução CNJ nº 396/2021 e TPADM TJAC nº 291/2023.

5.1.1.19. Requisitos Legais: Conforme detalhado no item 2.10. O cumprimento de todos esses dispositivos será condição indispensável para a regular execução contratual, sendo passível de fiscalização e sanções administrativas em caso de descumprimento.

6. REQUISITOS FUNCIONAIS

6.1. 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 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano).

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:

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.2. Centro de Operações de Segurança (SOC) - Grupo 1 - Item 1

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.

6.2.1. 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:

6.2.1.1. 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.

6.2.1.2. 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:

6.2.1.3. 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 pela

6.3. Administração da Solução de SIEM - Grupo 1 - Item 2

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.

6.3.1. 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.

6.4. Serviços de Monitoramento em Fontes Abertas e Inteligência Cibernética (Threat Intelligence) - Grupo 1 - Item 3

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;

6.5. Takedown / Serviço de Remoção de Conteúdo Malicioso - Grupo 1 - Item 3

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.

6.6. Plataforma de Gestão de Vulnerabilidades - Grupo 1 - item 4

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.

6.7. Serviços de Testes de Invasão (RED TEAM) - Item 7

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.

6.7.1. 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.

6.7.1.1. 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.

6.8. 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;

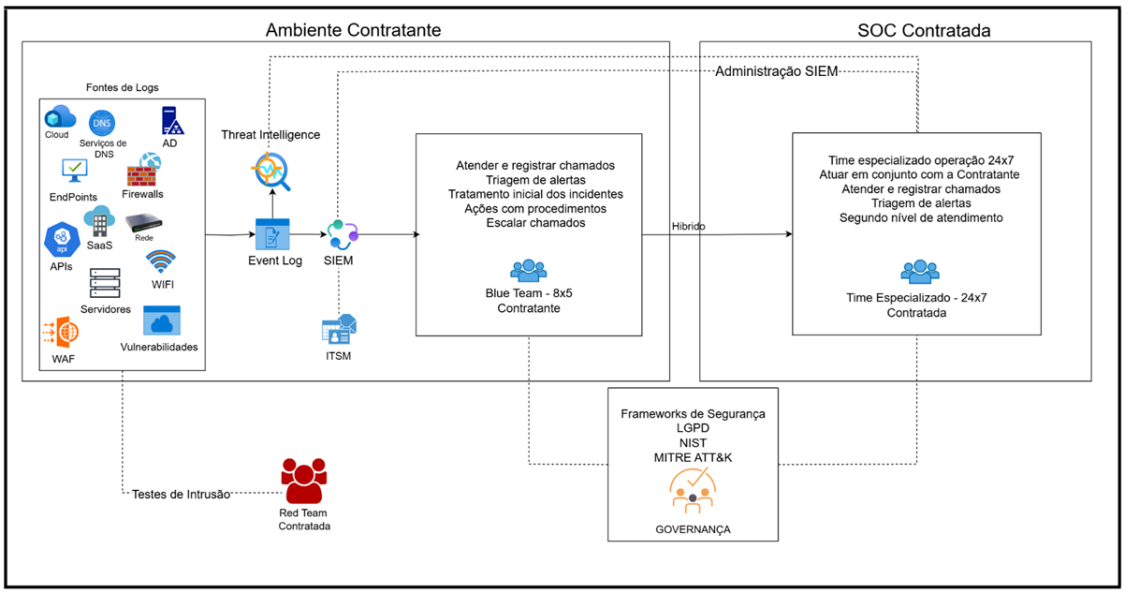
Mobiliário básico como mesas, cadeiras e armários, conforme a necessidade das atividades;

Equipamentos de informática, tais como computadores, monitores, VideoWall 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.



6.9. 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.

6.10. 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

6.10.1. 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.

6.10.2. Acordo de Nível de Serviços – SLA para SOC e Blue Team/Siem/Threat Intelligence/Gestão De Vulnerabilidade - Grupo 1

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

6.10.3. 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.

6.11. 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.

6.12. 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.

6.13. 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.

6.14. 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.

6.15. 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.

7. ASSINATURAS

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

8. APROVAÇÃO

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

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

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

Eliélcio Canedo da Silva
Subsecretário de Contratações de TIC

PODER JUDICIÁRIO
DO ESTADO DO ACRE

Integrante Técnico - Portaria nº 3847/2025/TJAC

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

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

Documento assinado eletronicamente por **AMILAR SALES ALVES**, **Gerente de Segurança da Informação** em 02/06/2026 às 11:40:37.

Documento assinado eletronicamente por **ALLEXANDRA MACEDO DE SOUZA OLIVEIRA**, **Chefe de Divisão** em 02/06/2026 às 14:57:13.

Documento assinado eletronicamente por **ANGELO MAXIMO DE MELO SILVA**, em 02/06/2026 às 13:30:36.

Documento assinado eletronicamente por **ELIELCIO CANEDO DA SILVA**, **Técnico Judiciário** em 02/06/2026 às 13:27:03.

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 **9NL7.0DBD.HRKG.4AQL**