Poder Judiciário

Tribunal de Justiça do Estado do Espírito Santo

Secretaria de Tecnologia da Informação

ESTUDO TÉCNICO PRELIMINAR (ETP) - TIC

Contratação de Serviços Gerenciados de Segurança da Informação com Central de Operações de Segurança (Security Operations Center - SOC)

SUMÁRIO

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

A transformação digital do Poder Judiciário impôs ao TJES uma dependência crescente de serviços digitais contínuos e confiáveis para assegurar a prestação jurisdicional, a integridade dos dados e a transparência perante a sociedade. O Programa de Modernização do Poder Judiciário do Estado do Espírito Santo (PROMOJUES), instituído pela Resolução PJES nº 006/2023, consolida esse direcionamento estratégico ao explicitar a necessidade de incremento de governança, eficiência e segurança da informação, em consonância com a Estratégia Nacional de Tecnologia da Informação e Comunicação do

Poder Judiciário (ENTIC-JUD), prevista na Resolução CNJ nº 370/2021, e com a linha de financiamento do BID destinada à modernização do sistema de justiça e segurança. Nesse contexto, a proteção cibernética torna-se requisito estruturante para a continuidade dos serviços judiciais e para a proteção de dados pessoais sob guarda institucional.

Observa-se, ademais, o crescimento do número de ataques direcionados a Tribunais de Justiça no país. Somado ao avanço da migração de ativos e serviços para ambientes de nuvem, esse cenário reforça que o principal ativo do Tribunal é a informação. A busca permanente de aderência à Lei Geral de Proteção de Dados e a proteção de ativos e dados institucionais constituem condição indispensável para a continuidade e a confiabilidade dos serviços digitais disponibilizados à sociedade, o que exige capacidade de monitoramento, resposta e melhoria contínua compatível com o nível de risco atual.

No plano nacional, destaca-se a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ nº 396/2021. Tal estratégia explicita objetivos e pilares para elevar a maturidade cibernética dos órgãos do Judiciário, contemplando governança, fortalecimento de infraestruturas críticas, instituição de equipes de resposta a incidentes e arranjos de cooperação. A adoção de serviços de SOC guarda aderência direta a essas diretrizes, pois viabiliza monitoramento contínuo, gestão de vulnerabilidades, resposta coordenada e geração de evidências para governança e accountability.

No plano interno, o Tribunal possui Política de Segurança da Informação (PSI) formalmente instituída pela Resolução PJES nº 06/2018, com diretrizes e responsabilidades atribuídas à Secretaria de Tecnologia da Informação (STI) para implementar controles tecnológicos, analisar e tratar incidentes e sustentar a melhoria contínua do sistema de gestão de segurança. A despeito desse arcabouço, a intensidade e a sofisticação dos incidentes exigem capacidade operacional contínua, processos padronizados, telemetria abrangente e mecanismos de correlação e resposta em tempo oportuno, sob pena de indisponibilidade de sistemas críticos, comprometimento da confidencialidade e perda de evidências para responsabilização e prestação de contas.

Para organizar o tratamento e a resposta a incidentes, o TJES instituiu a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR-TJES) por meio do Ato Normativo PJES nº 124/2024, com atribuições de receber e classificar alertas, responder a incidentes, analisar artefatos maliciosos, tratar vulnerabilidades e identificar tendências. Trata-se de passo institucional relevante. Contudo, por natureza e composição,

a ETIR demanda estrutura tecnológica e serviços especializados que potencializem sua atuação, com monitoramento contínuo, orquestração de respostas, geração de alertas acionáveis e relatórios gerenciais que permitam decisões baseadas em risco e evidências.

O PROMOJUES prevê, como entregas específicas, a implementação de política e soluções de cibersegurança, incluindo gestão de vulnerabilidades, proteção avançada, controle de acessos privilegiados, realização periódica de testes de intrusão e, de modo expresso, a contratação e a instalação de Centro de Operações em Segurança (SOC). Esse conjunto de produtos revela que a elevação da maturidade cibernética é objetivo programático do Tribunal e que a implantação de serviços SOC é o meio adequado para alcançar resultados mensuráveis em disponibilidade, integridade, confidencialidade e continuidade de negócios.

Diante desse cenário, identificam-se os seguintes problemas a serem resolvidos, com impacto direto no interesse público: i) risco de interrupções ou degradação de desempenho em sistemas judiciais eletrônicos, com prejuízo à razoável duração do processo e à continuidade da prestação jurisdicional; ii) exposição a incidentes não detectados ou tardiamente detectados, com potenciais violações de dados pessoais e sanções regulatórias; iii) ausência de monitoramento unificado e de correlação de eventos de segurança em toda a superfície tecnológica; iv) capacidade limitada para investigação, resposta e lições aprendidas em escala compatível com o volume e a criticidade dos serviços; v) necessidade de apoiar a ETIR com telemetria, automação e playbooks, de modo a ampliar a efetividade da resposta e reduzir tempos de detecção e recuperação; vi) necessidade de evidências e trilhas de auditoria que sustentem governança, responsabilização e transparência do programa de segurança. Essas lacunas, persistentes, contrariam o desenho institucional da PSI e podem pressionar negativamente os resultados estratégicos do PROMOJUES.

A solução a ser contratada deverá aprimorar os sistemas de segurança já existentes e fortalecer a atuação do quadro técnico do Tribunal. Espera-se que viabilize capacidades atualmente insuficientes, tais como monitoramento contínuo vinte e quatro horas por dia, sete dias por semana, gestão sistemática de vulnerabilidades, detecção precoce e resposta coordenada a incidentes, uso de inteligência de ameaças, execução periódica de testes de intrusão, geração de evidências para auditoria e conformidade com a Lei Geral de Proteção de Dados, além de mecanismos de transferência de conhecimento e suporte especializado para elevar o nível de maturidade em segurança cibernética. A análise das alternativas possíveis deverá considerar critérios de cobertura, integração com a infraestrutura

tecnológica existente, níveis de serviço pactuados e mensuráveis, custo total de propriedade e aderência às diretrizes da ENTIC-JUD, da ENSEC-PJ e da PSI.

Por fim, a adoção do SOC se harmoniza com a governança do PROMOJUES. A resolução instituidora determina a gestão de riscos, o acompanhamento sistemático da execução e a prestação de contas dos resultados. Ao prover métricas, indicadores e evidências de segurança, a solução favorece o controle gerencial, a transparência e a responsabilização, além de reduzir o risco de paralisações e perdas de dados que possam comprometer a confiança da sociedade e dos usuários do serviço de justiça.

Em síntese, a necessidade de implantação de SOC decorre de imperativos estratégicos e operacionais já reconhecidos no PROMOJUES e na PSI institucional, da instituição da ETIR-TJES e do aumento do risco cibernético no setor público. A contratação é medida necessária e proporcional para assegurar a continuidade do serviço jurisdicional, a proteção de dados e a conformidade com as diretrizes institucionais e nacionais aplicáveis.

1.1.1. Análise do Cenário Atual

O panorama atual evidencia um aumento significativo na sofisticação e agressividade dos ataques cibernéticos contra instituições públicas, em especial os Tribunais de Justiça. Entre novembro de 2020 e abril de 2022, foram registrados 13 (treze) ataques direcionados a tribunais brasileiros, fato que demonstra a vulnerabilidade do ecossistema judicial e o risco potencial de interrupção de serviços essenciais.

Segundo dados nacionais do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), houve crescimento consistente nos incidentes reportados nos últimos anos. O volume de notificações recebidas pelo órgão, que em 2019 girava em torno de 875 mil registros, alcançou em 2020 a marca de 1,4 milhão e, em 2021, ultrapassou 1,9 milhão de notificações. Em 2022, apesar da ligeira redução, o patamar manteve-se elevado, ainda acima de 1,5 milhão de incidentes reportados. Esse cenário revela a permanência de ameaças em escala massiva, exigindo atuação contínua e preventiva.

A análise por tipologia demonstra que ataques por *phishing* representam parcela expressiva, com números superiores a 400 mil registros anuais desde 2020, configurando um dos principais vetores de fraude e comprometimento de credenciais. Os escaneamentos de rede aparecem em volume igualmente elevado, superando 300 mil notificações anuais, o

que evidencia tentativas sistemáticas de mapeamento de vulnerabilidades em ambientes institucionais. Também se registram números relevantes de invasões bem-sucedidas e de negação de serviço (DoS/DDoS), os quais comprometem diretamente a disponibilidade dos sistemas.

Outro dado preocupante refere-se à crescente complexidade dos ataques. Não apenas houve aumento do número absoluto de incidentes, mas também da variedade e sofisticação, com combinação de técnicas como spear phishing, ransomware, uso de credenciais comprometidas e exploração automatizada de falhas críticas. Isso demonstra que a ameaça deixou de ser episódica e passou a se configurar como risco estrutural, capaz de afetar diretamente a continuidade da prestação jurisdicional.

No caso do TJES, a infraestrutura tecnológica conta com ativos de segurança básicos, como firewalls e antivírus corporativos, mas tais ferramentas, isoladamente, não se mostram suficientes diante do cenário descrito. A evolução dos métodos de ataque exige monitoramento contínuo, inteligência de ameaças, correlação de eventos e resposta coordenada, recursos que atualmente não são plenamente executados de forma estruturada.

Além disso, a equipe técnica da STI encontra-se sobrecarregada pela multiplicidade de funções, que incluem gestão contratual, fiscalização de fornecedores, suporte técnico, elaboração de termos de referência e atendimento a incidentes de rotina. Esse acúmulo compromete a capacidade de atuação proativa em segurança cibernética, exigindo uma estrutura especializada que amplie a vigilância, a capacidade de correlação de eventos e a orquestração de respostas.

Em síntese, os dados estatísticos nacionais e a análise local apontam para um cenário de risco crescente, no qual os ataques cibernéticos tornaram-se mais frequentes, complexos e impactantes, enquanto os recursos internos permanecem aquém da demanda. Este contexto reforça a urgência de dotar o TJES de mecanismos especializados que ampliem sua capacidade de prevenção, monitoramento, resposta e recuperação, garantindo a continuidade e a confiabilidade dos serviços digitais disponibilizados à sociedade.

1.2. Identificação da demanda no Plano de Contratações de STIC

O projeto não figurou no Plano de Contratações da STIC. Está previsto no PROMOJUES.

1.2.1. Identificação das Necessidades do Negócio

A solução em análise encontra respaldo em diversos instrumentos de planejamento, normas e políticas públicas que orientam a atuação do Poder Judiciário e, em especial, o Tribunal de Justiça do Espírito Santo. Todos convergem para a necessidade de fortalecer a governança de TIC, proteger dados pessoais e assegurar a continuidade dos serviços digitais essenciais.

Na esfera institucional, o Planejamento Estratégico do TJES (2021-2026), aprovado pela Resolução nº 12/2021, prevê objetivos diretamente relacionados à governança tecnológica, à segurança da informação e à gestão de dados. Entre eles destacam-se: *AC.12.01 Aperfeiçoar a governança e a gestão de TIC*, *AC.12.02 Aprimorar a segurança da informação e a gestão de dados e AC.12.02.002 Implantar e gerenciar o atendimento à LGPD*. A implantação de serviços especializados de monitoramento e resposta, como o SOC, é uma forma de materializar esses compromissos, garantindo que os sistemas de informação do TJES operem com confiabilidade, rastreabilidade e níveis de segurança compatíveis com o grau de criticidade dos serviços judiciais.

No âmbito normativo nacional, a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ nº 370/2021, estabeleceu diretrizes claras para a modernização tecnológica dos tribunais, incluindo como eixo fundamental o *aprimoramento da segurança da informação e da gestão de dados.* A contratação de um SOC contribui para esse objetivo, elevando a maturidade institucional medida pelo iGovTIC-JUD e alinhando o TJES aos parâmetros nacionais de governança em TIC. De forma complementar, a *ENSEC-PJ*, reforça a necessidade de criação de mecanismos permanentes de monitoramento, detecção e resposta a incidentes, diretriz que se ajusta integralmente à implantação de uma estrutura SOC.

No contexto organizacional do próprio Tribunal, o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2021-2026, revisado em 2025) atualizou prioridades e reafirmou a centralidade da segurança cibernética para a consecução dos objetivos estratégicos. O documento identifica a importância da gestão de riscos tecnológicos, da continuidade de negócios e do fortalecimento da proteção de dados. A solução em estudo é, portanto, um elo natural entre o que o PDTIC projeta como necessidade e o que o Planejamento Estratégico e a ENTIC-JUD demandam em nível macro.

Em termos de obrigações legais e atribuições internas, a PSI atribui expressamente à STI o dever de implementar controles, tratar incidentes e garantir a melhoria contínua da segurança da informação. Esse papel ganhou novo fôlego com a reestruturação da STI em 2025, que criou a Coordenação de Infraestrutura de Operações e a Seção de Segurança da Informação, unidades responsáveis por prover grande parte da gestão técnica associada ao SOC, como a integração com sistemas já existentes, o acompanhamento dos serviços contratados e a análise dos relatórios gerados. Assim, a contratação se insere em uma estrutura organizacional já redesenhada para sustentar a governança e operacionalização desses serviços.

Por outro lado, não se pode ignorar os compromissos assumidos no PROMOJUES. Entre as entregas previstas no programa, estão expressamente contempladas a gestão de vulnerabilidades, a proteção avançada de estações, a realização periódica de testes de intrusão e a implantação de um Centro de Operações em Segurança. A futura contratação, portanto, encontra-se não apenas em sintonia com as metas estratégicas, mas também programaticamente prevista no escopo do PROMOJUES e vinculada ao Contrato de Empréstimo BID nº 5883/OC-BR.

Finalmente, há ainda o alinhamento com obrigações legais externas que recaem sobre o Tribunal, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que exige a adoção de medidas técnicas e administrativas adequadas para proteger dados pessoais, e a Lei nº 11.419/2006, que dispõe sobre a informatização do processo judicial, impondo requisitos de autenticidade, integridade e disponibilidade dos sistemas. Ambos os diplomas encontram respaldo na solução aqui considerada, uma vez que um SOC é capaz de monitorar acessos, detectar violações, produzir trilhas de auditoria e reduzir riscos de indisponibilidade.

Em conclusão, a análise demonstra que a solução buscada se articula de forma plena com o Planejamento Estratégico do TJES, a ENTIC-JUD, a ENSEC-PJ, o PDTIC 2021-2026, a PSI institucional, a estrutura organizacional da STI, o PROMOJUES e a legislação aplicável (LGPD e Lei 11.419/2006). O conjunto desses instrumentos revela que o fortalecimento da segurança cibernética é não apenas uma escolha de gestão, mas um imperativo institucional e jurídico para assegurar a continuidade dos serviços, a proteção dos dados e a confiança da sociedade no ecossistema digital da Justiça capixaba.

1.3. Caracterização da Demanda

1.3.1. Descrição da Solução

A solução consiste na contratação de Serviços Gerenciados de Segurança da Informação, que incluem atividades de monitoramento, detecção, análise e resposta de incidentes cibernéticos, incluindo gestão de vulnerabilidades, gerenciamento de patches, administração e supervisão de ferramentas de segurança (em modelo SaaS), testes de intrusão e simulações de ataques, dentre outros itens relacionados à segurança da informação, conforme exigências estabelecidas neste documento.

Considerando os aspectos técnicos, a complexidade do ambiente de TI do TJES e a natureza dos serviços, optou-se por agrupar os itens da contratação. Tal agrupamento é justificado pelos seguintes fatores:

a. É um modelo amplamente utilizado em contratações de objeto análogo no setor público;
b. Simplifica as atividades de gestão, fiscalização e controle do contrato;
c. Minimiza potenciais conflitos que poderiam surgir entre diferentes prestadores de serviços.; e
d. Favorece o atingimento de melhores níveis de desempenho devido à continuidade e coesão dos serviços executados.

A solução de Serviços Gerenciados de Segurança da Informação inclui os seguintes itens:

Torre de serviços 01 - Purple Team - Atendimento de requisições	
Item	**Descrição**
1	**Serviço de Administração, Operação, Manutenção e Atendimento de Requisições**, para garantir o correto funcionamento das ferramentas de coleta de *logs* das demais ferramentas de segurança, bem como promover a interação rotineira com toda a equipe de segurança da informação do TJES para que, de forma provocativa, a estimule a realizar as customizações e configurações necessárias para a integração destas ferramentas com o Serviço de Monitoramento e Correlacionamento – SIEM, descrito no **Item 3**. Isso será alcançado através da realização permanente de ações proativas voltadas para a segurança do

	parque computacional do TJES com o objetivo de mantê-lo estável, disponível e íntegro. Por meio da "Análise de Lacunas" (*gap analysis*), serão realizados diagnósticos e estabelecidas as diferenças entre o nível de desempenho da infraestrutura atual e o nível de desempenho desejado, identificando e desenvolvendo planos para colmatar a lacuna existente entre os dois níveis, com o objetivo de abordar quaisquer deficiências ou áreas de melhoria, a fim de aumentar o desempenho geral e atingir as metas e objetivos desejados.
Torre de serviços 02 - Blue Team - Gestão de incidentes de segurança e monitoramento de ataques cibernéticos	
Item	**Descrição**
2	**Serviço de gestão de vulnerabilidades**, que tem por objetivo, de forma proativa e recorrente, identificar, avaliar e priorizar possíveis vulnerabilidades de segurança da informação no ambiente e sistemas críticos do TJES a fim de evitar que ataques obtenham sucesso explorando vulnerabilidades conhecidas, reduzindo o risco de violação de segurança, bem como gerenciar a aplicação dos *patches* e atualizações conforme necessário. Esse serviço visa possibilitar a identificação e solução rápida das vulnerabilidades antes que elas possam ser exploradas por agentes mal-intencionados.
3	**Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança**, que realiza o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TJES, através de correlacionamento de *logs*, pacotes de redes e comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, que devem ser analisados, podendo ser transformados em um incidente de segurança da informação, conforme definido na **Política de Gestão de Incidentes**. O **Serviço de gestão de incidentes de segurança**, por sua vez, objetiva identificar, analisar, remediar, conter e documentar eventos de segurança da informação que forem transformados em um incidente de segurança da informação, de forma a promover a mais rápida resposta e

	recuperação do ambiente, obedecendo os principais *frameworks* e as boas práticas de mercado, incluindo: ● Time de Resposta a Incidentes (Computer Security Incident Response Team – CSIRT); ● Gerenciamento de Eventos e Informações de Segurança (Security Information and Event Management – SIEM);
4	**Gerenciamento da Orquestração e Automação de Resposta a incidentes (*Security Orchestration, Automation and Response* – SOAR)**, referindo-se às tecnologias que permitem às organizações coletarem entradas monitoradas pela equipe de operações de segurança. Por exemplo, alertas do sistema SIEM e outras tecnologias de segurança — onde a análise e triagem de incidentes podem ser realizadas aproveitando uma combinação de poder humano e de máquina — ajudam a definir, priorizar e conduzir atividades padronizadas de resposta a incidentes. As ferramentas SOAR permitem que uma organização defina a análise de incidentes e os procedimentos de resposta em um formato de fluxo de trabalho digital.
5	**Gerenciamento de Proteção Contra Riscos Digitais (*Digital Risk Protection* – DRP),** que tem o objetivo de mapear e prevenir a exfiltração de dados confidenciais através de vazamentos de dados provocados ou acidentais, a partir da análise *Deep* e *Dark Web*, das diversas redes sociais e demais repositórios desse tipo de informação.
6	**Gerenciamento de Patches (Patch Management)** O serviço de Gestão de Patches tem como objetivo assegurar que todos os sistemas, aplicações e dispositivos do ambiente de Tecnologia da Informação e Comunicação (TIC) do TJES estejam devidamente atualizados com os patches de segurança e correções mais recentes, visando mitigar vulnerabilidades e proteger contra explorações por parte de agentes maliciosos.

No que tange aos Testes de Invasão, a solução proposta será composta pelos serviços distribuídos da seguinte forma:

Torre de serviços 03 - Red Team - Serviço de Testes de invasão (também conhecidos como Pentests ou Testes de Intrusão), tem como objetivo principal: identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Dando visibilidade aos problemas, explorando estas falhas em busca de entender sobre a sua origem e, por fim, sugerir correções.	
Item	Descrição
1	***Gray Box* (Caixa Cinza) –** modalidade em que a CONTRATADA possui informações parciais, fornecidas pelo CONTRATANTE, para subsidiar a estratégia de invasão.
2	***Black Box* (Caixa Preta) –** a tentativa de invasão é feita sem nenhum conhecimento prévio do ambiente testado.

1.3.2 Definições Complementares

Para facilitar a compreensão, é possível explicar os termos com base em definições usuais no mercado de segurança da informação:

- **Equipe Azul (Blue Team – Defesa):** grupo responsável por proteger os ativos digitais da organização contra ataques. Sua atuação concentra-se em monitorar sistemas, identificar tentativas de invasão e responder a incidentes, adotando medidas que aumentem a resiliência e assegurem a continuidade dos serviços.
- **Equipe Vermelha (Red Team – Ataque):** grupo que desempenha o papel de um adversário, realizando simulações de ataques cibernéticos contra a organização. Seu objetivo é explorar vulnerabilidades, testando os mecanismos de defesa para revelar falhas que poderiam ser exploradas em um ataque real.
- **Equipe Roxa (Purple Team – Integração):** grupo que atua como elo entre as Equipes Azul e Vermelha. Sua função é promover a cooperação e a troca de informações entre quem defende e quem ataca, transformando os resultados dos testes ofensivos em melhorias práticas para a defesa. Dessa forma, contribui para elevar de forma contínua a maturidade da organização em segurança cibernética.

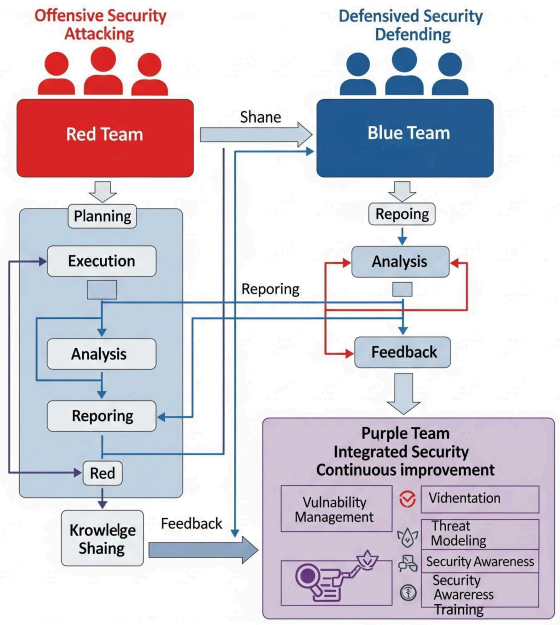

Figura 1: Ilustração da atuação dos times

1.3.3 Requisitos necessários e suficientes à escolha da solução de TIC

Todos os itens/objetos da contratação deverão observar os requisitos mínimos relacionados à manutenção, operação e suporte dos serviços de Segurança da Informação, quais sejam:

- Prover monitoramento contínuo (24x7x365) de todos os ativos críticos do Tribunal, com geração de alertas em tempo real e registros auditáveis.
- Disponibilizar equipe técnica especializada em segurança cibernética, com experiência comprovada em resposta a incidentes, análise forense e gestão de vulnerabilidades.
- Disponibilizar time multidisciplinar capaz de correlacionar eventos de diferentes fontes (rede, sistemas, endpoints, aplicações em nuvem) e propor medidas de mitigação adequadas.
- Demonstrar a capacidade técnica dos profissionais designados por meio da apresentação de certificações reconhecidas no mercado, tais como CISSP, CISM, CEH, CompTIA Security+, GIAC, ou equivalentes, quando aplicável.
- Prover serviços de inteligência cibernética (threat intelligence), incluindo análise de tendências de ataques, indicadores de comprometimento e compartilhamento de informações relevantes.

- Emitir relatórios periódicos de conformidade, auditoria e segurança, com indicadores de desempenho (KPIs) e de qualidade do serviço (SLAs), alinhados às boas práticas internacionais.
- Fornecer mensalmente ou sempre que demandado a base de dados com todos os registros, tratativas e demais informações relacionados a chamados, contendo todas as informações que possam identificar corretamente a demanda, contendo, no mínimo:
    i. Número/ID do chamado
    ii. Data e hora de abertura
    iii. Nome do solicitante
    iv. Contato do solicitante
    v. Responsável pelo atendimento
    vi. Categoria/tipo do chamado
    vii. Descrição do problema ou solicitação
    viii. Localização (se aplicável)
    ix. Prioridade/urgência
    x. Status atual
    xi. Histórico de interações
    xii. Data e hora de encerramento
- Prover suporte técnico para orientação e esclarecimentos relacionados a arquitetura de segurança, políticas de proteção de dados, resposta a incidentes e continuidade de negócios.
- Disponibilizar infraestrutura tecnológica compatível com as necessidades do SOC, incluindo sistemas de gestão de eventos e informações de segurança (SIEM), orquestração e automação de resposta a incidentes (SOAR) e ferramentas de análise de vulnerabilidades.
- Garantir que todos os serviços prestados sejam executados em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), com a Política de Segurança da Informação do TJES e demais normas aplicáveis.

1.3.4 Requisitos de Arquitetura Tecnológica

Independentemente da torre de serviços contratada, todas as soluções e ferramentas empregadas na execução deverão observar os seguintes requisitos:

- As ferramentas deverão ser de propriedade da CONTRATADA, devidamente licenciadas em seu nome, não sendo admitida a utilização de softwares livres, open-source ou desenvolvidos internamente (in-house).
- Deverá fornecer ao CONTRATANTE, sempre que solicitado, acesso de leitura às consoles de gerenciamento utilizadas, para fins de auditoria dos serviços prestados, durante toda a vigência do contrato.
- A prestação deverá ocorrer por meio de solução hospedada em nuvem do fabricante ou em ambiente de nuvem da própria CONTRATADA.
- A nuvem em que as soluções serão hospedadas deverá estar situada, no mínimo, em data center classificado como TIER 3, garantindo alta disponibilidade, redundância e tolerância a falhas.
- Os softwares ofertados deverão ser entregues em sua versão mais estável e atualizada, devidamente cobertos por contratos de suporte e atualização de versões junto ao fabricante durante todo o período de vigência do serviço. Da mesma forma, os equipamentos eventualmente fornecidos deverão estar cobertos por contratos de garantia do fabricante;
- O atendimento aos requisitos definidos para cada serviço poderá ser realizado de forma integrada, mediante composição com outros equipamentos ou softwares utilizados em diferentes itens, desde que não haja alteração na topologia da rede nem exposição de ativos a riscos de segurança da informação, especialmente quanto à integridade, confidencialidade e disponibilidade.

1.3.4.1 Portal de Indicadores de Serviço

A CONTRATADA deverá prover um sistema, no modelo SaaS (*software as a service*), denominado portal de indicadores, destinado à consolidação das informações provenientes das soluções que compõem o objeto contratual.

Esse portal deverá ser disponibilizado ao TJES com, no mínimo, as seguintes funcionalidades:

I. O portal deverá estar acessível a CONTRATANTE via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSLv1.2 ou superior;

II. Possibilidade de criação ilimitada de usuários, com atribuição de perfis distintos e níveis de acesso diferenciados, conforme a necessidade do TJES.

III. Alteração personalizada das visualizações gráficas pelos usuários, permitindo a troca entre diferentes formatos de acordo com a preferência individual, não existindo vinculação entre os usuários.

IV. O portal deverá disponibilizar, no mínimo, a opção de visualização nos seguintes modelos gráficos para os usuários:

   a. Gráfico do tipo Pizza;
   b. Gráfico do tipo Barra;
   c. Gráfico do tipo Área.

V. **Indicadores de risco (KRI)**: O portal de indicadores deverá exibir as vulnerabilidades encontradas nas auditorias mais recentes, com recurso de “drill down” para detalhamento por tipo e criticidade, além da possibilidade de filtragem que exclua vulnerabilidades de menor relevância (baixa ou média).

VI. **Indicadores de metas e desempenho (KGI e KPI)**: O portal de indicadores deverá possuir relatório gráfico indicando o tempo médio de tratamento de incidentes em cada fase (análise, contenção, erradicação e recuperação), com filtros por períodos (exemplo: últimos 15, 30 ou 45 dias) e comparativos entre incidentes recentes e anteriores. Deverá ainda:

   a. Possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando uma linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio;
   b. Oferecer a possibilidade de consulta deste gráfico para cada uma das fases de atendimento (Análise, contenção, erradicação e recuperação);

VII. **Indicadores por Categoria**: O portal de indicadores deverá disponibilizar gráficos que permitam a classificação e a visualização dos incidentes de acordo com as categorias previstas no processo de resposta a incidentes. No mínimo, deverão ser contempladas as seguintes classificações:

   a. Origem do incidente;
   b. Status do incidente;
   c. Prioridade do incidente;
   d. Nível de risco;
   e. Grupo de atendimento responsável.

VIII. Todos os indicadores disponibilizados pelo portal deverão contar com a funcionalidade de drill down, permitindo que os usuários detalhem informações, criem visualizações específicas e apliquem filtros sobre os dados apresentados.

IX. Cada indicador exibido deverá oferecer, adicionalmente, a possibilidade de exibição em formato tabular, de modo a permitir a análise dos dados brutos que originam os gráficos.

X. O portal deverá manter o histórico de dados pelo período mínimo de 12 (doze) meses, assegurando também a criação de filtros temporais para consultas em diferentes intervalos.

XI. O TJES poderá, a qualquer tempo, solicitar o fornecimento dos dados brutos coletados pelas soluções integrantes do objeto contratado.

XII. As informações disponibilizadas pelo portal deverão representar o estado do ambiente em tempo real, com atualização automática e contínua.

XIII. A ferramenta deverá permitir a definição e customização de limiares (thresholds) para serviços e eventos, de forma a gerar alarmes vinculados aos Acordos de Nível de Serviço (SLA) que serão estabelecidos no Termo de Referência.

XIV. O portal deverá prover mecanismos de análise de risco e geração de métricas de disponibilidade, por meio de relatórios e dashboards consolidados de todas as soluções que compõem o objeto.

1.3.4.2 Requisitos Gerais das Torres 1 e 2

a. Todos os equipamentos e softwares fornecidos pela CONTRATADA, quando necessários à execução das atividades de segurança, deverão atender integralmente às especificações técnicas do objeto durante toda a vigência contratual. Isso inclui garantia de funcionamento, manutenção preventiva e corretiva, atualização contínua dos produtos e monitoramento de segurança em regime ininterrupto (24 horas por dia, 7 dias por semana).

b. Os equipamentos eventualmente fornecidos deverão ser novos, de primeiro uso, e não poderão, no momento da entrega da proposta técnica, constar em listas de descontinuidade do fabricante (end-of-sale, end-of-support, end-of-life ou equivalentes). Em outras palavras, não poderão possuir previsão de término de fornecimento, suporte ou ciclo de vida útil.

c. Os softwares ofertados pela CONTRATADA deverão ser instalados em suas versões mais estáveis e atualizadas, estando obrigatoriamente cobertos por

contratos de suporte e atualização de versão junto ao fabricante durante toda a vigência do item de serviço correspondente. Da mesma forma, todos os equipamentos vinculados ao objeto deverão possuir garantia oficial do fabricante.

d. O atendimento aos requisitos de cada serviço poderá ser realizado de forma integrada, mediante composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, desde que essa integração não altere a topologia de rede nem exponha ativos a riscos adicionais de segurança da informação, especialmente no que se refere à integridade, confidencialidade e disponibilidade.
e. A CONTRATADA deverá conceder ao CONTRATANTE acesso às consoles dos produtos implantados, possibilitando o acompanhamento, a auditoria e a definição de ações relacionadas ao ambiente.
f. As mudanças nos ambientes de tecnologia deverão seguir o processo formal de gerenciamento de mudanças do TJES. Sempre que convocada, a CONTRATADA deverá participar das reuniões para este fim, prestando informações técnicas sobre os ambientes e serviços sob sua responsabilidade. Alterações complexas, que envolvam múltiplas equipes ou fornecedores e que possam gerar riscos de indisponibilidade de serviços prioritários, deverão ser tratadas como Projeto, devendo a CONTRATADA apresentar proposta formal contendo análise de riscos e avaliação de impactos.
g. Compete ainda à CONTRATADA testar e emitir parecer técnico sobre qualquer novo Item de Configuração (IC) que venha a suportar os serviços de segurança do TJES, mediante elaboração de nota técnica com análise de riscos para o ambiente. A liberação de novos ICs dependerá de aprovação expressa do TJES, sendo que liberações que representem risco a serviços prioritários deverão igualmente ser tratadas como Projeto.
h. A CONTRATADA deverá realizar monitoramento contínuo e avaliação crítica dos serviços prestados, elaborando curvas de comportamento, estabelecendo a volumetria média de acessos e identificando padrões anômalos de utilização. O objetivo é permitir a detecção antecipada de potenciais incidentes de segurança da informação, de forma preventiva, antes que ocasionem impacto nos serviços em produção.
i. Manutenções preventivas ou corretivas que impliquem risco de interrupção dos serviços deverão ser previamente agendadas e executadas fora do horário regular, salvo autorização expressa do CONTRATANTE. Quando tais manutenções demandarem parada prolongada do ambiente, deverão ocorrer preferencialmente

em finais de semana. Tais atividades não ensejarão custos adicionais ao valor contratado, devendo a CONTRATADA prever os respectivos encargos em sua composição de preços.

j. Todos os serviços de manutenção são considerados de natureza contínua e deverão minimizar qualquer necessidade de paralisação do ambiente de produção. Após cada manutenção, os serviços impactados deverão ser testados e somente serão considerados aceitos após validação da área demandante e/ou da fiscalização designada pelo CONTRATANTE, que verificará o atendimento às características técnicas esperadas.

k. O padrão de acessos ao ambiente deverá ser monitorado continuamente, sendo definidos, em conjunto com o CONTRATANTE, os limites (thresholds) a partir dos quais um evento será caracterizado como incidente de segurança da informação.

l. Todos os serviços deverão ser executados por profissionais devidamente qualificados, possuidores de programas de formação e/ou certificações oficiais, em conformidade com os perfis técnicos requeridos para cada atividade.

m. A CONTRATADA deverá elaborar relatórios mensais sobre a utilização e capacidade dos Itens de Configuração (ICs) relacionados aos serviços, apresentando seu desempenho em relação ao cumprimento dos níveis de serviço estabelecidos. Também será de sua responsabilidade o monitoramento contínuo dos acessos e dos ICs, criando base histórica para auditoria e gestão.

n. Todos os serviços deverão observar as normas, procedimentos e técnicas estabelecidos pelo TJES.

o. Todos os equipamentos e softwares utilizados pela CONTRATADA para a entrega deste serviço, devem ser declarados de forma clara e objetiva na proposta cadastrada para a fase de lances deste processo, incluindo, minimamente, fabricante, modelo, versão e quantitativo.

p. A proposta deverá ser complementada por planilha de comprovação do atendimento às especificações, item a item, contendo referências à documentação técnica oficial (manuais, catálogos, datasheets, artigos de suporte técnico do fabricante) e a página/tópico em que cada requisito se encontra descrito, ou, alternativamente, imagens das consoles que comprovem a conformidade.

1.3.4.3 Requisitos Gerais do Centro de Operações de Segurança (Security Operation Center - SOC)

Os serviços gerenciados de segurança que não demandarem atendimento presencial deverão ser executados a partir da infraestrutura da Central de Operações de Segurança (Security Operations Center – SOC), a qual deverá dispor, de forma comprovada, de mecanismos de redundância para garantir a continuidade das operações em caso de indisponibilidade do SOC principal. Ambos deverão estar ativos e atender, no mínimo, aos seguintes requisitos:

- Utilizar sistema de gerenciamento de CFTV que possibilite o rastreamento de movimentações no ambiente da CONTRATADA, com capacidade de recuperação das imagens gravadas;
- Garantir cobertura completa por filmagem de toda a área, com armazenamento das imagens por período mínimo de 90 (noventa) dias;
- Manter registro de entrada e saída de visitantes em todos os acessos ao SOC, com identificação individual, preservado por no mínimo 90 (noventa) dias;
- Dispor de solução para monitoramento contínuo de disponibilidade e desempenho;
- Manter o perímetro protegido contra intrusão física e acessos não autorizados;
- Ser vigiado permanentemente por equipe de segurança especializada, em regime ininterrupto de 24x7x365;
- Adotar controle de acesso físico com, no mínimo, dois fatores de autenticação;
- Estar configurado de forma que a falha de um equipamento isolado não comprometa a continuidade dos serviços;
- Possuir sistema de fornecimento ininterrupto de energia elétrica, composto por grupo gerador e unidades de alimentação contínua (UPS), assegurando a transição entre o fornecimento de energia e o gerador;
- Incluir mecanismos de proteção contra incêndio, bem como plano de recuperação de desastres devidamente testado e documentado;
- Possuir processos implementados que assegurem a confidencialidade, integridade e disponibilidade das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001, sendo obrigatória a apresentação da certificação correspondente em 30 dias após a emissão da Ordem de Serviço correspondente;

A CONTRATADA deverá adotar controles de segurança adequados, incluindo mecanismos de criptografia, de modo a assegurar a confidencialidade de todos os dados e informações do CONTRATANTE que venham a ser processados em seu ambiente ou em ambiente de terceiros por ela contratados.

A CONTRATADA deverá comunicar formalmente o CONTRATANTE sempre que identificar falhas de implementação em serviços que possam expor o ambiente a vulnerabilidades ou risco de indisponibilidade.

1.3.4.4 Fornecimento de Link Dedicado

a) A CONTRATADA deverá fornecer links de comunicação dedicados e de uso exclusivo, com acesso restrito e criptografado, para conectar o Datacenter do CONTRATANTE ao(s) SOCs ou nuvens da CONTRATADA.
b) Todo e qualquer tráfego de comunicação entre a CONTRATANTE e a CONTRATADA necessário para a operacionalização do serviço (incluindo, mas não se limitando a: logs, acessos a ativos de rede e estações de trabalho), deverá obrigatoriamente trafegar pelo link dedicado fornecido.
c) Especificamente para o tipo de conexão digital, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com links xDSL (executada a tecnologia HDSL). Deverá ser um link dedicado, ponto a ponto, não sendo admitidos links de Internet (seja qual for o seu formato) e o endereçamento usado será privativo (IPv4 e IPv6 a critério da CONTRATANTE).
d) A fim de garantir a segurança do tráfego bidirecional entre a TJES e os Centros de Operações de Segurança da CONTRATADA, as conexões devem ser criptografadas.
e) A solução de interconectividade não poderá ser estabelecida por VPN's do inglês virtual private network, do tipo site to site, assim como sendo feita através de conexão via internet para cada Centro de Operações de Segurança.
f) O tráfego não deverá passar de forma alguma pela internet.
g) Os equipamentos responsáveis pela interconexão são de responsabilidade da CONTRATADA, tanto na ponta da CONTRATANTE como nos dois centros de operação da CONTRATADA.
h) Os equipamentos utilizados pelo CONTRATANTE devem possuir redundância automática, sem intervenção manual em caso de falha.
i) A utilização não deverá ultrapassar 80% (oitenta por cento) de sua capacidade.

j) A CONTRATADA deverá prover redundância para este link de comunicação, podendo ser utilizado, outro link dedicado, dupla-abordagem de meio físico como redundância, sendo vedado o uso dos links de internet da CONTRATADA como link primário ou secundário/redundante.

k) Em caso de falha de link, reparo em 4 horas. Se um segundo link falhar enquanto o outro estiver em falha, reparo dos dois em 1 hora.

l) Os links primário e secundário (redundante) deverão possuir nível de SLA mínimo de 99%, com capacidade para atender integralmente a todos os requisitos desta prestação de serviços.

m) Caso a capacidade do link, dimensionada pela CONTRATADA, seja insuficiente para a prestação dos serviços, esta deverá providenciar o seu aumento, sem custos para o CONTRATANTE.

n) O endereçamento da rede interna para interconectividade e operação, deve ser definida pelo CONTRATANTE e não pela CONTRATADA.

1.3.4.5 Licenciamento dos Softwares

I. Softwares SaaS: A CONTRATADA se compromete a disponibilizar à CONTRATANTE o acesso e as licenças de uso dos softwares, na modalidade de Software como Serviço (SaaS).

II. Titularidade das Licenças: A CONTRATADA deve adquirir e/ou provisionar as licenças dos softwares que compõem a solução em nome do CONTRATANTE, garantindo que este seja o único titular e detentor dos direitos de uso e de acesso ao ambiente. Qualquer conta, subscrição ou licenciamento associado a este contrato deverá ser registrado diretamente sob o CNPJ e/ou nome do CONTRATANTE.

III. Acesso e Gestão: A CONTRATADA terá acesso e permissões de gestão sobre o ambiente SaaS para fins de execução do contrato. No entanto, o CONTRATANTE deverá ter acesso administrativo e controle sobre o ambiente.

1.4. Requisitos Técnicos

1.4.1 Torre 01 - Purple Team - Atendimento de Requisições

1.4.1.1 Serviço de Administração, Operação, Manutenção e Atendimento de Requisições

I. **Das Condições Gerais**

a. Será de responsabilidade da equipe designada a execução dos serviços contratados e o acompanhamento diário de sua qualidade, garantindo o atendimento integral aos Níveis Mínimos de Serviço estabelecidos.

b. Essa equipe deverá ter condições e tempo hábil para realizar, sempre que necessário, os ajustes e correções indispensáveis à continuidade do serviço. Qualquer evento que possa, ainda que em potencial, comprometer a regularidade da execução ou o cumprimento das metas definidas nos Níveis Mínimos de Serviço deverá ser comunicado de forma imediata e formal ao CONTRATANTE.

c. O objetivo central deste serviço é sustentar e operar as soluções e produtos de segurança do TJES, promovendo ações permanentes e proativas voltadas à proteção do parque computacional, bem como de outras soluções que venham a compor o ambiente de segurança do CONTRATANTE. Tais atividades deverão assegurar que o ambiente permaneça estável, disponível e íntegro.

II. **Da Avaliação do Ambiente**

a. A CONTRATADA deverá realizar, nos primeiros 30 (trinta) dias de execução deste serviço, uma avaliação completa do ambiente tecnológico do CONTRATANTE, com o propósito de identificar lacunas e oportunidades de melhoria (Gap Analysis), de modo a aferir o nível de maturidade dos controles de segurança implementados.

b. Essa avaliação deverá ser conduzida com base no framework de segurança MITRE ATT&CK, que reúne conhecimento global sobre táticas, técnicas e procedimentos (TTPs) utilizados por agentes maliciosos, permitindo medir a efetividade dos controles existentes. Alternativamente, poderão ser empregados outros frameworks reconhecidos, como o CIS Controls ou o NIST Cybersecurity Framework (CSF), conforme determinação do CONTRATANTE.

c. A análise deverá ser repetida anualmente durante todo o período de vigência contratual, de forma a acompanhar a evolução e a efetividade dos controles de segurança.

III. **Do Profissional**

a. A análise deverá ser conduzida por profissional designado pela CONTRATADA, o qual será responsável pela apresentação dos resultados ao gestor do contrato, aos fiscais designados e aos gestores de TI do TJES. Esse profissional deverá possuir, no mínimo, 3 (três) das seguintes certificações, ou equivalentes reconhecidas no mercado:

i. Certified Information Systems Security – CISSP®;
ii. Certified Information Security Manager – CISM®;
iii. Certified Intrusion Analyst – CIA®;
iv. GIAC Security Essentials – GSEC®;
v. GIAC Certified Incident Handler – GCIH;
vi. GIAC Continuous Monitoring – GMON ®;
vii. ISO/IEC 27001:2022;
viii. ISO/IEC 27005:2022;
ix. NIST CSF - Cyber Security Framework v2.0;
x. CSIRT - Cyber Security Incident Response Team;
xi. CIS Controls v8.0;
xii. Certified in Cybersecurity (CC);
xiii. Certified Security Specialist (E|CSS);
xiv. CompTIA - Security+;
xv. ISACA - CSX Cybersecurity Practitioner Certification (CSX-P);

b. O profissional será responsável pela condução inicial e subsequente das análises de lacunas (Gap Analysis) e assumirá, adicionalmente, a função de Gerente Técnico de Projetos do contrato, no que se refere às Torres de Serviços 01 e 02. Compete a esse gerente a orquestração das atividades entre as referidas torres, a apresentação dos Relatórios de Operações Mensais (ROMs) e a condução de todas as atividades técnicas vinculadas a esses grupos.

c. Esse profissional será também responsável por manter o alinhamento e a comunicação direta com o Gerente Técnico local das equipes especializadas da CONTRATANTE. Caberá ainda a ele receber os relatórios de testes de intrusão (pentests) executados pelo Grupo 03 – Pentest, encaminhando e

coordenando as ações necessárias para a correção tempestiva dos apontamentos realizados.

d. Para o Grupo 03 – Serviços de Testes de Invasão (Red Team**)** deverá ser designado outro Gerente de Projetos, exclusivo para aquele grupo.

e. Fica vedado que qualquer Gerente de Projetos, independentemente do grupo ou torre a que esteja vinculado, acumule a função de Preposto do Contrato.

IV. Dos Entregáveis

a. Os entregáveis dessa etapa são:

i) Metodologias e Ferramentas utilizadas;
ii) Relatório de GAPs;
iii) Infográfico de Maturidade;
iv) Artefatos de Avaliação;
v) Avaliação das Técnicas e Sub Técnicas;
vi) Matriz de Priorização.
vii) Data do Próximo GAP Analysis

V. Das Atividades

a. Principais atividades a serem executadas de forma contínua pela CONTRATADA:

i. Monitoramento e Acompanhamento:

a) Acompanhar de forma sistemática a execução dos serviços, assegurando o cumprimento dos níveis de serviço estabelecidos;

b) Priorizar os atendimentos classificados como críticos, de acordo com a definição do CONTRATANTE;

c) Monitorar permanentemente e avaliar de maneira crítica os produtos e serviços de segurança sob responsabilidade do CONTRATANTE;

d) Atuar de forma proativa na antecipação e identificação de incidentes de segurança, prevenindo impactos nos serviços;

e) Responder tempestivamente a eventos de Segurança da Informação (SI) que possam afetar a disponibilidade, a integridade ou a confidencialidade das informações

processadas nos sistemas ou serviços de TI do CONTRATANTE;

f) Atuar em situações de falha nos controles de segurança ou em cenários imprevistos que apresentem risco de comprometer os sistemas e serviços de TI;

g) Elaborar e disponibilizar relatórios técnicos e gerenciais que comprovem a execução dos serviços realizados;

h) Supervisionar a equipe designada, assegurando a correta execução das atividades de Segurança da Informação.

ii. Planejamento e Organização

a) Elaborar e apresentar ao CONTRATANTE o plano de execução dos serviços, contemplando prazos, recursos e responsabilidades;

Organizar a alocação de turnos e a escala dos profissionais de sua equipe, assegurando cobertura adequada às necessidades do serviço;

b) Definir e implementar plano de treinamento inicial e de capacitação contínua para os profissionais envolvidos na execução dos serviços;

c) Executar atividades correlatas à supervisão da equipe, garantindo a conformidade e a qualidade na entrega dos Serviços Gerenciados de Segurança;

d) Orientar a atuação da equipe técnica em situações críticas, bem como interagir com os usuários sempre que a situação demandar suporte direto.

iii. Gestão de Recursos:

a) Apoiar o TJES na construção, manutenção contínua e atualização de procedimentos sistematizados e da base de conhecimento, contemplando soluções de problemas e respostas padronizadas, mediante aprovação prévia do CONTRATANTE;

b) Receber, analisar e executar as demandas relacionadas à área de segurança da informação, providenciando a adequada alocação de recursos técnicos e humanos;

c) Consolidar os relatórios mensais (mês calendário) referentes aos Serviços Gerenciados de Segurança, apresentando informações gerenciais ao CONTRATANTE;
d) Supervisionar a equipe designada na execução das atividades conjuntas com a área de infraestrutura, observando integralmente a Política de Segurança da Informação do TJES e aplicando as melhores práticas de mercado;
e) Documentar e consolidar em manuais de procedimentos e na base de conhecimento todas as soluções adotadas. Para as atividades que não possuam rotinas definidas, a documentação deverá ser produzida após sua execução, sendo esta condição para a aceitação do serviço;
f) Manter atualizada a Base de Dados de Gerenciamento de Configuração dos ativos contemplados no objeto contratual;
g) Assegurar a disponibilidade do serviço de suporte técnico das soluções ofertadas, garantindo sua plena utilização durante toda a vigência contratual;
h) Executar os serviços de implantação de novas versões, patches, releases e service packs dos produtos de segurança utilizados no ambiente do CONTRATANTE. Quando houver suporte técnico de terceiros, a CONTRATADA deverá abrir chamados e coordenar a execução junto ao fabricante;
i) Apoiar o CONTRATANTE nas comunicações técnicas com os fabricantes dos produtos utilizados na execução contratual;
j) Elaborar relatórios mensais de desempenho, auditoria e operação dos ativos sob sua responsabilidade;
k) Implementar melhorias solicitadas pelos servidores do CONTRATANTE, a partir das aberturas de chamados no sistema de gestão de serviços de TI;
l) Apresentar sugestões de adoção de novas tecnologias que possam modernizar o ambiente tecnológico, subsidiando a equipe do CONTRATANTE na gestão de segurança da informação.

iv. Processos e Padrões:

a) Aplicar, obrigatoriamente, os seguintes processos preconizados pelo ITIL: Gerenciamento de Incidente, Cumprimento de Requisição, Gerenciamento de Problema, Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Mudança, Gerenciamento de Liberação e Implantação, Gerenciamento da Disponibilidade, Gerenciamento do Conhecimento, Gerenciamento de Níveis de Serviço e Gerenciamento do Catálogo de Serviço;
b) Consolidar e apresentar sugestões de melhoria voltadas à otimização dos serviços de segurança da informação;
c) Executar atividades de implantação, substituição e atualização de soluções de segurança da informação, prevendo prazos, custos, recursos e qualidade, em conformidade com as Práticas de Gerenciamento de Projetos – PMI.

v. Análise e Relatórios:

a) Monitorar e analisar os logs gerados pelos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, softwares utilizados, entre outros), propondo medidas corretivas e de melhoria;
b) Elaborar e consolidar relatórios periódicos sobre ataques identificados;
c) Apoiar tecnicamente a elaboração de relatórios detalhados sobre funcionalidades necessárias de equipamentos e softwares a serem adquiridos, no âmbito da segurança da informação, conforme demanda do CONTRATANTE;
d) Receber as diretrizes emitidas pela área de Segurança da Informação e providenciar a execução e alocação de recursos necessários ao atendimento;
e) Apoiar e participar da implementação de processos e da mensuração de indicadores de objetivos definidos pelo CONTRATANTE;
f) Executar todas as atividades em estrita conformidade com a Política de Segurança da Informação (PSI) e demais normas estabelecidas pelo CONTRATANTE;

g) Consolidar em manuais e scripts todos os serviços e soluções adotados, sejam eles novos ou já implantados no ambiente do CONTRATANTE;
h) Auxiliar na elaboração de procedimentos e metodologias de segurança, bem como verificar e reportar seu cumprimento pelas demais áreas de TI;
i) Apoiar o CONTRATANTE na análise e definição das regras de uso dos recursos computacionais;
j) Monitorar e propor soluções para os projetos e atividades em andamento, otimizando-os sob a ótica dos requisitos de Segurança da Informação;
k) Participar, quando solicitado, de reuniões com gestores e equipes envolvidas em projetos de desenvolvimento, manutenção de sistemas e administração de dados, apresentando soluções de segurança aplicáveis;
l) Apoiar o CONTRATANTE em projetos de Segurança da Informação;
m) Propor novos procedimentos de Segurança da Informação;
n) Implantar serviços de disseminação de alertas relacionados a Segurança da Informação;
o) Executar atividades relativas aos normativos e práticas de governança do CONTRATANTE no âmbito da segurança da informação;
p) Apoiar o CONTRATANTE em situações de mudanças decorrentes de atualizações ou remanejamentos de infraestrutura;
q) Realizar a configuração das ferramentas que compõem as soluções contratadas, assegurando seu uso eficiente;
r) Emitir e encaminhar relatórios de atividades ao CONTRATANTE, sempre que houver atendimento;
s) Acionar diretamente o fabricante das ferramentas, sempre que necessário, sem custos adicionais ao CONTRATANTE.

VI. Do Processo de atendimento para cumprimento de requisição de serviços

a. Ao receber uma solicitação de requisição de serviço via e-mail ou telefone, realizada por servidores autorizados da CONTRATANTE, o analista da Central de Serviços deverá registrar ou complementar as informações no sistema de acompanhamento.

b. Para as requisições abertas via web, o sistema de chamados fornecido pela CONTRATADA deverá realizar automaticamente o registro da solicitação.
c. Nas solicitações recebidas por e-mail ou telefone, o analista da Central de Serviços deverá, após efetuar o registro, proceder à categorização e priorização da requisição.
d. A categorização deverá relacionar o item de configuração ao grupo correspondente definido no Catálogo de Serviços. Todas as informações complementares levantadas deverão ser documentadas no chamado.
e. Para as requisições abertas via web, a categorização e a priorização deverão ser realizadas automaticamente pelo sistema de acompanhamento, obedecendo às mesmas regras aplicáveis ao registro manual.
f. O sistema de acompanhamento deverá identificar de forma automática se a requisição é ou não elegível para tratamento em primeiro nível.
g. Quando a solicitação for elegível em primeiro nível, o analista da Central de Serviços deverá atuar diretamente, desde que exista procedimento pré-estabelecido e aprovado pelo CONTRATANTE.
h. Caberá à CONTRATADA manter uma base de conhecimento atualizada com todos os procedimentos pré-estabelecidos e aprovados, integrada ao sistema de acompanhamento de chamados, garantindo acesso à CONTRATANTE para consultas e aprovações de novos procedimentos.
i. Será ainda responsabilidade da CONTRATADA a criação, revisão e manutenção dos procedimentos operacionais, cabendo à CONTRATANTE apenas a aprovação quando houver criação ou alteração.
j. O analista da Central de Serviços deverá registrar no sistema sua atuação, descrevendo todas as informações relevantes para o atendimento da requisição.
k. Em caso de solução, o analista deverá atualizar o chamado no sistema, registrando:
    i. o(s) item(ns) de configuração envolvidos; e
    ii. a categorização corrigida, se necessário.

l. Quando a requisição não for elegível em primeiro nível, o analista deverá encaminhá-la ao grupo solucionador adequado. Esse encaminhamento poderá ser automático, caso o Catálogo de Serviços já defina a elegibilidade e o grupo responsável.

m. O grupo solucionador, ao receber a requisição, deverá analisar se a demanda está dentro de seu escopo ou se deve ser encaminhada a outro grupo. Caso seja de sua competência, deverá executar o atendimento.

n. Se para o cumprimento da requisição for necessária uma mudança, o fluxo seguirá para o processo de gestão de mudanças do TJES. Nesse caso, a CONTRATADA apenas participará quando convocada, uma vez que a governança do processo de mudanças não integra o objeto contratual.

o. Se for necessário o acionamento de fornecedor externo (de serviços ou infraestrutura), o grupo solucionador deverá seguir as regras estabelecidas pelo CONTRATANTE. O chamado deverá ter seu status atualizado para “encaminhado para fornecedor” e permanecerá assim até o retorno.

p. O registro da solicitação no sistema do fornecedor, quando aplicável, deverá constar também no sistema da CONTRATADA. Caberá ao grupo solucionador acompanhar e monitorar o atendimento realizado pelo fornecedor.

q. Após a entrega do fornecedor, caberá ao grupo solucionador avaliar e validar o resultado, com base nos Níveis Mínimos de Serviço e nas regras definidas no contrato.

r. O grupo que executou a requisição deverá registrar no sistema todas as informações relevantes relacionadas ao cumprimento do serviço.

s. Quando a requisição for resolvida, o grupo responsável deverá atualizar o chamado para o status “resolvida”, registrando:

    i. o(s) item(ns) de configuração envolvidos; e

    ii. eventuais correções de categorização.

t. Após ser marcada como resolvida, a requisição deverá permanecer por 2 (dois) dias úteis com esse status, período no qual a CONTRATANTE poderá reabri-la caso entenda que a solução não foi satisfatória. Findo esse prazo, sem manifestação, o status deverá ser alterado para “fechada”.

u. O processo aqui descrito constitui o padrão mínimo a ser seguido pela CONTRATADA. Contudo, por se tratar de um serviço continuado, espera-se

da CONTRATADA a busca por melhorias contínuas, as quais poderão ser implementadas mediante aprovação da CONTRATANTE.

VII. Do Grupo Solucionador

a. A CONTRATADA deverá manter de forma híbrida (presencial e remota), uma torre de operação denominada Grupo Solucionador, com a finalidade de atuar no processo de administração, operação, manutenção e atendimento de requisições provenientes das diversas equipes técnicas.

b. Esse grupo terá como atribuições:
   i. Apoiar o processo de configuração para envio de eventos dos ativos de TIC às ferramentas de monitoramento e resposta (SIEM, SOAR ou equivalentes) utilizadas no SOC;
   ii. Facilitar a comunicação e a interação com o time de serviços remoto da CONTRATADA;
   iii. Atuar na aplicação de patches de segurança, incluindo a abertura, tramitação e execução das requisições de mudança junto à CONTRATANTE;
   iv. Apoiar a automação de ferramentas por meio de integração via APIs.

c. Os profissionais designados para este grupo poderão atuar em regime presencial ou remoto, conforme conveniência do CONTRATANTE.

d. Ainda que exista a previsão de atendimento presencial, compreende-se que o serviço de administração, operação, manutenção e atendimento de requisições possui escopo amplo, abrangendo tanto as atividades desenvolvidas pelos profissionais lotados na CONTRATANTE quanto o suporte das equipes remotas que integram a torre de serviços da CONTRATADA em seu SOC.

e. Todos os integrantes do Grupo Solucionador deverão ser colaboradores diretos da CONTRATADA, sendo vedada a terceirização ou subcontratação das funções atribuídas.

f. Caberá à CONTRATADA dimensionar adequadamente o número de profissionais necessários para a execução do serviço, de forma a garantir a plena observância dos níveis mínimos de serviço e prazos de atendimento definidos no contrato, sem impactos na qualidade ou na continuidade das entregas.

VIII. Das Certificações do Grupo Solucionador

a. Com a finalidade de assegurar que os profissionais envolvidos possuam conhecimento e competências suficientes para atender e resolver requisições de serviço relacionadas às tecnologias e fabricantes que integram o parque de segurança da CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, alocar no Grupo Solucionador da torre de operação, em regime presencial e/ou semipresencial nas dependências da CONTRATANTE, ao menos um (01) perfil de cada profissional, conforme tabela abaixo.

b. Cada analista deverá possuir, individualmente, ao menos uma (01) das certificações previstas na lista de requisitos técnicos, com exceção do Analista de GRC, que deverá possuir ao menos duas (02) certificações. Além disso, de forma coletiva, a equipe alocada deverá comprovar a detenção de, no mínimo, quatro (04) certificações distintas dentre aquelas listadas como obrigatórias, conforme segue:

SERVIÇO	Certificações	Tipo de Atuação
Analista de Governança, Risco e Conformidade (GRC)	02 (duas) obrigatórias: • ISO/IEC 27005 - Gestão de Riscos • ISO/IEC 27005 - Lead Risk Manager • ISO/IEC 31000 - RIsk Management • GRC - Governance Risk Compliance • ISO/IEC 22301 - Business Continuity Management • ICSO - Certified Information Security Compliance Officer • ISO/IEC 27001:2022	Remoto

	• ISO/IEC 27002:2022 - Information Security Controls Foundation • CPCO - Certified Privacy Compliance Officer	
Analista de Segurança 1	01 (uma) obrigatória: • CompTIA Security+®, ou • CCSA - Checkpoint Certified Security Administrator; • CEH - Certified Ethical Hacker; • CTIA - Certified Threat Intelligence Analyst; • CND - Certified Network Defender; • CPENT - Certified Penetration Test	Remoto
Analista de Segurança 2	01 (uma) obrigatória: • CompTIA Cibersecurity Analyst(CySA+®); • CCSA - Certified Cyber Security Analyst; • CEH (Certified Ethical Hacker)	Presencial

IX. Dos Requisitos mínimos de formação técnica

a. Durante a vigência contratual, a CONTRATADA deverá assegurar que cada membro da equipe alocado para a execução dos serviços atenda, no mínimo, aos seguintes requisitos:

i. Formação acadêmica: diploma registrado de curso de graduação na área de Tecnologia da Informação, ou diploma de graduação em qualquer área, desde que complementado por certificado de curso de pós-graduação em Tecnologia da Informação, com carga horária mínima de 360 (trezentos e sessenta) horas, emitido por instituição reconhecida pelo Ministério da Educação (MEC). Para efeito de comprovação, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025.

ii. Conhecimento técnico: domínio avançado em segurança da informação, comprovado por experiência profissional mínima de 2 (dois) anos em atividades de operação, sustentação e suporte em ambientes similares ao objeto deste contrato.

X. **Dos Documentos comprobatórios de vínculo e formação técnica**

a. Será exigido da CONTRATADA a apresentação da documentação comprobatória dos profissionais designados para compor o Grupo Solucionador, a fim de demonstrar o atendimento às exigências e obrigações estabelecidas. Deverão ser apresentados, no mínimo, os seguintes documentos:

i. Carteira de Trabalho e Previdência Social (CTPS), devidamente assinada pela CONTRATADA, ou documento equivalente para comprovação do vínculo de pessoa física por meio de empresa individual;

ii. Curriculum vitae atualizado, para comprovação das habilidades declaradas, acompanhado das certificações técnicas correspondentes;

iii. Cópia dos certificados mencionados no curriculum vitae, que comprovem formalmente a capacitação técnica exigida.

XI. **Das entregas: Indicadores estratégicos de administração, operação, manutenção e atendimento de requisições**

a. Para fins de acompanhamento e avaliação do serviço prestado, a CONTRATANTE estabeleceu indicadores-chave de desempenho que deverão ser monitorados pela CONTRATADA. Esses indicadores, consolidados em um único relatório, deverão ser disponibilizados de forma

online e em tempo real, por meio do Portal de Indicadores de Serviços de Segurança, conforme descrito no item referente ao serviço, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de requisições abertas	Soma de requisições abertas	Requisições abertas	Requisições	Número total de requisições abertas
Quantitativo de requisições por função	Soma de requisições abertas por função	Requisições por função	Requisições por função	Número total de requisições por função
Quantitativo de requisições concluídas	Soma de requisições concluídas	Requisições concluídas	Requisições concluídas	Número total de requisições concluídas
TOP 10 – Ativos configurados	Soma do número de configurações por ativo	Requisições por ativo	Ativo	TOP do número de requisições por ativo
TOP 10 – Requisições por origem	Soma do número de requisições por origem	Requisições por origem	Origem	TOP do número de requisições por origem
TOP 10 – Aplicações configuradas	Soma do número de aplicações configuradas	Requisições por Aplicações	Aplicações	TOP 10 requisições por aplicações

b. Os relatórios e indicadores deverão ser apresentados e discutidos mensalmente, com base nos dados consolidados do período, em reunião a ser realizada com a CONTRATANTE. Para tanto, a CONTRATADA deverá disponibilizar profissional com pleno conhecimento sobre todos os serviços contratados, responsável pela exposição e esclarecimento das informações. A apresentação deverá ocorrer presencialmente, nas dependências da CONTRATANTE, ou de forma virtual, por meio de solução de videoconferência, conforme conveniência da CONTRATANTE.

1.4.2 Torre 02 - Blue Team- Gestão de Incidentes de Segurança e Monitoramento de Ataques Cibernéticos

1.4.2.1 Serviço de Gestão de Vulnerabilidades

I. **Das Condições Gerais:**

a. O objetivo deste serviço é identificar, de forma proativa e recorrente, vulnerabilidades de segurança da informação presentes na infraestrutura tecnológica e nas aplicações do TJES, de modo a prevenir que ataques cibernéticos explorem fragilidades conhecidas e comprometam a confidencialidade, a integridade ou a disponibilidade dos sistemas e dados institucionais.

II. **Do Escopo do Serviço:**

a. O serviço abrange a realização de identificação, análise, apoio e a execução de correções para as vulnerabilidades identificadas nos equipamentos e soluções de segurança, cujo levantamento constará em documento a ser disponibilizado na Visita Técnica.
b. A CONTRATADA deverá efetuar checagens (scans) e varreduras regulares nos ativos e recursos tecnológicos da CONTRATANTE, valendo-se de simulações de ataque como ferramenta para apoiar a priorização das correções necessárias.

c. Será de responsabilidade da CONTRATADA, no âmbito do tratamento de vulnerabilidades identificadas, conduzir todas as etapas necessárias, incluindo identificação, registro, notificação, comunicação, preparação e homologação das ações corretivas.

I. No que se refere à infraestrutura e aos servidores, caberá à CONTRATADA providenciar a disponibilização das correções cabíveis. Em relação aos sistemas, a CONTRATADA deverá direcionar a demanda à área responsável do CONTRATANTE, prestando apoio técnico sempre que necessário para a adequada aplicação das correções.

II. Compete ainda ao CONTRATANTE manter a CONTRATADA constantemente informada sobre as necessidades identificadas e os riscos associados, de modo a subsidiar a pronta atuação conjunta.

d. A aplicação dos patches ou correções, qualquer que seja a área envolvida, deverá ocorrer obrigatoriamente com a participação e acompanhamento da equipe técnica do CONTRATANTE, garantindo a mitigação efetiva dos riscos e a preservação da segurança integral do ambiente tecnológico.

III. **Do Processo de Gestão de Vulnerabilidades**

a. A lista de ativos e recursos que deverão compor o processo de gestão de vulnerabilidades será disponibilizada às empresas que participarem da Visita Técnica, em decorrência do sigilo do ambiente computacional. A CONTRATADA poderá solicitar à CONTRATANTE informações complementares para a construção da lista de checagens, como faixas de rede, ativos prioritários, horários permitidos para execução e outros parâmetros relevantes.
b. De forma contínua, a CONTRATADA deverá realizar avaliação prévia no ambiente computacional da CONTRATANTE, atuando de forma consultiva para sugerir ajustes e complementar a lista de ativos e recursos inicialmente disponibilizada.
c. Com base nas variáveis e critérios definidos no Catálogo de Serviços e na lista de ativos e recursos fornecida pelo CONTRATANTE, a CONTRATADA deverá realizar checagens (scans) e varreduras no ambiente interno e externo, com o objetivo de identificar vulnerabilidades de segurança no ambiente, utilizando as ferramentas e soluções especificadas neste documento.
d. Após cada rotina de checagens e varreduras, a CONTRATADA deverá realizar análise de falsos positivos, de forma que somente vulnerabilidades efetivamente existentes sejam comunicadas à CONTRATANTE.
e. Concluída a análise de falsos positivos, a CONTRATADA deverá informar formalmente à CONTRATANTE as vulnerabilidades encontradas, em conformidade com os critérios e requisitos previstos na seção de entregas a serem realizadas.

f. Para vulnerabilidades identificadas que não possuam solução conhecida, a CONTRATADA deverá propor medidas de contorno, cuja aplicação deverá obedecer ao processo de gestão de mudanças definido pelo CONTRATANTE. Exemplos de medidas de contorno incluem a criação de regras de isolamento em firewall, WAF, IPS ou em outros controles de segurança disponíveis.
g. Para vulnerabilidades conhecidas e catalogadas em bases reconhecidas (CVE, CVSS ou equivalentes), a CONTRATADA deverá apresentar relatório técnico especificando a vulnerabilidade e propondo a respectiva solução, que poderá incluir, a título de exemplo, a aplicação de patch oficial do fabricante ou a adoção de patch virtual (virtual patching).
h. Após a entrega do relatório contendo as vulnerabilidades identificadas e suas respectivas recomendações, caberá ao TJES autorizar a aplicação das correções e definir a janela de execução adequada para sua implementação.
i. Será responsabilidade da CONTRATADA abrir chamados junto ao Grupo Técnico de Administração, Operação, Manutenção e Atendimento de Requisições da CONTRATADA (Purple Team) para a correção das vulnerabilidades identificadas, sempre que:
    I. As vulnerabilidades estiverem relacionadas à lista de ativos e recursos da CONTRATANTE, tais como switches, impressoras, servidores, estações de trabalho e aplicações instaladas nesses equipamentos;
    II. As vulnerabilidades estiverem associadas a falhas em códigos de aplicação (por exemplo, falhas de validação de entrada que possibilitem SQL injection), devendo a CONTRATADA reportá-las formalmente e apoiar consultivamente a equipe de desenvolvimento do TJES para que sejam corrigidas com a maior brevidade possível.
j. Como etapa final, a CONTRATADA deverá atualizar todos os controles e indicadores previstos na seção de entregas a serem realizadas.
k. O processo descrito representa o padrão mínimo esperado. Todavia, por se tratar de um serviço continuado, espera-se da CONTRATADA a proposição de melhorias contínuas, desde que aprovadas pelo CONTRATANTE. O ciclo de vida do processo de gestão de vulnerabilidades deverá ser executado de forma recorrente, não se limitando às rotinas previamente definidas, sendo

facultado à CONTRATANTE solicitar análises sob demanda a qualquer tempo.

I. Adicionalmente, a CONTRATADA deverá implantar, planejar, executar, analisar e relatar testes automatizados, repetitivos e contínuos de segurança, utilizando solução de simulação de violações e ataques (Breach and Attack Simulation – BAS), com os seguintes objetivos:
    I. Avaliar e validar a eficácia operacional dos controles de segurança, identificando lacunas na cadeia de proteção e na postura de segurança do TJES;
    II. Avaliar e validar se as fontes de registros, telemetria e regras de monitoramento, detecção e resposta estão sendo corretamente capturadas pela ferramenta de monitoramento, reduzindo a ocorrência de falsos positivos e falsos negativos;
    III. Executar simulações de ataque para validar hipóteses no processo de caçada contínua de ameaças, gerando registros (logs) e evidências que subsidiem as ferramentas de análise envolvidas;
    IV. De forma continuada e periódica, a CONTRATADA deverá:
        a) Identificar e compreender os ativos mais críticos e representativos a serem submetidos aos testes automatizados de segurança;
        b) Criar e configurar casos de uso, processos, ciclos e abrangência dos testes;
        c) Administrar e monitorar a execução dos testes, analisar os resultados obtidos e emitir recomendações técnicas;
        d) Configurar e calibrar a solução de testes de segurança para otimizar a eficácia das detecções e alertas, reduzindo o tempo médio de detecção (MTTD) e o tempo médio de reparo (MTTR) das falhas encontradas;
        e) Garantir que o licenciamento da solução abranja todo o ambiente do Data Center do TJES, permitindo a instalação simultânea de agentes em todos os equipamentos, ainda que as simulações sejam realizadas em até 20 (vinte) máquinas distintas por mês;
        f) Criar e aperfeiçoar painéis (dashboards) e relatórios personalizados, assegurando resultados claros, objetivos e

abrangentes.

IV. Das Ferramentas

a. Para a execução deste serviço, caberá à CONTRATADA o **fornecimento, implantação, operação, administração e sustentação de ferramenta de gestão de vulnerabilidades**, abrangendo todo o ciclo de vida das vulnerabilidades identificadas, desde a descoberta até a mitigação.
b. A ferramenta deverá atender integralmente aos quantitativos de ativos críticos e não críticos definidos na lista de ativos do TJES, conforme documento a ser disponibilizado às empresas durante a visita técnica, contemplando, no mínimo:
    I. **37 (trinta e sete) ativos críticos** localizados no Data Center;
    II. **7.000 (sete mil) endpoints** distribuídos no ambiente do TJES.
c. Será de responsabilidade da CONTRATADA disponibilizar solução Enterprise, devidamente licenciada para o quantitativo total de ativos, garantindo cobertura completa e contínua do ambiente tecnológico da CONTRATANTE. Não será admitida a utilização de ferramentas Open Source ou in-house, tendo em vista as limitações inerentes a tais soluções e a necessidade de recursos avançados de gestão, integração e conformidade.
d. A exigência de utilização exclusiva de ferramentas Enterprise justifica-se pelas características que as distinguem, sendo indispensáveis ao contexto da CONTRATANTE, organização de grande porte, com ambiente complexo e sujeita a rigorosa regulamentação. Entre os atributos obrigatórios, destacam-se:

    I. **Recursos e funcionalidades avançados:** suporte a análise de riscos, integração com outras soluções de segurança, automação de processos, relatórios personalizáveis, correlação de dados e análise de ameaças;
    II. **Suporte profissional especializado:** acesso a equipes de suporte do fabricante, com atualizações regulares e respostas rápidas;
    III. **Escalabilidade e desempenho:** capacidade para gerenciar grandes volumes de dados, múltiplos ativos, redes complexas e ambientes híbridos;

IV. **Integração e automação:** interoperabilidade com sistemas de segurança já existentes (firewalls, IDS/IPS, SIEM), com suporte a automação de processos;
V. **Personalização e relatórios:** dashboards customizáveis, métricas de risco e relatórios adaptados a diferentes públicos;
VI. **Compliance e regulamentações:** suporte a normas e legislações como PCI DSS, HIPAA, GDPR, LGPD, entre outras.

e. Para assegurar o cumprimento dos Acordos de Nível de Serviço previstos neste documento, a CONTRATADA deverá prover, sem ônus adicional ao CONTRATANTE, todos os módulos e complementos necessários ao pleno funcionamento da solução. A utilização de ferramentas adicionais, quando necessária, dependerá de avaliação e aprovação prévia da equipe técnica do TJES.
f. Além da ferramenta fornecida, espera-se que a CONTRATADA adote métodos e técnicas assistidas que complementem o processo de descoberta de vulnerabilidades, ampliando a abrangência e a precisão das análises.
g. Com o objetivo de mitigar riscos e evitar impactos durante as rotinas de validação, todas as ferramentas e métodos propostos deverão ser previamente apresentados ao time de Segurança da Informação do TJES, que deliberará sobre sua aprovação.

V. Dos Requisitos Mínimos da Ferramenta de Gestão Vulnerabilidades

a. **Personalização e Exportação de Relatórios**
   I. Deve permitir a personalização de relatórios classificados por vulnerabilidade ou por host;
   II. Deve possibilitar a exportação de relatórios, no mínimo, nos formatos HTML, CSV e PDF.
b. **Notificações e Comunicação**
   I. Deve possuir capacidade de enviar notificações com os resultados das varreduras por e-mail.
c. **Descoberta e Varredura de Ativos**
   I. Deve realizar a descoberta e varredura de ativos;
   II. Deve suportar varreduras em redes IPv4, IPv6 e FQDN;

III. Deve executar varreduras em busca de vulnerabilidades sem credenciais;
IV. Deve executar varreduras autenticadas com uso de credenciais, incluindo verificação de patches;
V. Deve contemplar varreduras em sistemas operacionais, dispositivos de rede, hypervisors, bancos de dados e servidores web.

d. **Auditoria e Conformidade**
I. Deve possuir trilha de auditoria;
II. Deve suportar hypervisores VMware vSphere ESX, KVM (Nutanix/Proxmox);
III. Deve suportar as principais soluções de nuvem (ex.: AWS, Azure, Google);
IV. Deve ser compatível, no mínimo, com os seguintes sistemas operacionais: Windows 7, Windows 10, Windows 11, Linux Debian, SUSE, Ubuntu, Red Hat Enterprise Linux;
V. Deve suportar varreduras autenticadas em bases de dados Oracle, SQL Server, MySQL, PostgreSQL e MariaDB;
VI. Deve oferecer varredura de conformidade personalizada para ambientes Windows e Unix;
VII. Deve incluir suporte à detecção de vírus, malwares, botnets e processos conhecidos ou desconhecidos;
VIII. Deve auditar o agente antivírus instalado, informando se está mal configurado ou com regras desatualizadas;
IX. Deve oferecer auditoria de configuração baseada em normas e padrões reconhecidos, tais como CIS, CERT, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA e PCI;
X. Deve suportar a configuração de políticas e templates de auditoria.

e. **Pontuação de Risco e Escaneamento**
I. Deve atribuir pontuação de risco às vulnerabilidades com base no padrão CVSS, apresentando cinco níveis (crítico, alto, médio, baixo e informativo);
II. Deve permitir a personalização dos níveis de gravidade para readequação da matriz de riscos;
III. Deve possibilitar escaneamento de número ilimitado de endereços IP/dispositivos de destino;

IV. Deve possuir interface de gerenciamento via web;

V. Deve permitir o agendamento de escaneamentos, incluindo definição de sub-redes ou IPs específicos como alvo.

f. **Resolução e Mitigação de Vulnerabilidades**

I. Deve indicar formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e ajustes de configuração necessários para eliminar ou reduzir a exposição ao risco;

II. Deve fornecer acesso a templates de escaneamento pré-determinados, para identificação de vulnerabilidades específicas;

III. Deve associar identificadores CVE (Common Vulnerabilities and Exposures) às vulnerabilidades identificadas, possibilitando geração de relatórios, gestão de riscos e mitigação de ameaças;

IV. Deve identificar vulnerabilidades de aplicação, incluindo Cross-Site Scripting, SQL Injection, entre outras;

V. Deve manter o histórico completo dos escaneamentos realizados anteriormente.

VI. Da Ferramenta: Solução Informatizada de Simulação de Violações e Ataques (BAS)

a. A solução de BAS deverá ser composta por agentes (softwares) ou atores simuladores virtuais, em conformidade com as exigências estabelecidas neste documento.

I. Todos os itens que compõem a solução de BAS, incluindo o sistema de gerenciamento, deverão ser produzidos pelo mesmo fabricante. Não serão aceitos componentes baseados em softwares genéricos, devendo obrigatoriamente ser fornecidos por fabricantes amplamente consolidados no mercado. Para referência de mercado, serão adotados estudos de institutos independentes, como Gartner, Forrester, IDC e ISG Group.

II. A solução deverá contemplar a versão mais estável e recomendada de software e/ou firmware pelo fabricante. O fabricante deverá possuir rede própria de *Threat Intelligence*, com atualização automática e contínua do portfólio de ameaças (*threat feed*).

III. A ferramenta deverá permitir gerenciamento centralizado por interface gráfica (GUI), acessível em formato web seguro (HTTPS) ou aplicativo cliente compatível com Windows 10 ou superior, podendo ser provida em nuvem (cloud), appliance virtual ou integrada à própria solução. Caso a gerência seja em nuvem, o encaminhamento de dados deverá ocorrer de forma criptografada, sem envio de informações de usuários, e os dados armazenados deverão permanecer protegidos por criptografia.

b. **Arquitetura**

I. A solução deverá disponibilizar agentes de software que possam ser instalados em máquinas físicas ou ambientes virtuais (servidores), bem como atores simuladores virtuais em formato de arquivos *.OVA, capazes de criar ambientes isolados destinados à reprodução de ataques.

II. Os agentes deverão ser compatíveis, no mínimo, com sistemas operacionais Linux e Windows (Server, 7, 10 e 11).

III. A solução deverá possibilitar a instalação de agentes, ou de máquinas virtuais em formato OVA/ISO, também em ambientes de cloud (nuvem) compatível com a existente na CONTRATANTE.

c. **Características da Solução**

I. Simular ataques em diferentes vetores, incluindo gateways de web e e-mail, WAF (Web Application Firewall), endpoints (EDR, antivírus) e em toda a Cyber Kill Chain, contemplando infiltração, movimento lateral, exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs);

II. Garantir que as simulações não gerem risco real de infecção ou comprometimento do ambiente da CONTRATANTE;

III. Basear o portfólio de ataques em frameworks de referência, como MITRE ATT&CK, OWASP, CVSS e NIST;

IV. Possuir portfólio de ataques, templates e cenários atualizado de forma contínua, manual e automática, com possibilidade de agendamento;

V. Permitir configuração de cenários de ataque e seleção de ataques específicos para execução;
VI. Permitir agendamento de simulações, inclusive com execução contínua e automatizada;
VII. Garantir execução ilimitada de todos os vetores de simulação disponíveis durante a vigência do contrato;
VIII. Possuir base de recomendações de remediação, com orientações sobre correções, mitigação de impactos e prevenção, alinhadas às recomendações de fabricantes de soluções de segurança;
IX. Oferecer atualização diária da base de malwares;
X. Possuir instrumentação de IoCs (Indicators of Compromise) provenientes de provedores de *Threat Intelligence* e/ou laboratório próprio do fabricante;
XI. Realizar simulações de campanhas de ameaças, apresentando relatórios com descrição detalhada, impactos e regiões afetadas;
XII. Disponibilizar APIs (Application Programming Interfaces) para integração com demais soluções de segurança;
XIII. Possuir integração nativa com soluções de SIEM e EDR;
XIV. Possuir integração com linguagens de script, como Python.

d. **Dashboard**

I. Disponibilizar dashboard interativo com visualização dos resultados das simulações, retratando o nível de risco em cada fase da Cyber Kill Chain, baseado no MITRE ATT&CK, com possibilidade de customização das visões;
II. Apresentar dados históricos de ataques simulados, incluindo rastreamento;
III. Detalhar, no mínimo:
    a) tipo de ataque simulado;
    b) ações executadas pelo artefato
    c) data da simulação
    d) taxa de penetração;
IV. Permitir backup ou recuperação da solução em caso de desastre, assegurando restauração, no mínimo, das configurações da BAS,

ainda que tal funcionalidade seja prestada sob demanda pelo fabricante.

e. **Relatórios e Logs**
   I. Gerar relatórios e registros de auditoria detalhados, identificando o histórico completo de acessos (logins) e ações por usuário ou grupo de usuários;
   II. Possuir a opção de gerar relatórios comparativos após cada avaliação, destacando diferenças em relação a testes anteriores e apontando vulnerabilidades críticas;
   III. Permitir exportação de relatórios, no mínimo, nos formatos PDF e CSV;
   IV. Apresentar relatórios detalhados sobre as ações executadas durante os ataques simulados;
   V. Permitir exportação de logs da solução por meio de API ou conectores compatíveis com soluções SIEM;
   VI. Ser capaz de criar incidentes de forma manual e automática, por meio de integrações com o SIEM.

VII. **Das Certificações do Grupo de gestão de vulnerabilidades**

a. Todos os profissionais da CONTRATADA que atuarem na execução dos serviços objeto deste contrato deverão atender aos seguintes requisitos mínimos:

   I. Possuir **certificação ou treinamento CCSA (Certified Cyber Security Analyst)**, ou equivalente/superior, cuja comprovação poderá ser apresentada em até 60 (sessenta) dias após a assinatura do contrato;
   II. Possuir **certificação ou treinamento oficial** dos fabricantes das soluções informatizadas necessárias à execução de suas atividades;
   III. A CONTRATADA deverá contar com, no mínimo, **um (01) profissional certificado Security+**, garantindo conhecimento técnico consolidado em Segurança da Informação;

IV. A CONTRATADA deverá contar com, no mínimo, **um (01) profissional com certificação CEH, OSCP ou equivalente**, assegurando experiência de hacker ético para atuação em situações críticas de segurança;

V. Para assegurar que os profissionais tenham capacidade de atuar em atividades relativas aos serviços contratados, a CONTRATADA deverá alocar profissionais certificados especificamente para cada grupo de serviços a ser executado;

VI. A critério do CONTRATANTE, poderão ser aceitas **certificações equivalentes ou superiores**, emitidas por entidades independentes e reconhecidas no mercado, desde que comprovada a similaridade dos domínios de conhecimento e dos critérios de qualificação e aprovação exigidos;

VII. A CONTRATADA deverá promover, no prazo máximo de 6 (seis) meses, a atualização das certificações de seus profissionais, sempre que houver atualização de versão ou migração para novas soluções de TIC em decorrência da modernização do ambiente tecnológico do TJES, contados a partir da comunicação formal da CONTRATANTE;

VIII. Todas as certificações apresentadas deverão permanecer válidas durante todo o período de prestação dos serviços.

b. Para assegurar que os profissionais envolvidos possuam conhecimento e habilidades necessárias à execução do processo de gestão de vulnerabilidades da CONTRATANTE, a CONTRATADA deverá compor o Grupo de Gestão de Vulnerabilidades com, no mínimo, um profissional de cada um dos seguintes perfis:

Perfis	Certificações	Tipo de Atuação
Analista de Segurança 1	02 (duas) obrigatórias: • CompTIA Security+® • ISC2 CC Certified in Cybersecurity • ISO/IEC 27001:2022 • CEH - Certified Ethical Hacker	Remota

	• CTIA - Certified Threat Intelligence Analyst • CND - Certified Network Defender • CPENT - Certified Penetration Test • ITCerts ITC-015 - Vulnerability Management Foundation • CSIRT - Cyber Security Incident Response Team • OSCP - Offensive Security Certified Professional • CCSA - Certified Cyber Security Analyst • CompTIA - Cybersecurity Analyst (CySA+)	
Analista de Segurança 2	02 (duas) obrigatórias: • Certified Ethical Hacker – CEH® • CompTIA Cybersecurity Analyst(CySA+®) • CIA ® (Certified Intrusion Analyst) • GSEC® (GIAC Security Essentials) • GCIH ® (GIAC Incident Handler) • GMON®(GIAC Continuous Monitoring). • CCSA - Certified Cyber Security Analyst	

Analista de Segurança Linux	02 (duas) obrigatórias: • Linux LPIC 1® • Linux LPIC 2® • Linux LPIC 3® • RHCSA • RHCSE	

VIII. **Dos Requisitos mínimos de formação técnica**

a. Durante a vigência contratual, a CONTRATADA deverá garantir que todos os profissionais alocados para a execução dos serviços atendam, no mínimo, aos seguintes requisitos:

I. **Formação acadêmica**: diploma registrado de curso de graduação na área de Tecnologia da Informação ou diploma de graduação em qualquer área, desde que complementado por certificado de pós-graduação em Tecnologia da Informação, com carga horária mínima de 360 (trezentas e sessenta) horas, emitido por instituição reconhecida pelo Ministério da Educação (MEC). Para efeito de comprovação, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025.

II. **Conhecimento técnico**: domínio avançado em segurança da informação, comprovado por experiência mínima de 6 (seis) meses em atividades de gestão de vulnerabilidades.

IX. **Dos Documentos comprobatórios de vínculo e formação técnica**

a. Será exigido da CONTRATADA a apresentação da documentação comprobatória dos profissionais designados para compor o Grupo de Gestão de Vulnerabilidades, de forma a atestar o cumprimento das exigências e obrigações estabelecidas neste documento. Deverão ser apresentados, no mínimo:

I. Carteira de Trabalho e Previdência Social (CTPS), devidamente assinada pela CONTRATADA, ou documento equivalente para

comprovação do vínculo de pessoa física por meio de empresa individual;

II. Curriculum vitae atualizado, para comprovação das habilidades declaradas, acompanhado das respectivas certificações técnicas;

III. Cópias dos certificados mencionados no curriculum vitae, que comprovem formalmente os conhecimentos e qualificações exigidos.

X. **Das entregas: Indicadores estratégicos gestão de vulnerabilidade**

a. Para fins de acompanhamento e avaliação da execução contratual, a CONTRATANTE estabeleceu indicadores-chave de desempenho que deverão ser monitorados pela CONTRATADA. Esses indicadores serão consolidados em um único relatório e disponibilizados em tempo real, de forma online, por meio do Portal de Indicadores de Serviços de Segurança, conforme descrito neste documento, a saber:

DENOMINAÇÃO	**FORMA DE CÁLCULO**	**FILTRO**	**AGRUPADOR**	**DESCRIÇÃO**
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades críticas por área responsável	Soma de vulnerabilidades críticas por área responsável	Vulnerabilidades críticas	Vulnerabilidades	Número total de vulnerabilidades de críticas por área responsável
Quantitativo de vulnerabilidades corrigidas	Soma de vulnerabilidades corrigidas	Vulnerabilidades corrigidas	Vulnerabilidades	Número total de vulnerabilidades corrigidas
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB	Soma de vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades em ativos	Soma de vulnerabilidades em ativos	Vulnerabilidades em ativos	Vulnerabilidades	Número total de vulnerabilidades em ativos
Quantitativo de vulnerabilidades corrigidas em ativos	Soma de vulnerabilidades corrigidas em ativos	Vulnerabilidades corrigidas em ativos	Vulnerabilidades	Número total de vulnerabilidades corrigidas em ativos
Quantidade de vulnerabilidades em códigos de aplicações	Soma de vulnerabilidades em códigos de aplicações	Vulnerabilidades em códigos de aplicações	Vulnerabilidades	Número total de vulnerabilidades em códigos de aplicações
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

1.4.2.2 Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança

I. **Das Condições Gerais**

a. O serviço tem por objetivo assegurar o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TJES, utilizando técnicas de correlação de logs, análise de pacotes de rede e identificação de comportamentos anômalos em aplicações, serviços e infraestrutura. Esses eventos deverão ser analisados de forma sistemática, podendo ser classificados e tratados como incidentes de segurança da informação, conforme definido nos processos institucionais de gestão de incidentes.
b. Além do monitoramento proveniente da ferramenta de análise avançada de logs e pacotes de rede, a CONTRATADA deverá estender a supervisão a todos os logs e eventos de segurança gerados pelas soluções do TJES. Tais soluções estão identificadas em um documento que será disponibilizado para as empresas que participarem da visita técnica. A CONTRATADA deverá observar que todos os ativos que vierem a ser incorporados futuramente ao ambiente do TJES devem obter o mesmo nível de monitoramento e análise.
c. Para viabilizar a execução do serviço, caberá à CONTRATADA a integração da solução de análise avançada de logs e pacotes de rede com os demais componentes de segurança do ambiente do CONTRATANTE, mediante processos estruturados de coleta de logs e eventos, garantindo visibilidade centralizada e tratamento unificado das informações.

d. A CONTRATADA deverá prover capacidade técnica e operacional plena para detecção e resposta a incidentes de segurança da informação, abrangendo toda a infraestrutura de TIC do TJES.

    i. A solução ofertada deverá possibilitar a indexação e busca de informações e logs, apresentando os resultados em formatos diferenciados para cada finalidade, contemplando tanto visões técnicas quanto visões executivas, por meio de painéis específicos.
    ii. O quantitativo total de ativos presentes no ambiente do TJES, bem como suas características básicas, está descrito em documento a ser

obtido pelas empresas durante a visita técnica, devendo a cobertura desse escopo ser garantida durante toda a vigência do contrato, independentemente do modelo de licenciamento adotado.

iii. Quando o modelo de licenciamento da solução ofertada for baseado em eventos por segundo (EPS), caberá à CONTRATADA dimensionar o ambiente do CONTRATANTE de acordo com a listagem de ativos fornecida. Será de inteira responsabilidade da CONTRATADA quaisquer erros de dimensionamento, bem como a realização de ajustes necessários no licenciamento, de forma a garantir a plena adequação da solução às necessidades do CONTRATANTE.

e. Quando o licenciamento se der por ingestão de logs, deverá ser considerado o tamanho médio de 1 KB por evento. Caberá à CONTRATADA dimensionar o ambiente do CONTRATANTE de acordo com a listagem de ativos fornecida, sendo de sua inteira responsabilidade quaisquer erros de dimensionamento, bem como a realização de ajustes necessários no licenciamento, de forma a garantir a plena adequação da solução às necessidades do CONTRATANTE.
f. Os valores citados configuram uma referência mínima, cabendo exclusivamente à CONTRATADA realizar o dimensionamento adequado da solução, de forma a abranger integralmente a infraestrutura de TIC do TJES.
g. Qualquer falha de dimensionamento ao longo da execução contratual não poderá implicar em custos adicionais ou ônus de qualquer natureza ao CONTRATANTE.
h. O serviço tem por finalidade analisar, documentar, conter e remediar os eventos de segurança da informação que venham a ser classificados como incidentes.
i. A execução deverá observar rigorosamente os frameworks NIST e SANS de resposta a incidentes de segurança da informação, além de boas práticas reconhecidas de mercado.
j. Para efeitos deste documento, considera-se incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, que afete os sistemas de informação do TJES e implique na perda ou comprometimento de um ou mais princípios da Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Privacidade.

k. As categorias e níveis de incidentes a serem tratados pelos serviços da CONTRATADA estão descritas em tópico específico deste documento.
l. O serviço de resposta a incidentes será responsável por monitorar equipamentos e softwares integrantes das soluções de segurança da CONTRATANTE, compreendendo a identificação, classificação e análise de eventos que possam afetar a disponibilidade, integridade, confidencialidade ou requisitos legais de privacidade.
m. A CONTRATADA deverá prover serviços efetivos de resposta aos incidentes de segurança da informação, considerando todos os eventos identificados no monitoramento.
n. Os serviços de monitoramento e resposta poderão ser prestados remotamente, por meio de um Centro de Operações de Segurança da Informação (SOC), desde que sejam integralmente observados os níveis de serviço estabelecidos neste documento.
o. O serviço deverá ser prestado em regime de operação contínua 24x7x365, ou seja, vinte e quatro horas por dia, sete dias por semana e trezentos e sessenta e cinco dias por ano.
    i. Fluxo do Serviço: O Blue Team (equipe remota da CONTRATADA) será responsável pelo monitoramento contínuo e pela identificação de eventos de segurança.
    ii. Ao detectar um evento, o Blue Team deverá iniciar imediatamente o processo de análise e avaliação.
    iii. Quando o evento for caracterizado como incidente de segurança, a equipe do Blue Team deverá comunicar de forma imediata ao Purple Team, acionando preferencialmente o representante local do Purple Team.
    iv. O Purple Team será o responsável por interagir diretamente com as equipes técnicas especializadas da CONTRATANTE.
    v. Após o recebimento da comunicação do Blue Team, o Purple Team deverá adotar medidas imediatas, em parceria com o Blue Team, elaborando estratégias e planos de ação para a neutralização do incidente.
    vi. Caberá ainda ao Purple Team fornecer orientações detalhadas às equipes técnicas do TJES sobre as etapas a serem adotadas para a contenção e remediação do incidente.

vii. Além da abertura de chamado para registro do incidente junto às equipes técnicas do TJES, o Purple Team também será responsável pelo monitoramento ativo da execução dos procedimentos de contenção, assegurando que as ações recomendadas sejam implementadas corretamente e dentro do tempo adequado.

viii. Durante todo o processo, a CONTRATADA (Blue Team e Purple Team) atuará com responsabilidade de detecção e orientação, não assumindo a administração direta dos elementos de infraestrutura de segurança do CONTRATANTE.

ix. Ainda assim, a CONTRATADA deverá disponibilizar sua expertise técnica para apoiar o CONTRATANTE em medidas como:

a) desenvolvimento de scripts;
b) construção de GPOs (Group Policy Objects);
c) aplicação de patches de correção;
d) implementação de outras ações que contribuam para a contenção e resposta a incidentes.

II. **Das Ferramentas: Solução de análise avançada de logs e pacotes de rede**

a. Para a execução do serviço, a CONTRATADA deverá fornecer, operar, sustentar e suportar solução de monitoramento que atenda aos seguintes requisitos técnicos:

i. Qualidade e origem da solução: não serão aceitos componentes baseados em software de uso genérico. As soluções deverão ser providas por fabricantes consolidados no mercado, tendo como referência relatórios de institutos independentes e imparciais, tais como Gartner, Forrester, IDC e ISG Group.

ii. Modalidade e abrangência: a solução deverá estar enquadrada na categoria Security Information and Event Manager (SIEM), baseada em arquitetura de big data, capaz de integrar gerenciamento de registros (logs), análise de comportamento de usuários e entidades (UEBA) e resposta a incidentes de segurança em um sistema único e abrangente.

iii. Análise comportamental: a funcionalidade de UEBA deverá possuir, de forma nativa, algoritmos de aprendizado de máquina, aptos a detectar com precisão ameaças avançadas.

iv. Processamento em larga escala: a solução deverá ser capaz de operar com grandes volumes de dados em tempo real, utilizando algoritmos de machine learning, e dispor de casos de uso específicos para detecção de ameaças complexas.

v. Aderência ao MITRE ATT&CK: a solução deverá gerar detecções alinhadas ao framework MITRE ATT&CK, possuindo no mínimo 25 regras de detecção relacionadas a táticas, técnicas ou procedimentos (TTPs), devendo tais regras ser atualizadas regularmente em conformidade com as revisões do framework.

vi. Modelagem por Kill Chain: a solução deverá consolidar eventos ao longo do tempo utilizando modelos Kill Chain, possibilitando a análise de riscos em cenários complexos.

vii. Hunting de ameaças: deverá permitir a realização de ameaça hunting por meio de pesquisas em linguagem natural, garantindo agilidade na investigação.

viii. Gestão de acesso: o TJES deverá dispor, a qualquer tempo e sem necessidade de abertura de demanda prévia, de acesso direto à console, eventos e funcionalidades da solução, bem como de gestão integral sobre as identidades de acesso ao ambiente, incluindo a criação de papéis e a definição de funções baseadas em perfis.

ix. Linha do tempo: a análise de eventos deverá ser apresentada em linha temporal, facilitando a correlação e compreensão dos incidentes.

x. Autenticação: a solução deverá adotar, de forma obrigatória, autenticação multifator (2FA) nativa.

xi. Parsing de logs: deverá dispor de recursos para interpretação automática de logs (parsing).

xii. Monitoramento de sensores: a solução deverá incluir mecanismos para monitorar a saúde de todos os sensores que enviam logs para a console central, assegurando a confiabilidade do fluxo de dados.

III. **Da Arquitetura da Solução**

a. Considerando que os fabricantes de soluções de SIEM adotam diferentes modelos de cálculo para dimensionamento (variando entre a metrificação por ativos até a mensuração da quantidade de eventos gerados no ambiente) e levando em conta que o TJES não dispõe de ferramenta ativa de SIEM que

permita extrair dados históricos confiáveis, não é possível fixar previamente um número exato para o dimensionamento da solução.

b. A solução ofertada deverá estar integralmente licenciada, operacional e funcional, cobrindo toda a infraestrutura de TIC do TJES, conforme descrito no documento que lista os ativos presentes no parque do PJES e que será obtido quando da visita técnica, devendo:
    i. Deverá garantir indexação e busca de informações e logs;
    ii. Deverá prover apresentação de resultados em painéis técnicos e executivos, orientados às diferentes finalidades.
c. Estima-se que a solução de SIEM deverá estar dimensionada para suportar, no mínimo, o volume de eventos por segundo (EPS) necessário para atender integralmente à demanda do TJES, garantindo desempenho e disponibilidade adequados.
d. Não serão aceitas soluções baseadas em consoles compartilhados, devendo o ambiente lógico disponibilizado ser de uso exclusivo do TJES. A única exceção admitida será para soluções que utilizem recursos de segregação lógica por multilocação (multitenancy), desde que devidamente garantida a separação das instâncias.
e. O licenciamento da solução deverá assegurar que o processamento ocorra em tempo real ou, alternativamente, que seja mantido *buffer* de eventos, ainda que o volume de tráfego ultrapasse os limites licenciados em períodos de pico.
f. A solução deverá ser ofertada na modalidade nuvem (*Software as a Service – SaaS*), sendo exigido que o fabricante possua, no mínimo, as seguintes certificações de segurança:
    i. SOC 2 Tipo II;
    ii. ISO 27001.
g. A solução deverá possuir política de retenção configurável, assegurando a preservação de evidências para fins de conformidade normativa e de eventuais investigações forenses.
    i. Deverá ser garantida a retenção de dados brutos pelo período mínimo de 30 (trinta) dias em ambiente de armazenamento quente (hot storage).

ii. Os dados processados e os metadados de eventos deverão ser mantidos em registros no banco de dados e/ou data lake da solução pelo período mínimo de 12 (doze) meses.

h. A solução deverá oferecer alta disponibilidade e dispor de mecanismos de recuperação de desastres (disaster recovery), assegurando a continuidade do serviço.

i. Deverá permitir a filtragem e compressão seletiva de dados, com redução de até 90% no ponto de coleta.

j. Será exigido o armazenamento em cache local e/ou em buffer nos coletores, garantindo que nenhum dado seja perdido em trânsito em caso de problemas de rede ou picos no volume de eventos.

k. A solução deverá oferecer suporte ao mascaramento de dados, por meio de controles de acesso granulares baseados em função (RBAC), possibilitando a ofuscação de informações potencialmente sensíveis na camada de interface do usuário.

l. Deverá suportar administração delegada tanto para funcionalidades da interface quanto para acesso a dados e configurações, com base em controle de acesso por função (RBAC).

m. A solução deverá incluir ferramenta de Security Data Lake baseada em Big Data, com arquitetura aberta e escalável, capaz de coletar e reter dados pelos períodos definidos, em atendimento às exigências de conformidade e às necessidades de investigação.

n. A comunicação dos ativos do CONTRATANTE com o ambiente das soluções contratadas deverá ocorrer por meio de gateway interno, sempre que o acesso às respectivas consoles demandar conexão externa, de forma a assegurar controle, rastreabilidade e proteção nas interações realizadas pela internet..

IV. Das Integrações

a. A solução deverá oferecer suporte nativo à integração com variadas fontes de eventos, utilizando métodos tais como: syslog, formatos estruturados (CEF, LEEF, JSON, XML), arquivos, bancos de dados por meio de conexão JDBC, conexão via APIs (AWS, Azure, Box, Crowdstrike, SentinelOne, Trend, Symantec, Netskope, Zscaler, Skyhigh, McAfee, SVN, Splunk, QRadar,

Netwitness, Google Workspace, Office 365, Okta, Proofpoint, Tenable, Qualys, Rapid7), WMI, consultas LDAP/LDAPS, fluxos de rede (Netflow, sFlow, jFlow), Hadoop, registros não estruturados (Regex) e agentes de terceiros (ex.: Snare).

b. Deverá permitir integração com diferentes tipos de fontes de dados, abrangendo:

   i. dados de identidade;
   ii. logs de atividades e transações;
   iii. logs de eventos de segurança;
   iv. fluxos de rede;
   v. logs de aplicativos e soluções em nuvem;
   vi. permissões de acesso;
   vii. fontes de inteligência de ameaças.

c. A solução deverá possibilitar conexão com sistemas de gerenciamento de identidade externos, tais como eDirectory, Active Directory/LDAP ou demais soluções de IAM (Identity and Access Management), incluindo Microfocus Identity Manager (IDM), viabilizando o enriquecimento contextual dos eventos por meio da adição de identidade de usuários.
d. Deverá ser capaz de se conectar nativamente, por APIs ou outros mecanismos, a serviços em nuvem, como AWS (S3, CloudTrail, CloudWatch, GuardDuty, VPC Flow Logs), Box, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskope, ServiceNow, Jira, entre outros.
e. A solução deverá permitir a criação de analisadores (parsers) personalizados para ingestão de novas fontes de informação, além de possuir parsers pré-configurados prontos para uso. A análise, normalização e categorização dos coletores deverão ser totalmente personalizáveis.
f. Deverá disponibilizar API RESTful para integração bidirecional com outras tecnologias.
g. A CONTRATADA será responsável por fornecer e habilitar integrações com fontes externas de inteligência de ameaças, inclusas no valor do serviço ofertado.
h. A solução deverá possuir recursos de mascaramento de dados (Data Masking), com o objetivo de proteger informações confidenciais.

i. Deverá incluir recursos nativos de workflow, além da possibilidade de criação de workflows customizáveis para resposta a incidentes de segurança.

V. **Da Capacidades de Investigação**

a. A solução deverá realizar o enriquecimento de eventos com dados contextuais no momento da captura e ingestão, acrescentando informações como:
   i. identidade do usuário;
   ii. contexto da atividade;
   iii. metadados de ativos;
   iv. informações de rede;
   v. localização geográfica;
   vi. dados provenientes de inteligência de ameaças.

b. O enriquecimento deverá ocorrer em tempo real, adicionando atributos contextuais de usuário e entidade, de modo a viabilizar a construção de perfis comportamentais, comparações entre pares ou grupos, bem como a condução de pesquisas e investigações.

c. A solução deverá detectar ameaças cibernéticas avançadas e ameaças internas (*insider threats*) por meio de algoritmos de aprendizado de máquina, que permitam a criação de perfis e linhas de base de comportamento de usuários e entidades.

d. Deverá dispor de conteúdo pré-empacotado com casos de uso e modelos de ameaças prontos para utilização, incluindo:
   i. detecção de ameaças internas (*insider threats*) baseada em aprendizado de máquina;
   ii. detecção de ameaças cibernéticas (*cyber threats*) baseada em aprendizado de máquina;
   iii. detecção de ameaças em ambientes de nuvem (*cloud threats*) baseada em aprendizado de máquina.

e. A solução deverá fornecer mecanismos para modelagem e ajuste da pontuação de risco *(risk score*), considerando perfil do usuário ou entidade, gravidade da ameaça e a combinação ou sequência de eventos em determinado período.

f. A modelagem de risco deverá ser ajustável a partir da interface da solução, em conformidade com as prioridades organizacionais do TJES.

g. A pontuação de risco deverá ser atribuída com base em violações detectadas e em modelos de ameaças capazes de agrupar eventos relacionados a um mesmo usuário ou entidade, ainda que se estendam por dias, semanas ou meses, apresentando-os em uma cadeia de eliminação com estágios pré definidos.
h. A solução deverá incorporar algoritmos preditivos para identificar usuários de risco, como aqueles em processo de desligamento da instituição.
i. Deverá prover análises de diferentes tipos de anomalias, incluindo:
    i. desvios temporais;
    ii. volume incomum de transferência de dados;
    iii. origem ou destino atípicos dos eventos;
    iv. padrões anômalos por usuário ou grupo de pares;
    v. anomalias relacionadas à localização geográfica e velocidade de deslocamento;
    vi. rastreamento de usuários e entidades presentes em listas de observação.
j. A solução deverá contar com algoritmos de aprendizado não supervisionado, para analisar eventos atuais e históricos, identificando associações e padrões de comportamento por fonte de evento, considerando períodos como dias, semanas e horários. Qualquer desvio em relação ao padrão estabelecido deverá ser marcado como anomalia.
k. Deverá também contemplar algoritmos de aprendizado supervisionado, voltados à detecção de ameaças de malware avançadas, como DGA (Domain Generation Algorithm), ataques de phishing e campanhas de spam.
l. A solução deverá empregar técnicas de análise de raridade, permitindo identificar atividades incomuns ou nunca antes observadas.
m. Deverá dispor de análise comportamental por enumeração, capaz de criar linhas de base para eventos recorrentes e identificar desvios significativos em relação ao padrão normal.
n. Deverá incluir técnicas de análise de tráfego de rede, com capacidade de identificar padrões de beaconing, agentes de usuário incomuns, conexões suspeitas com URLs, domínios DGA e outros vetores de ataque.
o. A solução deverá permitir a definição de políticas baseadas em regras para detecção de ameaças conhecidas, que deverão atuar como intensificadores

de risco e ser combinadas com verificações não assinadas nos modelos de ameaças.

p. Deverá contemplar mecanismos de modelagem de ameaças compostas, capazes de correlacionar eventos que isoladamente seriam de baixo risco, mas que, em conjunto, indiquem situação de alto risco.
q. Deverá reduzir significativamente a ocorrência de falsos positivos, utilizando recursos avançados de aprendizado de máquina para diferenciar comportamentos normais e anômalos no ambiente monitorado.

VI. Da Visualização e Relatórios

a. A solução deverá dispor de relatórios de ameaças, capazes de oferecer visibilidade sobre a postura de segurança cibernética da instituição. Entre os elementos mínimos a serem contemplados, destacam-se: usuários de alto risco, ativos críticos, principais ameaças identificadas e endereços IP maliciosos mais recorrentes.
b. Deverá dispor de relatórios de operações de segurança, assegurando visibilidade sobre a utilização e comportamento dos recursos monitorados. Por exemplo:
    i. sessões de VPN de maior duração;
    ii. principais eventos relacionados a extração ou saída de dados;
    iii. distribuição geográfica dos eventos de login;
    iv. principais tentativas de login malsucedidas.
c. A solução deverá prover relatórios de conformidade, alinhados a requisitos normativos e regulatórios específicos, tais como PCI, SOX, HIPAA, GDPR/LGPD e ISO 27002.
d. Deverá oferecer relatórios executivos de alto nível, consolidando informações sobre violações, incidentes e operações de segurança em formato acessível à alta administração.
e. Deverá apresentar relatórios de atividade de usuários, possibilitando rastrear padrões de comportamento e eventuais desvios.
f. A solução deverá permitir a visualização gráfica dos dados em múltiplos formatos, incluindo, no mínimo: gráfico de linhas, gráfico de barras, gráfico de pizza, mapas geográficos, tabelas, gráficos de bolhas e gráficos de relacionamento entre origem e destino.

g. Deverá permitir visualizações relacionais, possibilitando a associação de diferentes atributos e a análise de suas interdependências.
h. Todas as características descritas deverão ser atendidas por uma única solução integrada, não sendo admitida a composição de diferentes ferramentas para satisfazer os requisitos estabelecidos.

VII. Da Instalação e administração da solução de SIEM

a. A solução de SIEM deverá ser implementada sem restrições quanto à quantidade de coletores, garantindo a cobertura integral do ambiente do TJES.
b. A infraestrutura necessária para a instalação dos coletores será disponibilizada pelo TJES, considerando que se trata de gateways operando dentro do ambiente institucional.
c. Caberá à CONTRATADA a implementação e gestão integral da solução de SIEM e de todos os seus componentes, compreendendo atividades de instalação, configuração, operação e sustentação.
d. A CONTRATADA deverá ser responsável pela criação de regras de correlação alinhadas às necessidades específicas do ambiente tecnológico do TJES, com o objetivo de identificar, de forma tempestiva, incidentes de segurança da informação.
e. Entre as responsabilidades da CONTRATADA incluem-se:
    i. criação de relatórios e modelos;
    ii. definição de filtros de pesquisa;
    iii. execução de rotinas de backup;
    iv. criação e manutenção de dashboards;
    v. gestão de perfis e usuários;
    vi. utilização plena dos recursos nativos da solução ofertada.
f. Deverá ser apresentado plano detalhado de instalação e configuração, contemplando todos os tipos de ativos em produção na rede do TJES.
g. A CONTRATADA será responsável por manter a solução e seus componentes atualizados, devendo aplicar a versão mais recente disponibilizada pelo fabricante, compatível com a solução adotada.
h. A instalação dos coletores deverá ser previamente agendada com o TJES, sendo executada, preferencialmente, no horário regular de expediente (segunda a sexta-feira, das 8h às 19h).

i. Atividades que possam representar risco ao funcionamento normal das unidades do TJES deverão ser realizadas fora do horário de expediente, sem ônus adicional para o CONTRATANTE.

j. A CONTRATADA deverá adotar e integrar, quando aplicável, a solução já existente do TJES com ferramentas consolidadas de mercado voltadas à gestão de patches, sendo que, de forma preferencial, será usada a ferramenta do TJES e, alternativamente, caso esta não atenda aos requisitos mínimos de funcionamento, será utilizada a ferramenta da CONTRATADA. A solução também deverá encaminhar os dados tanto para o SIEM do TJES quanto para o SIEM implementado pela CONTRATADA.

VIII. Da Responsabilidades da CONTRATADA

a. A CONTRATADA deverá, em colaboração com o CONTRATANTE, criar e implementar casos de uso (regras) nas ferramentas disponibilizadas no serviço de Monitoramento e Visibilidade de Ataques, contemplando, no mínimo:
   i. lista de casos de uso candidatos;
   ii. categorização dos casos de uso em três eixos: orientados a ameaças, orientados a controles e orientados a ativos críticos do TJES;
   iii. lista de casos de uso não operacionalizáveis;
   iv. lista de casos de uso implementados;
   v. lista de casos de uso removidos.

b. A CONTRATADA deverá revisar periodicamente os casos de uso, realizando as adaptações e evoluções necessárias, de acordo com a dinâmica das ameaças e com as necessidades da CONTRATANTE.

c. Caberá ainda à CONTRATADA produzir e entregar informações de inteligência acionável, consistentes em:
   i. procedimentos para triagem de alertas;
   ii. procedimentos para resposta a incidentes, em conformidade com os casos de uso estabelecidos.

IX. Do Processo de resposta a incidente de Segurança da Informação

a. O início do processo de resposta a incidentes de segurança ocorrerá sempre que um evento adverso for submetido pelo Serviço Gerenciado de

Monitoramento, Triagem, Tratamento e Resposta a Ataques Cibernéticos e Incidentes de Segurança, descrito em tópico específico neste documento.

b. Tal processo não se limita, contudo, ao fluxo automático: o corpo técnico de segurança do CONTRATANTE poderá, a qualquer tempo, abrir manualmente um incidente de segurança junto à Central de Serviços, seguindo as diretrizes estabelecidas no tópico de solicitações.
c. Após a abertura do incidente, caberá ao Grupo de Resposta a Incidentes de Segurança (Blue Team) da CONTRATADA:
    i. realizar a análise inicial dos logs e artefatos encaminhados;
    ii. identificar, em primeira instância, as fontes geradoras dos registros coletados.
    iii. Uma vez concluída a análise preliminar, o Blue Team deverá trabalhar para identificar os vetores de ataque que impactaram o ambiente do CONTRATANTE.
d. Como etapa seguinte, o Blue Team deverá comunicar formalmente o time de segurança da informação do TJES, dentro dos prazos estabelecidos nos SLAs deste documento, apresentando as informações iniciais do incidente e as linhas de atuação propostas para sua contenção e remediação.
e. Entre os dados e informações iniciais esperados da CONTRATADA.

Prioridade	Representação/número de prioridade ou severidade do incidente, em uma escala de 1 a 4 sendo 1 a maior prioridade.
Categoria/Classificação	Palavra única que classifica o tipo do incidente, como *malware*, *phishing*, *misconfiguration* entre outros.
Entidades fontes	Se aplicável, os detalhes dos nomes dos dispositivos, endereço de e-mails, endereços IPs, detalhes da vulnerabilidade ou outros fatores de identificação que apontam para a fonte do incidente.

Entidades de destino	Os detalhes de nomes dos dispositivos, endereços de e-mail, endereços IPs ou outros fatores de identificação que apontam para os ativos afetados.
Ações recomendadas	Instruções inteligentes e simples a serem seguidas que detalhem as ações de remediação já tomadas pela CONTRATADA e ações que a CONTRATANTE precisa tomar.
Fontes da Detecção	Detalhes das fontes dos logs ou os dispositivos de segurança que identificaram (ou colaboraram) na descoberta do incidente. Essa informação será útil para análise de causa raiz ou remediação direcionada.

f. A severidade de cada incidente de segurança deverá ser definida conjuntamente pelo Blue Team da CONTRATADA e pelo corpo técnico do TJES, considerando a combinação entre impacto (grau de criticidade do negócio afetado) e urgência (velocidade necessária para a resolução).
g. Após as análises iniciais, o Blue Team deverá realizar uma análise aprofundada do incidente, tomando por base o comportamento do ataque e/ou dos artefatos maliciosos (como malwares).
h. Todo o processo de análise, bem como os resultados obtidos, deverá ser documentado na ferramenta de gestão de incidentes de segurança da informação do CONTRATANTE, garantindo ao TJES a rastreabilidade e o acompanhamento contínuo das etapas de tratamento.
i. Identificados o comportamento e os vetores de ataque, caberá ao Blue Team definir a estratégia de mitigação e contenção. Caso a estratégia envolva alterações no parque computacional do TJES, estas deverão ser previamente autorizadas pelo corpo técnico de segurança do CONTRATANTE.
    i. Uma vez autorizada a alteração, a CONTRATADA deverá abrir chamado junto ao Serviço de Administração, Operação, Manutenção e Atendimento de Requisições, solicitando a execução da modificação necessária.

j. Após a mitigação do incidente, o Blue Team deverá iniciar o recolhimento de todas as evidências e a identificação dos serviços afetados, de forma a subsidiar o processo de análise forense.
k. A restauração dos serviços e soluções impactadas será de responsabilidade do Grupo Técnico de Administração, Operação, Manutenção e Atendimento de Requisições, que deverá atuar de forma coordenada com o Blue Team.
l. As evidências coletadas durante o processo de tratamento deverão subsidiar a análise forense, cujo objetivo será identificar pessoas, locais e/ou eventos relacionados ao incidente, correlacionar todas as informações disponíveis e gerar um laudo técnico conclusivo sobre o caso.
m. A CONTRATADA deverá realizar a reconstrução do ataque para todos os incidentes que resultarem em invasão, vazamento de informações ou outros impactos relevantes, ou ainda quando for considerado necessário.
    i. Essa reconstrução deverá ser realizada em ambiente controlado (sandbox) de propriedade e/ou sob gestão da CONTRATADA.
    ii. Quando aplicável, poderá ser utilizada a solução de sandbox disponibilizada pelo CONTRATANTE.
n. O Blue Team deverá registrar na ferramenta de gestão de incidentes as lições aprendidas, contribuindo para a formação de uma base de conhecimento institucional sobre ataques adversos, a ser continuamente expandida ao longo da vigência do contrato.
o. O processo aqui descrito constitui o mínimo esperado a ser seguido pela CONTRATADA. Contudo, considerando que o objeto deste documento caracteriza-se como serviço continuado, é esperado que a CONTRATADA proponha e implemente melhorias contínuas, as quais deverão ser previamente analisadas e aprovadas pelo CONTRATANTE.

X. Das Ferramentas

a. O Serviço de Gestão de Incidentes de Segurança deverá ser prestado pela CONTRATADA com o apoio de ferramenta própria de ITSM (IT Service Management).
b. Essa ferramenta deverá possibilitar a criação, registro, acompanhamento e encerramento de incidentes de segurança, assegurando a rastreabilidade de todas as etapas do tratamento.

c. A solução deverá gerir de forma estruturada todo o ciclo de vida dos incidentes de segurança, desde a abertura até a análise de lições aprendidas, incluindo documentação, comunicação com o TJES e geração de relatórios técnicos e executivos.

XI. Do Grupo de respostas a incidentes de segurança

a. O **Grupo de Resposta a Incidentes de Segurança (Blue Team)** deverá ser constituído de forma exclusiva para a execução das atividades relacionadas à resposta a incidentes, não sendo permitido que seus profissionais desempenhem funções em outros serviços previstos neste documento.
b. Todos os profissionais alocados a este grupo deverão, obrigatoriamente, integrar o quadro permanente de colaboradores da CONTRATADA, sendo vedada qualquer forma de terceirização ou subcontratação para a execução deste serviço.
c. Caberá à CONTRATADA dimensionar adequadamente o número de profissionais necessários para assegurar a entrega do serviço, devendo fazê-lo de modo a não comprometer os Acordos de Nível de Serviço (SLAs) estabelecidos e sem impor quaisquer custos adicionais à CONTRATANTE.

XII. Das Certificações grupo de resposta a incidente de segurança

a. A fim de assegurar que os profissionais envolvidos possuam o conhecimento técnico e a habilidade prática necessários para executar o processo de resposta a incidentes de segurança no âmbito do CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o Grupo de Resposta a Incidentes de Segurança (Blue Team) com, no mínimo:

Quantidades mínimas	Perfis	Certificações	Descrição	Tipo de Atuação

1 Perfil	Analista de Segurança I	Ao menos 02 (duas) pessoas com 01 (uma) das certificações a seguir (distintas): • ISC2 - CC - Certified in Cybersecurity • Certified Ethical Hacker – CEH® • CompTIA Cybersecurity Analyst(CySA+®) • GSEC® (GIAC Security Essentials); • ITCerts - CISA - Certified	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.	Remota

		Information Security Analyst		
2 Perfis	Analista de Segurança II	01 (uma) certificação obrigatória, por profissional: Certified Ethical Hacker GCIH ® (GIAC Incident Handler); CIA ® (Certified Intrusion Analyst); ITCerts - CISA - Certified Information Security Analyst	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 36 (trinta e seis) meses em segurança da informação.	Remota
2 Perfis	Analista de Segurança III	Mínimo de 01 (uma) certificação da solução a ser utilizada no serviço	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos	Remota

			utilizando ferramentas e soluções de SIEM. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.	

XIII. Dos Requisitos mínimos de formação técnica

a. Durante toda a vigência contratual, a CONTRATADA deverá assegurar que todos os profissionais alocados ao Grupo de Resposta a Incidentes de Segurança (Blue Team) mantenham, no mínimo, os seguintes requisitos:
   i. **Formação acadêmica**: diploma registrado de curso de nível superior em Tecnologia da Informação ou em qualquer outra área de graduação, desde que complementado por pós-graduação lato sensu em Tecnologia da Informação, com carga horária mínima de 360 (trezentas e sessenta) horas, expedida por instituição reconhecida pelo Ministério da Educação (MEC). Para efeito de comprovação da formação acadêmica, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025.
   ii. **Experiência profissional**: conhecimento avançado em segurança da informação, com experiência comprovada de, no mínimo, 06 (seis) meses em atividades relacionadas à resposta a incidentes de segurança da informação.

XIV. Dos Documentos comprobatórios de vínculo e formação técnica

a. Será exigido da CONTRATADA a apresentação da seguinte documentação referente aos profissionais designados para compor o Grupo de Resposta a Incidentes de Segurança (Blue Team), a fim de comprovar o atendimento integral às exigências e obrigações estabelecidas neste documento:
   i. Carteira de Trabalho e Previdência Social (CTPS), devidamente assinada pela CONTRATADA, ou documento equivalente para

comprovação do vínculo de pessoa física por meio de empresa individual;

ii. Curriculum Vitae atualizado, contendo a descrição detalhada das habilidades, experiências e qualificações profissionais;

iii. Certificações técnicas correspondentes, em cópia autenticada ou acompanhada dos originais para conferência, conforme mencionadas no currículo, como comprovação das competências técnicas exigidas.

XV. **Das entregas: Indicadores estratégicos de gestão de incidentes de segurança**

a. Para acompanhamento e avaliação do serviço prestado, a CONTRATANTE definiu um conjunto de Indicadores-Chave de Desempenho (KPIs), que deverão ser obrigatoriamente consolidados em um único relatório integrado, disponibilizado em tempo real e de forma online, por meio do Portal de Indicadores de Serviços de Segurança da CONTRATADA, conforme previsto em tópico específico deste documento, a saber:

Denominação	**Forma de cálculo**	**Filtro**	**Agrupador**	**Descrição**
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de incidentes que resultaram em comprometimento da segurança	Soma de incidentes abertos que resultaram em comprometimento da segurança	Incidentes com comprometimento	Incidentes com comprometimento	Número total de incidentes com comprometimento
Quantitativo de incidentes que tenham potencial de comprometer a segurança	Soma de incidentes que tenham potencial de comprometer a segurança	Incidentes com potencial	Incidentes com potencial	Número total de incidentes com potencial

Denominação	**Forma de cálculo**	**Filtro**	**Agrupador**	**Descrição**
Quantitativo de incidentes que não tenham potencial de comprometer a segurança	Soma de incidentes que não tenham potencial de comprometer a segurança	Incidentes sem potencial	Incidentes sem potencial	Número total de Incidentes sem potencial
TOP 10 – IP de destino de incidentes de segurança	Soma do número de incidentes por IP de destino	Incidentes abertos/tratados por IP de destino	IP de destino	TOP do número de incidentes por IP de destino
TOP 10 – Incidentes de segurança por origem	Soma do número de incidentes por origem	Incidentes abertos/tratados por origem	Origem	TOP do número de incidentes por origem interna ou externa
TOP 10 – Tipos de Incidentes	Soma do número de incidentes por tipo	Incidentes abertos/tratados por tipo	Tipo	TOP 10 por tipo de incidente
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de pacotes correlacionados	Soma de pacotes correlacionados	pacotes correlacionados	pacotes correlacionados	Número total de pacotes correlacionados

Denominação	**Forma de cálculo**	**Filtro**	**Agrupador**	**Descrição**
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes abertos	Número total de incidentes abertos
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos/pacotes correlacionados por regra de correlacionamento	Eventos e pacotes correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos e pacotes correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos e pacotes correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem

Denominação	**Forma de cálculo**	**Filtro**	**Agrupador**	**Descrição**
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos e pacotes correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

b. Os relatórios e indicadores definidos deverão ser apresentados e discutidos mensalmente, com base em dados consolidados, durante a Reunião Mensal de Alinhamento, prevista em tópico específico neste documento.
c. A apresentação ficará a cargo de profissional da CONTRATADA com perfil de Gerente de Projetos, conforme tópico específico neste documento, que detenha conhecimento abrangente sobre todos os serviços prestados no âmbito deste contrato, assegurando a clareza e a consistência das informações apresentadas ao CONTRATANTE.

1.4.2.3 Serviço de Gestão de Incidentes de Segurança - Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response - SOAR)

I. **Das Condições Gerais**

a. Este serviço tem como finalidade automatizar os processos e fluxos de trabalho relacionados às operações de segurança cibernética, assegurando maior eficiência e consistência na execução das atividades.
b. A automação deverá abranger tanto tarefas rotineiras quanto atividades complexas ou de difícil execução manual, reduzindo o tempo de resposta e mitigando riscos decorrentes de falhas humanas.
c. O serviço deverá ainda promover a orquestração integrada das diferentes ferramentas de segurança utilizadas no ambiente tecnológico do CONTRATANTE, garantindo que operem de forma coordenada, com mínima intervenção humana.

II. **Processo de Orquestração e Automação de Resposta a Incidentes**

a. O Serviço de Orquestração, Automação e Resposta (SOAR) deverá, no mínimo:
   i. consolidar dados e extrair informações relevantes de múltiplas fontes de inteligência e das tecnologias de segurança já existentes, assegurando sua integração e interação com todas as fontes de informação que compõem os Serviços Gerenciados de Segurança;
   ii. automatizar processos de segurança, visando reduzir o tempo de resposta às ameaças, eliminar desperdícios de recursos e promover maior eficiência operacional.
   iii. A CONTRATADA deverá operar este serviço de forma integrada à sua solução de software para a gestão da operação de segurança (SecOps), utilizando como insumos:
      1) as informações coletadas pelo Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Ataques Cibernéticos e Incidentes de Segurança;
      2) os resultados da análise e classificação de incidentes de segurança da informação;
      3) demais fontes externas de dados necessárias para uma atuação eficaz.
   iv. A solução SOAR deverá ser capaz de gerenciar e integrar-se de forma eficaz aos fluxos oriundos:
      1) dos processos de detecção e resposta a incidentes;
      2) da solução de SIEM;
      3) de incidentes relacionados à segurança da informação e privacidade.
   v. O processo deverá permitir a definição de fluxos abrangentes, que contemplem todas as fases do ciclo de vida de um incidente, desde o registro e triagem inicial até a resolução e prevenção, assegurando padronização, rastreabilidade e melhoria contínua.

III. **Ferramenta**

a. A CONTRATADA deverá fornecer a ferramenta e promover a automação de processos e fluxos de trabalho de forma interativa, prática e de fácil implementação, assegurando o atendimento às seguintes características mínimas:

i. Possibilidade de criação de, no mínimo, 100 (cem) playbooks;
ii. Disponibilizar interface web para administração de catálogo de serviços, níveis de serviço e dashboards de visualização;
iii. Fornecer informações em tempo real, de forma gráfica, por meio de dashboards;
iv. Incluir recursos gráficos de workflow, que permitam a criação de processos e rotinas operacionais de forma visual, ou dispor de workflow automatizado para resposta e gerenciamento de incidentes, possibilitando a execução automática de ações de criação, alteração, escalonamento, documentação e fechamento de incidentes;
v. Permitir o envio automático e agendado de relatórios e gráficos gerenciais, direcionados a grupos de usuários ou usuários específicos;
vi. Possuir componente próprio para a modelagem gráfica e automação de processos e fluxos de trabalho;
vii. Ser capaz de analisar e correlacionar eventos, viabilizando a automação de ações padronizadas, verificações de status, recursos de auditoria e medidas de fiscalização;
viii. Disponibilizar fluxos de trabalho pré-configurados, que possam ser customizados e ajustados de acordo com as necessidades do TJES, permitindo a automação de processos de resposta a incidentes cibernéticos;
ix. Possibilitar a automação de fluxos de trabalho diretamente na console, tanto a partir de templates pré-definidos pela solução, quanto de novos casos de uso criados sob demanda, sem necessidade de programação ou alteração do código-fonte;
x. Incluir ferramenta para criação de formulários, permitindo a definição de campos específicos para cada processo ou fluxo de trabalho, bem como a criação manual de playbooks, de modo a personalizar critérios de execução, inserção de informações e controles, também sem necessidade de programação ou alteração de código;
xi. Eliminar a necessidade de criação manual de tabelas, colunas e campos de banco de dados, ou de ajustes de código-fonte, garantindo que tais modificações ocorram de forma transparente aos operadores e administradores da solução;

xii. Permitir a criação de dashboards personalizados, possibilitando que cada usuário configure sua visualização de acordo com suas necessidades, igualmente sem necessidade de programação;

xiii. Garantir a integração da automação de processos com os demais controles de segurança em uso no ambiente do TJES;

xiv. Disponibilizar a edição dinâmica de relatórios em forma de gráficos gerenciais, exibidos nos painéis e dashboards da solução;

xv. Ser capaz de integrar-se a soluções de segurança de terceiros, a fim de permitir a execução de ações adicionais de bloqueio contra ataques cibernéticos;

xvi. Incluir funcionalidade nativa de automação e orquestração de respostas a eventos detectados, com integração à infraestrutura de segurança, contemplando dispositivos como firewalls, soluções de EDR, Active Directory, entre outros componentes relevantes.

IV. Indicadores estratégicos do Serviço de Orquestração

a. Para o acompanhamento e a avaliação dos serviços prestados, a CONTRATANTE estabeleceu um conjunto de Indicadores-Chave de Desempenho (KPIs).

b. Esses indicadores deverão ser reunidos em um relatório único e integrado, a ser disponibilizado de forma online e em tempo real, por meio do Portal de Segurança da CONTRATADA.

c. O relatório deverá contemplar métricas que permitam aferir a efetividade das ações executadas, a qualidade dos serviços entregues e o cumprimento dos níveis mínimos de serviço pactuados, a saber:

DENOMINAÇÃO	**FORMA DE CÁLCULO**	**FILTRO**	**AGRUPADOR**	**DESCRIÇÃO**
Quantitativa de Playbooks de Automação	Soma de playbooks configurados	Playbooks	Playbooks	Número total de playbooks configurados

		Configurados		
Quantitativo de playbooks acionados	Soma de playbooks acionados	Playbooks Acionados	Playbooks	Número total de playbooks acionaodos
Eficiência dos playbooks acionados	Percentual de playbboks que obtiveram sucesso na contenção do incidente em relação ao total de acionamentos	Playbooks eficientes	Playbooks	Número total de playbooks efetivos

d. Os relatórios e indicadores de desempenho deverão ser apresentados e discutidos mensalmente na Reunião de Alinhamento, conforme previsto neste documento.
e. A apresentação será realizada por profissional da CONTRATADA com perfil de Gerente de Projetos, e que detenha conhecimento abrangente sobre todos os serviços prestados no âmbito contratual, garantindo a consistência e a completude das informações repassadas ao CONTRATANTE.

V. **Grupo Técnico de Serviço de Gerenciamento da Orquestração e Automação de Resposta a incidentes**

a. Os serviços previstos para este grupo deverão ser executados pela mesma equipe de profissionais alocada ao Grupo Técnico descrito no de Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Ataques Cibernéticos e Incidentes de Segurança, observando-se, em especial, o item que trata do perfil de Analista de Segurança III.
b. Caberá a este profissional desempenhar as atividades específicas associadas a este grupo de serviços, em conformidade com os requisitos

estabelecidos neste documento, assegurando a continuidade, a uniformidade e a qualidade técnica da execução contratual.

1.4.2.4 Serviço de Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)

I. O serviço tem como finalidade realizar o monitoramento contínuo e ininterrupto de termos e ativos digitais acessíveis em ambientes públicos da internet, abrangendo as camadas de superfície (surface web), profunda (deep web) e oculta (dark web).
   a. O monitoramento deverá contemplar, no mínimo, canais de fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensagens, lojas de aplicativos, feeds, campanhas de phishing, práticas de typosquatting, redes sociais, serviços de vídeo streaming, páginas de comércio eletrônico e referências a vítimas de malwares.
   b. Os eventos identificados deverão ser processados, organizados e enriquecidos, resultando em informações estruturadas e úteis ao negócio do CONTRATANTE.
   c. O serviço deverá obedecer a um processo cíclico de refinamento e enriquecimento de dados de riscos digitais, assegurando atualização contínua e relevância das informações geradas.
   d. Para tanto, a CONTRATADA deverá dispor de equipe especializada em investigação proativa (*threat hunting*), inteligência de ameaças cibernéticas (*threat intelligence*) e serviços de remoção de conteúdos ilícitos ou infratores (*takedown services*), de forma a garantir a proteção efetiva da presença digital do CONTRATANTE.

II. **Ferramenta**

   a. **Coleta e Processamento de Dados**
      i. A solução deverá dispor de plataforma web segura, capaz de coletar, organizar, contextualizar e enriquecer eventos de riscos digitais de forma automática, em larga escala, sem necessidade de intervenção humana.
      ii. A CONTRATADA deverá dispor de equipe especializada em inteligência de ameaças cibernéticas, responsável por gerar novos contextos, realizar remoção de conteúdo, criar e revisar regras,

aprovar processos, automatizar fluxos e promover melhoria contínua da plataforma.

iii. A solução deverá identificar, coletar, processar e organizar informações, de forma automatizada e manual, em: chats, redes sociais, páginas da internet superficial, profunda e oculta, fóruns, repositórios de textos e códigos, aplicativos de mensagens, lojas de aplicativos, páginas de comércio eletrônico, entre outras fontes acessíveis.

iv. Deverá realizar coleta diária de informações de, no mínimo, 60 fontes externas de inteligência em categorias como phishing, códigos secretos, chaves, senhas, propriedade intelectual, vítimas de malwares, botnets, deep web, perfis falsos, typosquatting, aplicativos falsos em marketplaces, citações à marca, BINs de cartões de crédito, APIs expostas, documentos confidenciais e vazamento de dados.

v. As informações coletadas deverão ser processadas em plataforma de suporte a grandes volumes de dados, com mecanismos de normalização e enriquecimento de contexto.

b. **Configuração e Visualização**

i. A solução deverá permitir alteração simples e ágil dos critérios de busca, mediante filtros e coletores.

ii. Deverá fornecer painel de visualização das informações coletadas, com possibilidade de buscas avançadas

iii. Deverá permitir a visualização de perfis relacionados a palavras-chave, realização de buscas nos dados, incluindo buscas avançadas com critérios e entidades diferentes;

iv. Deve permitir a navegação interativa, com apresentação das informações relacionadas.

v. Os dados filtrados deverão ser apresentados em painéis dinâmicos que exibam as principais fontes identificadas.

vi. Deverá possibilitar a exportação das informações em relatórios nos formatos PDF, CSV ou JSON.

vii. As pesquisas deverão apresentar dados por contexto, metadados e tipo de fonte.

viii. A solução deverá integrar-se por API/REST com plataformas terceiras, alimentando sistemas externos com os eventos coletados.
ix. Deve ser capaz de identificar a emissão e criação de domínios suspeitos ou similares (*typosquatting*), assim como certificados digitais associados.
x. Deve realizar pesquisas sobre marcas, executivos, domínios e BINs.
xi. A ferramenta deverá possuir capacidade de análise de imagens para detecção de abusos de marca, conforme modelos fornecidos pelo TJES.
xii. Todas as ocorrências deverão conter descrição, recomendação e avaliação do impacto.
xiii. Deve suportar regras avançadas baseadas em expressões regulares e padrões binários (YARA).
xiv. Os termos monitorados deverão ser apresentados em área dedicada no portal, com possibilidade de edição ou remoção.
xv. A solução deverá detectar páginas de phishing ativas e validar domínios suspeitos em repositórios específicos.

c. **Coleta e Monitoramento de Fontes**

i. Deverá incluir coleta em sites, redes sociais e aplicativos, como Twitter, Facebook, YouTube, Instagram, LinkedIn, Discord, Telegram, IRC, Pastebin, Apple Store, Google Play e GitHub.
ii. A solução deverá possuir métodos de coleta pré-existentes em internet superficial, profunda e oculta.
iii. Deverá informar anomalias em registros de domínios (Whois, DNS).
iv. Monitorar BINs de cartões de crédito do TJES em canais de fraude e mensagerias.
v. Realizar análise de áudio em, no mínimo, três plataformas de mensagens, com transcrição autônoma quando identificado conteúdo relevante.
vi. Realizar análise de conteúdo em imagens para identificar riscos digitais relacionados ao TJES.
vii. Identificar, disponibilizar e possibilitar a análise de trechos anteriores e posteriores dos textos capturados, sendo possível identificar a origem e o desdobramento do(s) assunto(s) pesquisado(s), de acordo

com as necessidades do TJES. Caso a ferramenta não realize a análise de forma autônoma, será aceito que tal análise seja realizada pela equipe da CONTRATADA, especializada no processo investigativo;

viii. Atuar em canais de hacktivismo, fraudes e crimes cibernéticos, incluindo Telegram, IRC e Discord.

ix. A solução deverá possuir foco em fontes de conteúdo nacionais e relevantes, com capacidade de identificar grupos de fraudadores do sistema financeiro brasileiro, esquemas voltados à burla de sistemas de e-commerce, portais de pagamento, além da comercialização de dados de pessoas físicas e informações bancárias.

x. Deverá possibilitar a inclusão e o monitoramento contínuo de novos grupos em aplicativos de mensageria, de acordo com as necessidades do CONTRATANTE.

xi. Será obrigatória a extração de metadados de cada mensagem coletada, contemplando: autor, aplicativo de origem, data e hora de envio e data e hora de coleta, com precisão de segundos.

xii. A solução deverá realizar monitoramento das principais redes sociais do mercado, abrangendo, no mínimo, Twitter, Instagram, YouTube, LinkedIn, TikTok e Facebook.

xiii. Deverá monitorar, no mínimo, a rede de compartilhamento de textos Pastebin e as plataformas de compartilhamento de códigos GitHub, GitLab e Bitbucket, incluindo análise estática de código.

xiv. Deverá contemplar o monitoramento de buckets em nuvens públicas, no mínimo AWS S3 e Azure Blob, a fim de identificar informações ou arquivos confidenciais e sensíveis.

xv. A solução deverá identificar credenciais comprometidas associadas às marcas do TJES, obtidas por malwares do tipo Trojan Stealers e RATs (Remote Access Trojans).

xvi. Deverá possuir recurso de monitoramento de páginas de referência, com utilização de código JavaScript para detecção proativa de phishing e identificação de sites falsos.

xvii. A CONTRATADA deverá garantir sigilo absoluto e confidencialidade sobre todos os serviços prestados, sendo vedada a divulgação, total

ou parcial, de informações ou documentos aos quais venha a ter acesso em razão da execução contratual.

d. **Remoção de Conteúdo Infrator**

i. O serviço de remoção de conteúdo infrator deverá possibilitar a retirada do ar de sites maliciosos, páginas de phishing ou domínios que utilizem o nome, a marca ou a imagem do TJES, mesmo que de forma similar, em conformidade com o quantitativo contratado.

ii. Também deverá contemplar a remoção de perfis falsos de funcionários, executivos ou da própria instituição em redes sociais, assim como a exclusão de quaisquer tipos de informação disponíveis e acessíveis que violem direitos de uso do TJES ou permitam a burla de mecanismos de proteção estabelecidos.

iii. O escopo inclui, ainda, a retirada de conteúdos que representem ataques à reputação institucional ou tentativas de captura de credenciais, bem como a exclusão de informações relacionadas ao TJES publicadas em redes sociais como Facebook, Twitter, LinkedIn, Instagram, YouTube e outras plataformas, sem a devida autorização da instituição.

iv. Deverá abranger a remoção de aplicativos falsos e maliciosos distribuídos em lojas digitais de dispositivos móveis, como Google Play Store e Apple Store, além de documentos, informações confidenciais, dados de cartões de crédito, divulgações relacionadas a produtos, sistemas ou colaboradores do TJES. Inclui, ainda, o monitoramento de sites de compartilhamento de arquivos e textos, como Pastebin, Ghostbin e equivalentes.

v. A plataforma disponibilizada pela CONTRATADA deverá oferecer conexão segura por meio do protocolo HTTPS, permitir a abertura de chamados a partir de referências de eventos e realizar a busca de contexto sobre o TJES em menções envolvendo marca, domínios, BINs, VIPs e IPv4.

vi. A CONTRATADA deverá possuir mecanismos próprios para monitoramento das principais redes sociais e lojas de aplicativos, bem como prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, verificando o uso indevido da

marca do TJES em nomes de domínio ou URLs, com indicação da entidade registradora e dos dados proprietários do domínio.

vii. Deverá ainda atender às solicitações do TJES para inclusão de novas palavras-chave ou listas de termos relacionados ao contexto institucional, sempre que demandado, para elaboração de parâmetros de busca. Além disso, será responsável por emitir alertas atualizados sobre o andamento de cada processo de remoção de conteúdo infrator.

viii. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências, tanto em andamento quanto finalizadas, permitindo filtros por período, categorias e outros critérios relevantes. A plataforma deverá estar disponível em formato multi-idioma, no mínimo em português (Brasil) e inglês, cabendo à CONTRATADA a tradução de relatórios que não estejam originalmente em português.

ix. Por fim, a solução deverá oferecer alertas diversificados e customizados, com segmentação por categorias, tipo de eventos e níveis de risco, sendo disponibilizados, no mínimo, por API, e-mail e SMS.

e. **Ambiente de monitoramento:**

ITEM	DESCRIÇÃO	ATIVOS	QUANTIDADE
01 - A	Monitoramento de Surface web, deep web e dark web	Pessoas de interesse	1200
01 - B	Monitoramento de Surface web, deep web e dark web	Pessoas VIP	800
02	Monitoramento de Surface web, deep web e dark web	Produtos e Marcas	15
03	Sites e contas fraudulentas	Takedown por ano	60

04	Monitoramento de fontes de informações	Domínios e Subdomínios	15
05	Monitoramento de vazamento de informações	Nomes de empresas fornecedoras	100

III. Processo de monitoramento e visibilidade de ataques cibernéticos

a. A CONTRATADA deverá implantar solução de análise avançada de logs e pacotes de rede, assegurando sua operação, administração e sustentação, bem como a implementação de melhorias contínuas durante todo o período de vigência contratual.
   i. A solução deverá contemplar a criação e manutenção de regras específicas voltadas à identificação de ataques direcionados ao ambiente tecnológico do TJES, garantindo agilidade na resposta e mitigação de riscos à infraestrutura de TIC.
   ii. Será igualmente atribuição da CONTRATADA desenvolver parsers que possibilitem a integração entre as ferramentas de segurança já existentes, assegurando interoperabilidade, padronização de dados e uma visão consolidada da postura de segurança institucional.
   iii. Para fins de acompanhamento técnico e gerencial, caberá também à CONTRATADA a criação de dashboards e relatórios customizados, permitindo análises detalhadas em diferentes níveis, de caráter tanto operacional quanto executivo.
   iv. A manutenção da solução implicará ainda na responsabilidade da CONTRATADA de realizar a abertura de chamados técnicos junto ao fabricante ou fornecedor sempre que necessário, de forma a garantir a aplicação de correções, atualizações de versões e suporte adequado aos componentes da ferramenta, sem prejuízo à continuidade dos serviços.
b. Adicionalmente, a CONTRATADA será responsável pela implantação, operação e suporte de ferramenta dedicada ao monitoramento de ameaças em ambientes de Deep Web e Dark Web.

c. Esse recurso deverá viabilizar a detecção de riscos externos, identificar indícios de fraudes, campanhas maliciosas e outros comportamentos adversos, ampliando a capacidade preventiva do TJES e fortalecendo a sua resiliência frente a ameaças cibernéticas emergentes.

IV. Classificação dos Eventos

a. Para o sucesso de um processo de monitoramento de ataques cibernéticos, é indispensável a definição prévia dos tipos de eventos de segurança que deverão ser identificados e tratados. Nesse sentido, a primeira responsabilidade da CONTRATADA consiste no estabelecimento de uma linha de base de eventos a serem monitorados, a qual servirá como referência para detecção e ação diante de ocorrências relevantes.
b. A definição dessa linha de base não poderá ser realizada de forma unilateral pela CONTRATADA. O CONTRATANTE deverá participar ativamente do processo, em caráter consultivo, assegurando alinhamento entre as necessidades institucionais e as práticas operacionais adotadas. Contudo, permanece sob responsabilidade da CONTRATADA a efetiva implementação e manutenção da linha de base de eventos de segurança monitorados.
c. Espera-se que a linha de base seja revisada periodicamente, no mínimo em ciclos mensais, de modo a refletir a constante evolução do cenário de ameaças. Entretanto, tal revisão não deve se restringir a esse intervalo, considerando que novos vetores de ataque surgem diariamente. É dever da CONTRATADA manter-se atualizada quanto a essas novas ameaças, promovendo a devida atualização da linha de base para que, caso sejam direcionadas ao ambiente do CONTRATANTE, possam ser detectadas tempestivamente pelos serviços contratados.
d. O produto final de um evento de segurança decorre da correlação entre os insumos coletados, tais como logs e pacotes de rede, originados dos diversos itens de configuração que compõem o parque tecnológico do CONTRATANTE. Uma vez definida a linha de base, caberá à CONTRATADA verificar se todos os insumos necessários para a correta geração dos eventos estão sendo devidamente encaminhados para a solução de monitoramento.
e. Se for identificada a ausência de insumos - como logs ou pacotes de rede - em determinado item de configuração, será obrigação da CONTRATADA

realizar a correção ou habilitação necessária, sempre que tais ativos estiverem contemplados no objeto contratual. Nos casos em que o item de configuração não esteja inserido no escopo do contrato, mas seja essencial para a correta geração do evento, a CONTRATADA deverá notificar formalmente o CONTRATANTE para que providencie a adequação.

f. Superada a fase de coleta e validação de insumos, dar-se-á início ao processo de classificação dos eventos, também sob responsabilidade da CONTRATADA. O grupo de monitoramento deverá concentrar suas ações nos eventos mais significativos, analisando e classificando-os em três categorias principais:
    i. **Eventos de Informação**: São eventos que não exigem ação imediata, tendo como objetivo verificar a funcionalidade dos itens de configuração de segurança. Servem para confirmar se ferramentas e soluções estão operando conforme esperado, além de subsidiar a geração de estatísticas, como a taxa de atualização de vacinas de antivírus em estações de trabalho.
    ii. **Eventos de Aviso**: Referem-se a situações em que há comportamento anômalo quando comparado à linha de base do ambiente, sem que ainda tenha ocorrido impacto direto nos serviços ou infraestrutura. Um exemplo seria a elevação súbita no volume de tentativas de port scan, passando de mil para dez mil em uma hora, embora os mecanismos de defesa (como *firewalls*) continuem bloqueando tais tentativas sem prejuízo à performance.
    iii. **Eventos de Exceção**: Corresponde a ocorrências que indicam impacto efetivo nos pilares da segurança da informação — confidencialidade, integridade, disponibilidade e privacidade. Um exemplo seria uma infecção por *ransomware* não bloqueada pelas soluções antivírus da CONTRATANTE. É este o único tipo de evento capaz de acionar o processo formal de resposta a incidentes de segurança da informação, conforme disciplinado neste documento.

V. **Resposta aos eventos**

a. Uma vez concluída a etapa de classificação, inicia-se o processo de resposta, cuja responsabilidade recai integralmente sobre a CONTRATADA.

b. As ações de resposta devem ser conduzidas conforme a categoria atribuída ao evento, de modo a assegurar que cada ocorrência seja tratada de forma proporcional ao risco envolvido, a saber:

   i. **Eventos do tipo Informação**: Não demandam ações corretivas ou de mitigação. Entretanto, como já previsto neste documento, esses eventos têm caráter essencial para a verificação do funcionamento adequado das soluções de segurança em operação. Assim, espera-se que a CONTRATADA utilize tais registros para validar continuamente a eficácia dos controles implementados e assegurar sua plena operacionalidade.

   ii. **Eventos do tipo Aviso**: Exigem acompanhamento humano direto. Nessa situação, deve haver a garantia de que um analista do grupo de monitoramento esteja validando o evento em tempo hábil, verificando se há indícios de evolução para um evento do tipo Exceção. Cabe a esse profissional analisar a anomalia, investigar a causa raiz do comportamento atípico do ambiente e tomar as providências cabíveis para mitigar potenciais riscos antes que causem impacto efetivo.

   iii. **Eventos do tipo Exceção**: Devem ser obrigatoriamente tratados como incidentes de segurança. A CONTRATADA deverá, nesses casos, proceder com a abertura de registro na ferramenta de gestão de incidentes do CONTRATANTE, observando os critérios definidos no processo de resposta a incidentes de segurança da informação. Uma vez realizada a abertura e devidamente registrado o incidente, encerra-se a participação do grupo de monitoramento, passando o tratamento subsequente às equipes responsáveis pela resposta formal ao incidente.

VI. Encerramento do Evento

a. O encerramento dos eventos constitui a etapa final do processo de monitoramento e resposta, sendo de inteira responsabilidade da CONTRATADA. Após a execução das ações corretivas ou mitigatórias cabíveis, cada evento deverá ter seu status atualizado na ferramenta de gestão, passando de “aberto” para “encerrado”.

b. É fundamental que todo o ciclo de tratamento, independentemente da fase em que o evento se encontre, seja devidamente documentado no módulo de tratamento da ferramenta da CONTRATADA. Esse registro deve conter informações completas e consistentes, assegurando rastreabilidade e transparência em todas as etapas do processo.
c. Cabe destacar que a integridade desses registros é de responsabilidade da CONTRATADA, sendo expressamente vedada a exclusão de qualquer evento, independentemente de sua classificação ou fase de tratamento. A preservação integral dos dados é requisito essencial para auditoria, conformidade regulatória e lições aprendidas.
d. Por fim, ressalta-se que o processo aqui descrito representa o mínimo esperado em termos de execução. Considerando que o serviço contratado possui caráter continuado, a CONTRATADA deverá adotar práticas de melhoria contínua, podendo propor ajustes e evoluções que aprimorem a eficiência e a eficácia do processo, desde que previamente aprovados pelo CONTRATANTE.

VII. Grupo de monitoramento de ataques cibernéticos

a. Os Serviços de Monitoramento de Ataques Cibernéticos poderão ser prestados pela mesma equipe de profissionais já alocada para o grupo técnico responsável pela gestão de vulnerabilidades, desde que respeitados os perfis e qualificações exigidos para ambas as funções.
b. Todos os profissionais designados para compor o Grupo de Monitoramento de Ataques devem, obrigatoriamente, integrar o quadro de colaboradores da CONTRATADA, sendo vedada qualquer forma de terceirização ou subcontratação deste serviço. Essa exigência visa assegurar a continuidade, a confiabilidade e a confidencialidade das atividades desempenhadas.
c. Caberá à CONTRATADA o adequado dimensionamento da equipe, garantindo número suficiente de profissionais para a execução integral das atribuições, de forma a não comprometer os níveis mínimos de serviço pactuados e assegurar o pleno atendimento aos requisitos de disponibilidade e qualidade estabelecidos no contrato.

VIII. Certificações do Grupo de Monitoramento de Ataques

a. A fim de assegurar que os profissionais envolvidos possuam o conhecimento e a qualificação necessários para a execução eficaz do processo de monitoramento de ataques cibernéticos no ambiente do CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o Grupo de Monitoramento de Ataques com, no mínimo, o perfil profissional listado a seguir:

Perfis	Certificações	Descrição	Tipo de Atuação
Analista Threat Intelligence I	Certified Threat Intelligence Analyst (CTIA)	Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.	Remota

IX. Requisitos mínimos de formação técnica

a. Durante a execução dos serviços, a CONTRATADA se obriga a manter todos os profissionais do Grupo de Monitoramento de Ataques em conformidade com os seguintes requisitos:

i. **Formação acadêmica:** diploma devidamente registrado de curso de nível superior em Tecnologia da Informação ou em qualquer outra área, desde que complementado por certificado de pós-graduação em Tecnologia da Informação, com carga horária mínima de 360 (trezentas e sessenta) horas, emitido por instituição reconhecida pelo Ministério da Educação (MEC). Para efeito de comprovação, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025;

ii. Conhecimento avançado em Segurança da Informação, com experiência comprovada de, no mínimo, 06 (seis) meses em

atividades de monitoramento de ataques cibernéticos, utilizando ferramentas e soluções de SIEM (Security Information and Event Management) e ATD (Advanced Threat Detection), assegurando atuação alinhada às melhores práticas de mercado.

X. **Documentos comprobatórios de vínculo e formação técnica**

a. Será exigido da CONTRATADA a apresentação das seguintes documentações dos profissionais designados para compor o Grupo de Monitoramento de Ataques, a fim de comprovar o atendimento às exigências e obrigações estabelecidas neste documento:

i. Comprovação de vínculo empregatício formal com a CONTRATADA;
ii. Curriculum vitae atualizado, contendo a descrição das experiências e habilidades técnicas relevantes;
iii. Cópia das certificações técnicas exigidas e mencionadas no currículo, que comprovem a qualificação e o conhecimento do profissional para execução das atividades previstas.

XI. **Indicadores estratégicos de monitoramento de ataques cibernéticos**

a. Para fins de acompanhamento e avaliação do serviço de monitoramento de ataques cibernéticos a ser prestado pela CONTRATADA, o CONTRATANTE estabeleceu indicadores-chave de desempenho que deverão ser observados e reportados.

b. Esses indicadores serão consolidados em um único relatório, entregue de forma online e em tempo de execução, por meio do Portal de Segurança da CONTRATADA, garantindo visibilidade contínua e transparente sobre a execução dos serviços contratados, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativa de Menções	Soma de menções detectadas	Menções detectadas	DRP	Número total de menções detectadas

Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	DRP	Número total de incidentes abertos
Quantitativo de takedown realizados	Soma de takedown realizados	Takedown	DRP	Número total de Takedown realizados

c. Tais relatórios e indicadores deverão ser apresentados e discutidos na Reunião Mensal de Alinhamento, prevista neste documento, ocasião em que serão consolidados os dados referentes ao período anterior e analisados os resultados alcançados frente aos níveis de serviço pactuados.
d. A reunião contará com a presença obrigatória de profissional alocado pela CONTRATADA no perfil de Gerente de Projetos, devidamente qualificado e com pleno conhecimento de todos os serviços prestados, de modo a esclarecer dúvidas, detalhar ocorrências e propor eventuais ações corretivas ou de melhoria contínua.

1.4.2.6 Serviço de Gestão de Patches (*Patch Management*)

I. **Das Condições Gerais**

a. O serviço de Gestão de Patches tem como finalidade garantir que todos os sistemas, aplicações e dispositivos integrantes da infraestrutura de Tecnologia da Informação e Comunicação (TIC) do TJES permaneçam continuamente atualizados, em conformidade com as correções de segurança e atualizações disponibilizadas pelos fabricantes.
b. A atualização sistemática por meio da aplicação de patches de segurança constitui prática essencial para a mitigação de vulnerabilidades conhecidas e para a redução da superfície de ataque do ambiente institucional. Esse processo visa assegurar a proteção contra exploração por agentes maliciosos, preservando a integridade, a disponibilidade e a confidencialidade dos serviços digitais críticos para a atividade jurisdicional.

II. **Do Escopo do Serviço**

a. O serviço de Gestão de Patches compreenderá um conjunto de atividades estruturadas e contínuas, voltadas para assegurar a atualização adequada de todos os sistemas, aplicações e dispositivos do TJES. As ações previstas abrangem desde a identificação das atualizações até a verificação pós-implantação, garantindo segurança, estabilidade e conformidade do ambiente tecnológico, como:

   i. **Identificação de Patches**: Realizar o monitoramento constante das atualizações de segurança disponibilizadas pelos fabricantes de sistemas operacionais, aplicações e dispositivos utilizados pelo TJES, incluindo patches, hotfixes e service packs.
   ii. **Avaliação de Patches:** Efetuar análise criteriosa da relevância e do impacto de cada atualização identificada, levando em consideração a criticidade dos ativos envolvidos e as vulnerabilidades que se pretende corrigir.
   iii. **Planejamento de Implantação:** Elaborar planos detalhados para implantação, contemplando cronogramas, definição de janelas de manutenção e procedimentos formais de rollback em caso de falhas ou incompatibilidades.
   iv. **Testes de Patches:** Executar testes prévios em ambiente controlado, com o objetivo de validar a compatibilidade e a estabilidade das atualizações antes de sua aplicação em ambiente de produção.
   v. **Implantação de Patches**: Realizar a aplicação planejada das atualizações em sistemas, aplicações e dispositivos do TJES, observando as melhores práticas de segurança e gestão de mudanças.
   vi. **Verificação Pós-Implantação**: Confirmar a efetividade das atualizações aplicadas, verificando se os sistemas permanecem funcionais, íntegros e livres das vulnerabilidades corrigidas.
   vii. **Relatórios e Documentação:** Elaborar relatórios periódicos que demonstrem o status das atualizações implantadas, vulnerabilidades mitigadas, possíveis desvios e problemas encontrados. Manter documentação consolidada e atualizada de todos os procedimentos e histórico de patches aplicados.

III. Do Processo de Gestão de Patches

a. O processo de gestão de patches será conduzido de forma estruturada, contemplando desde a identificação e análise das atualizações até a sua verificação final em ambiente de produção. A execução caberá integralmente à CONTRATADA, em conformidade com as boas práticas de segurança e governança de TIC, assegurando que todos os ativos do TJES permaneçam atualizados e protegidos contra vulnerabilidades conhecidas. As atividades deverão contemplar, no mínimo:

   i. **Descoberta e Análise:** A CONTRATADA deverá empregar ferramentas e métodos específicos para a descoberta contínua de novos patches e atualizações de segurança, aplicáveis a todos os equipamentos relacionados no documento que elencam os ativos do TJES , que poderá ser obtido quando ocorrer a visita técnica. A análise inicial deverá considerar a vulnerabilidade corrigida, a classificação de severidade conforme CVSS v3.1 (quando aplicável) e o impacto potencial da atualização no ambiente tecnológico do TJES.
   ii. **Classificação e Priorização:** Cada patch identificado será classificado segundo o nível de severidade (Crítica, Alta, Média ou Baixa) e a relevância do ativo afetado. As atualizações categorizadas como Críticas ou Altas deverão receber tratamento preferencial, com execução em caráter prioritário para reduzir o tempo de exposição a riscos.
   iii. **Planejamento e Agendamento:** A implantação seguirá plano formalmente elaborado pela CONTRATADA, contendo a lista de ativos a serem atualizados, as janelas de manutenção e os procedimentos de contingência. O plano deverá ser submetido previamente à aprovação do TJES. Atividades que possam implicar indisponibilidade de serviços deverão ser realizadas fora do horário regular de expediente, preferencialmente em finais de semana, sem custos adicionais para a CONTRATANTE.
   iv. **Testes e Aprovação:** Antes da aplicação em ambiente produtivo, os patches deverão ser submetidos a testes em ambiente de homologação ou em subconjunto representativo de ativos. Esses testes visam assegurar compatibilidade, estabilidade e ausência de regressões. Os resultados obtidos deverão ser apresentados ao TJES, que deliberará sobre a autorização para implantação.

v. **Implantação:** A execução das atualizações será realizada diretamente pela equipe técnica da CONTRATADA, observando o plano aprovado. Nos casos em que o gerenciamento do ativo seja de responsabilidade da equipe interna do TJES, a CONTRATADA deverá atuar em conjunto, realizando as devidas aberturas de chamados no sistema oficial de gestão de serviços de TI da instituição.

vi. **Verificação e Relato:** Após a aplicação, a CONTRATADA deverá realizar a verificação da efetividade da atualização, confirmando a instalação correta do patch e a plena funcionalidade dos sistemas impactados. Deverá ainda ser elaborado relatório de conformidade contendo os patches aplicados, as vulnerabilidades eliminadas e eventuais observações ou não conformidades encontradas.

IV. Das Ferramentas para Gestão de Patches

a. A CONTRATADA deverá adotar e integrar, quando aplicável, a solução já existente do TJES com ferramentas consolidadas de mercado voltadas à gestão de patches, sendo que, de forma preferencial, será usada a ferramenta do TJES e, alternativamente, caso esta não atenda aos requisitos mínimos de funcionamento, será utilizada a ferramenta da CONTRATADA.

b. A solução também deverá encaminhar os seguintes dados tanto para o SIEM do TJES quanto para o SIEM implementado pela CONTRATADA:

i. **Inventário de Ativos:** Manter inventário permanentemente atualizado, contemplando sistemas operacionais, aplicações, dispositivos de rede e demais ativos do ambiente tecnológico do TJES.

ii. **Varredura de Vulnerabilidades:** Integrar mecanismos de varredura que permitam identificar a ausência de atualizações críticas e a presença de vulnerabilidades conhecidas, de modo a subsidiar a priorização e o planejamento da aplicação de patches.

iii. **Automação de Processos:** Oferecer recursos de automação para todo o ciclo de gestão de patches, incluindo etapas de download, testes em ambiente controlado e implantação em produção.

iv. **Agendamento Flexível:** Possibilitar o agendamento de implantações de forma granular, considerando janelas de manutenção previamente

estabelecidas, bem como a segmentação por grupos de ativos ou criticidade do serviço.

v. **Rollback:** Disponibilizar mecanismos de reversão que permitam restaurar o estado anterior do sistema em situações de falhas ou impactos não previstos decorrentes da aplicação de patches.

vi. **Relatórios e Dashboards:** Fornecer relatórios detalhados sobre o status das atualizações, vulnerabilidades corrigidas, conformidade com políticas internas e pendências detectadas. Os dados deverão ser apresentados em dashboards dinâmicos e personalizáveis, de modo a atender tanto às necessidades técnicas quanto gerenciais.

vii. **Suporte Multiplataforma:** Garantir compatibilidade com os principais sistemas operacionais (Windows, Linux), bancos de dados corporativos (Oracle, SQL Server, MySQL, PostgreSQL, MongoDB) e aplicações críticas em uso pelo TJES.

viii. **Integração com SIEM:** Permitir a integração nativa dos logs e eventos gerados pelo processo de patch management com a solução de SIEM adotada pelo TJES, assegurando a correlação dos eventos de atualização com demais alertas de segurança monitorados.

V. Do Grupo Técnico do Serviço de Gestão de Patches

a. O grupo destinado à execução do serviço de gestão de patches deverá atuar de forma exclusiva, sendo vedada a utilização dos profissionais nele alocados em outros serviços abrangidos no presente documento.

b. Todos os integrantes desse grupo deverão obrigatoriamente compor o quadro funcional da CONTRATADA, não sendo permitida a terceirização ou subcontratação das atividades relacionadas.

c. Caberá à CONTRATADA dimensionar adequadamente a quantidade de profissionais necessários para a execução das tarefas, de modo a assegurar a plena continuidade do serviço e evitar qualquer impacto no cumprimento dos acordos de nível de serviço estabelecidos.

VI. Das Certificações do Grupo Técnico de Gestão de Patches

a. Com o objetivo de assegurar que os profissionais designados tenham efetiva competência técnica para conduzir o processo de gestão de patches no ambiente do TJES, a CONTRATADA deverá compor o Grupo Técnico de

Gestão de Patches com, no mínimo, um (01) profissional no perfil de Analista de Segurança.

i. Este profissional deverá possuir, obrigatoriamente, ao menos duas certificações técnicas dentre as relacionadas a seguir:

Perfis	**Certificações**	**Descrição**
Analista de Segurança	CompTIA Security+® ITCerts ITC-015 - Vulnerability Management Foundation Microsoft Certified: Azure Security Engineer Associate, Red Hat Certified Engineer (RHCE) ou Linux Professional Institute Certification (LPIC) Nível 2 ou superior.	Conhecimento avançado em gestão de patches e vulnerabilidades, com experiência comprovada de no mínimo 12 (doze) meses em ambientes corporativos de médio a grande porte. Capacidade de atuar proativamente na mitigação de vulnerabilidades.

VII. Dos Requisitos Mínimos de Formação Técnica

a. Durante a vigência contratual, a CONTRATADA deverá assegurar que todos os profissionais alocados para a execução do serviço de gestão de patches mantenham, de forma contínua, a seguinte qualificação mínima:

i. **Formação acadêmica**: diploma de curso de graduação em Tecnologia da Informação, devidamente registrado, ou diploma de graduação em qualquer área, desde que complementado por certificado de pós-graduação em Tecnologia da Informação, com carga horária mínima de 360 (trezentos e sessenta) horas, emitido por instituição reconhecida pelo Ministério da Educação (MEC). Para efeito de comprovação, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025.

ii. **Experiência e conhecimento técnico**: comprovação de conhecimento avançado em segurança da informação, com atuação prévia de, no mínimo, 6 (seis) meses em atividades de gestão de patches e administração de vulnerabilidades, devidamente demonstrada em documentação hábil.

VIII. Dos Documentos Comprobatórios de Vínculo e Formação Técnica

a. Será exigido da CONTRATADA a apresentação da documentação comprobatória referente aos profissionais que comporão o Grupo Técnico de Gestão de Patches, de modo a assegurar o atendimento integral das exigências e obrigações estabelecidas neste documento. Para tanto, deverão ser apresentados, no mínimo:

i. Carteira de Trabalho devidamente assinada pela CONTRATADA, comprovando o vínculo empregatício formal;
ii. Curriculum Vitae atualizado, com descrição das habilidades técnicas, experiências profissionais e certificações pertinentes;
iii. Cópias dos certificados técnicos mencionados no Curriculum Vitae, a fim de demonstrar o conhecimento declarado e validar as qualificações exigidas.

IX. Das Entregas: Indicadores Estratégicos de Gestão de Patches

a. Para acompanhamento e avaliação da execução contratual, o CONTRATANTE estabeleceu indicadores-chave de desempenho que deverão ser monitorados pela CONTRATADA. Esses indicadores serão consolidados em um único relatório integrado, disponibilizado em tempo real e de forma online, por meio do Portal de Indicadores de Serviços de Segurança da CONTRATADA, conforme descrito neste documento.

Denominação	**Forma de Cálculo**	**Filtro**	**Agrupador**	**Descrição**
Percentual de Ativos com Patches Atualizados	(Total de Ativos Atualizados / Total de Ativos em Escopo) x 100	Por tipo de ativo, por sistema operacional, por criticidade	Gestão de Patches	Proporção de ativos que possuem todos os patches de segurança aplicados.

Tempo Médio para Aplicação de Patches Críticos	Soma dos tempos de aplicação de patches críticos / Número de patches críticos aplicados	Por patch, por sistema, por equipe	Gestão de Patches	Tempo médio decorrido entre a identificação de um patch crítico e sua aplicação.
Número de Incidentes Evitados por Patch	Contagem de incidentes de segurança cuja causa raiz seria uma vulnerabilidade corrigida por patch	Por vulnerabilidade, por período	Gestão de Patches	Quantidade de incidentes de segurança prevenidos devido à aplicação de patches.
Percentual de Patches Aplicados na Janela	(Total de Patches Aplicados na Janela / Total de Patches Agendados) x 100	Por tipo de patch, por período	Gestão de Patches	Proporção de patches que foram aplicados dentro das janelas de manutenção definidas.

b. Os relatórios e indicadores de desempenho deverão ser apresentados e discutidos mensalmente, com base nos dados consolidados do período, durante a Reunião Mensal de Alinhamento prevista neste documento. A apresentação deverá ser conduzida por profissional com perfil de Gerente de Projetos, que possua pleno conhecimento de todos os serviços contratados, garantindo a adequada análise dos resultados e a proposição de medidas de aprimoramento.

1.4.3 Torre 03 - Red Team - Serviços de Testes de Invasão

1.4.3.1 Pentests

I. **Das Condições Gerais**

a. O serviço de Teste de Invasão deverá ser executado com a utilização de metodologias reconhecidas de mercado, contemplando abordagens do tipo *gray box* e *black box*, de forma a garantir uma análise realista e abrangente do ambiente tecnológico do TJES. Os testes terão como finalidade principal a identificação, o mapeamento e a documentação de vulnerabilidades que possam comprometer a segurança dos sistemas, dos processos e da infraestrutura tecnológica da instituição.
b. O escopo de cada atividade será definido pelo CONTRATANTE por meio de ordens de serviço específicas, podendo abranger, entre outros, redes corporativas, aplicativos web, aplicativos móveis, componentes de infraestrutura de TI e demais sistemas de informação críticos. Para a execução das avaliações, deverão ser aplicadas técnicas e ferramentas especializadas que permitam simular tentativas de acesso não autorizado ou de escalonamento de privilégios, sempre com o intuito de validar a resiliência dos controles de segurança existentes e recomendar medidas de correção.
c. Com o objetivo de assegurar a eficácia e a qualidade do serviço, a CONTRATADA deverá designar um Gerente de Projetos exclusivo para a condução do serviço de Teste de Invasão. Esse profissional será distinto daquele responsável pelo gerenciamento dos demais serviços contratados, garantindo dedicação integral, gestão especializada e foco nos resultados obtidos em cada ciclo de testes.
d. O serviço de Teste de Invasão será executado em duas modalidades: interna e externa. Em ambas as modalidades, o propósito será identificar, mapear, documentar, controlar e apoiar na remediação das vulnerabilidades detectadas, fornecendo evidências técnicas e relatórios detalhados que subsidiem a tomada de decisão e o aprimoramento contínuo da segurança institucional.

II. Das Ferramentas

a. Para a execução dos Testes de Invasão, a CONTRATADA deverá adotar metodologias reconhecidas internacionalmente, observando rigorosamente os padrões técnicos de referência. As técnicas e ferramentas a serem utilizadas deverão estar alinhadas às melhores práticas de mercado e possibilitar a validação abrangente dos controles de segurança existentes no ambiente do TJES.

b. Entre os referenciais obrigatórios, destacam-se:

   i. OSSTMM 3 (The Open Source Security Testing Methodology Manual), metodologia aberta de testes de segurança que abrange múltiplos domínios e camadas de infraestrutura;
   ii. ISSAF/PTF (Information Systems Security Assessment Framework), framework destinado à avaliação de segurança de sistemas de informação com base em processos sistemáticos;
   iii. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment), guia técnico do NIST para execução de testes e avaliações de segurança da informação;
   iv. NIST Special Publication 800-42 (Guideline on Network Security Testing), diretriz voltada especificamente para a realização de testes de segurança em redes;
   v. OWASP Testing Guide 3.0 (The Open Web Application Security Project), guia amplamente utilizado para testes de segurança em aplicações web, cobrindo as principais vulnerabilidades de software.

c. Adicionalmente, a CONTRATADA poderá propor a utilização de frameworks e normativos complementares pertencentes ao seu portfólio, desde que devidamente reconhecidos e comprovadamente aptos a complementar os padrões aqui listados. A aprovação para uso de metodologias adicionais ficará a critério do CONTRATANTE, mediante análise técnica e validação de sua aplicabilidade ao ambiente.

d. Para fins deste documento, os termos “pentest”, teste de penetração, teste de intrusão e teste de invasão serão considerados equivalentes e utilizados como sinônimos.

e. Os alvos, premissas e condições de cada teste de invasão deverão ser formalmente definidos e aprovados pelo CONTRATANTE por meio de Ordem de Serviço (OS) específica, que detalhará o escopo, os sistemas e ativos a serem avaliados, bem como os limites técnicos da execução.

f. Os testes de invasão serão realizados internamente (a partir de pontos da rede corporativa do CONTRATANTE) e externamente (a partir de conexões originadas na Internet), de modo a assegurar uma visão abrangente das vulnerabilidades do ambiente.

g. O CONTRATANTE poderá, a seu critério, acompanhar e supervisionar todas as fases dos testes, devendo manifestar previamente tal interesse na respectiva Ordem de Serviço.

h. Quaisquer atividades que apresentem risco de degradação ou comprometimento dos serviços em produção deverão ser obrigatoriamente reportadas pela CONTRATADA antes de sua execução, a fim de garantir a continuidade e a disponibilidade das operações críticas do TJES.

i. O processo de execução dos testes de invasão deverá contemplar, no mínimo, as seguintes fases:

   i. **Planejamento**: definição do escopo, premissas, metodologias e ferramentas a serem aplicadas;
   ii. **Descoberta**: mapeamento inicial de ativos, superfícies de ataque e pontos de vulnerabilidade;
   iii. **Ataque**: aplicação controlada de técnicas de exploração, visando validar falhas de segurança;
   iv. **Relatório Preliminar**: documentação inicial dos achados e vulnerabilidades identificadas;
   v. **Apresentação de Resultados**: reunião técnica para apresentação das evidências, recomendações e atividades executadas durante o teste;
   vi. **Reavaliação Pós-Correção**: realização de novo ciclo de testes após a aplicação das medidas de remediação;
   vii. **Relatório Final** – consolidação das evidências, classificação das vulnerabilidades, avaliação dos riscos e recomendações finais.

III. Planejamento

a. Todas as premissas, processos e atividades definidos e aprovados na Ordem de Serviço (OS), incluindo cronogramas e condições específicas, deverão ser formalmente detalhados e apresentados na fase de planejamento dos testes. Essa etapa inicial terá a finalidade de alinhar escopo, metodologias e expectativas entre a CONTRATADA e o CONTRATANTE, garantindo rastreabilidade e segurança em todas as fases da execução.

b. Para a coleta de informações e avaliação do ambiente corporativo do TJES, poderão ser aplicadas diferentes técnicas de Testes de Invasão, conforme definido no escopo da OS. Entre elas, destacam-se:

   i. **Pentest Gray Box (Técnica da Caixa Cinza ou Híbrida):** a avaliação será conduzida por especialista que disponha de conhecimento limitado acerca do alvo. As informações fornecidas pelo CONTRATANTE, em conjunto com a OS, orientarão o teste, que terá como objetivo avaliar a resiliência do ambiente considerando parte de seu funcionamento previamente conhecido.

   ii. **Pentest Black Box (Técnica da Caixa Preta):** a avaliação será conduzida por especialista com pouco ou nenhum conhecimento prévio sobre o ambiente, garantindo a condição de desconhecimento total. Este tipo de teste simula com maior fidelidade a atuação de atacantes externos, que não possuem informações internas sobre os sistemas e ativos da organização.

c. Nos casos em que forem utilizadas as técnicas de Caixa Preta ou Caixa Cinza, os relatórios de avaliação deverão obrigatoriamente ser acompanhados das respectivas declarações de “não conhecimento” ou “conhecimento parcial” do ambiente avaliado. Tais declarações servirão como comprovação da integridade metodológica adotada e como garantia de que as condições previamente estabelecidas foram devidamente respeitadas.

IV. Precificação

a. O modelo de pagamento adotado para o Serviço de Testes de Invasão tem como objetivo assegurar transparência, previsibilidade e adequação às características específicas de cada cenário avaliado. Reconhece-se que a diversidade de ativos, a complexidade de ambientes e as distintas abordagens técnicas podem impactar diretamente o esforço necessário para a execução dos testes. Nesse sentido, será empregada uma estratégia de precificação baseada em horas, permitindo que, sempre que necessário, sejam alocadas horas adicionais para a execução de testes mais aprofundados, contemplando maior número de ativos, utilização de diferentes técnicas e a produção de resultados mais detalhados.

b. Cada Ordem de Serviço (OS) emitida para realização de testes de invasão deverá especificar a quantidade de horas de trabalho destinada à etapa de Ataque, sendo estabelecido o mínimo obrigatório de 40 (quarenta) horas por teste. Essa etapa constitui a métrica central de precificação, de modo que os custos relacionados às demais fases do processo de pentest (planejamento, descoberta, relatório, apresentação de resultados, reavaliação pós-remediação etc.) deverão estar diluídos na métrica horária da etapa de Ataque.
c. A estrutura de precificação será organizada em duas dimensões: (i) as técnicas de teste empregadas - Gray Box (caixa cinza) e Black Box (caixa preta) - e (ii) o valor da hora de cada uma dessas modalidades. Dessa forma, a profundidade e a abrangência dos testes estarão diretamente relacionadas à quantidade de horas alocadas em cada OS, garantindo flexibilidade e alinhamento entre a complexidade da demanda e o investimento aplicado.
d. A taxa horária praticada será fixa, estabelecida a partir dos custos operacionais da CONTRATADA, do nível de experiência da equipe alocada e da complexidade técnica envolvida. Para viabilizar a execução dos serviços, serão disponibilizados pacotes de horas, a serem demandados e formalizados por meio de Ordem de Serviço, que poderão ser utilizados pelo TJES para a contratação de testes de penetração nos diversos sistemas de informação sob sua responsabilidade.

V. **Descoberta**

a. Na fase de Descoberta, a CONTRATADA deverá utilizar, no mínimo, ferramentas de análise e gestão de vulnerabilidades previstas neste documento, bem como técnicas manuais de análise. Antes da utilização efetiva, tanto as ferramentas quanto a metodologia de execução das análises manuais deverão ser apresentadas ao TJES para ciência e aprovação.

b. Os resultados desta fase deverão constar detalhadamente no Relatório de Teste de Invasão, contemplando os seguintes quesitos, sempre que aplicáveis:

i. **Coleta Passiva:** Deverão ser empregadas técnicas de obtenção de informações sem interação direta com o alvo, incluindo, no mínimo:

I) Consultas de DNS via *whois* e *nslookup*;

II) Pesquisas em mecanismos de busca;
III) Monitoramento de listas de discussão;
IV) Verificação de blogs e conteúdos publicados por colaboradores;
V) Técnicas de *dumpster diving* ou *trashing*;
VI) Coleta de informações publicamente disponíveis;
VII) Captura de pacotes por meio de *passive eavesdropping* (*packet sniffing*);
VIII) Identificação de serviços por meio de captura de *banners*.

ii. **Coleta Ativa:** Deverão ser aplicadas técnicas que envolvem interação direta com o ambiente, abrangendo, no mínimo:
I) *Port scanning* para mapeamento da rede;
II) Varredura de vulnerabilidades em ativos e aplicações;

iii. A varredura deverá abranger a identificação de:
I) Hosts ativos na rede;
II) Portas abertas e serviços em execução;
III) Serviços vulneráveis identificados nos hosts;
IV) Sistemas operacionais em uso;
V) Vulnerabilidades associadas a sistemas operacionais e aplicações mapeadas;
VI) Configurações em desacordo com boas práticas de segurança;
VII) Rotas críticas e possíveis impactos decorrentes de sua alteração ou desconfiguração;
VIII) Vetores de ataque e cenários potenciais de exploração;
IX) Vulnerabilidades classificadas de acordo com bases reconhecidas (CVE);
X) Vulnerabilidades de Alto, Médio e Baixo Risco;
XI) Informações necessárias à fase subsequente de ataques.

iv. **Serviços e Aplicações Web:** Deverão ser avaliados ainda os seguintes aspectos relacionados a aplicações e serviços web:
I) Uso inadequado de sistema de arquivos e de arquivos temporários;

II) Vazamento de informações em decorrência de configurações padrão de tratamento de erros;
III) Deficiências no tratamento de entradas de dados;
IV) Vulnerabilidades decorrentes de más configurações de serviços;
V) Práticas inseguras de gerenciamento de sessões web.

VI. **Ataque (exploração)**

a. Quaisquer atividades que apresentem indícios de comprometimento de algum ambiente ou ativo deverão ser imediatamente reportadas pela CONTRATADA antes de sua execução, de modo a preservar a disponibilidade dos ambientes e serviços críticos do CONTRATANTE.

b. A CONTRATADA deverá realizar testes de vulnerabilidade e invasão em endereços IPs, URLs, aplicações ou quaisquer ativos definidos no escopo do ambiente computacional, incluindo servidores, bancos de dados, ativos de rede, ativos de segurança e demais equipamentos relevantes.

c. Deverão ser aplicadas, no mínimo, as seguintes técnicas de ataque:

i. Violações do protocolo HTTP;
ii. SQL Injection;
iii. LDAP Injection;
iv. Cookie Tampering;
v. Cross-Site Scripting (XSS);
vi. Directory Traversal;
vii. Buffer Overflow;
viii. Execução de Comandos no Sistema Operacional (OS Command Execution);
ix. Command Injection;
x. Remote Code Inclusion;
Server Side Includes (SSI) Injection;
xi. File Disclosure;
Information Leak;
Explorações de Zero Day;
xii. Negação de Serviço Distribuída (DDoS);

xiii. Negação de Serviço (DoS);
xiv. Ataques contra protocolo TCP;
xv. Ataques direcionados a aplicações.

d. Para ataques de negação de serviço e contra protocolo TCP deverão ser exploradas, no mínimo, as seguintes técnicas:

i. Exploração de bugs em serviços, aplicativos e sistemas operacionais;
ii. SYN Flooding;
iii. Fragmentação de pacotes IP;
iv. Smurf e Fraggle;
v. Teardrop, Nuke e Land;
vi. Sequestro de conexões TCP;
vii. Previsão de números de sequência TCP;
viii. Ataque de Mitnick;
ix. Source Routing.

e. Nos ataques em nível de aplicação deverão ser testados, no mínimo:
i. Buffer Overflow;
ii. Vulnerabilidades relacionadas ao SNMP;
iii. Vírus, Worms e Cavalos de Tróia.

f. Para ataques de injeção de código, deverão ser aplicados:
i. XSS (Cross-Site Scripting);
ii. Comprometimento de acessos remotos;
iii. Mecanismos de manutenção de acesso;
iv. Técnicas de encobrimento de rastros da invasão.

g. Para os testes em serviços WEB, internos (Intranet) e externos (Internet), deverão ser observados os padrões definidos na publicação OWASP Testing Guide 3.0, contemplando:

i. **Coleta de Informações:** OWASP-IG-001 a OWASP-IG-006;
ii. **Gerenciamento de Configuração:** OWASP-CM-001 a OWASP-CM-008;
iii. **Autenticação:** OWASP-AT-001 a OWASP-AT-010;
iv. **Gerenciamento de Sessão:** OWASP-SM-001 a OWASP-SM-005;
v. **Autorização:** OWASP-AZ-001 a OWASP-AZ-003;

vi. **Negócio Lógico:** OWASP-BL-001;
vii. **Validação de Dados:** OWASP-DV-001 a OWASP-DV-016;
viii. **Negação de Serviço:** OWASP-DS-001 a OWASP-DS-008;
ix. **Serviços Web:** OWASP-WS-001 a OWASP-WS-007;
x. **AJAX (Asynchronous JavaScript and XML):** OWASP-AJ-001 e OWASP-AJ-002.

h. Cada teste de invasão deverá gerar relatórios técnicos contendo, no mínimo:
   i. Referência-base (Whitepaper) utilizada para o teste;
   ii. Ameaças identificadas durante a execução;
   iii. Riscos levantados ao ambiente computacional;
   iv. Propostas de contramedidas para mitigar as vulnerabilidades encontradas.

VII. Relatório de Teste de Invasão

a. Ao término da fase de ataque, a CONTRATADA deverá elaborar e entregar ao CONTRATANTE um relatório técnico intitulado “Relatório de Teste de Invasão”, específico para cada teste realizado. Este relatório deverá conter, no mínimo, as seguintes informações:

   i. Objetivos, premissas e escopo do teste de invasão;
   ii. Datas e horários em que os testes foram executados;
   Metodologia de análise de vulnerabilidades utilizada;
   iii. Descrição detalhada das ações realizadas, das metodologias aplicadas e das vulnerabilidades identificadas;
   iv. Categorização das vulnerabilidades e sua respectiva severidade;
   v. Registro de possíveis problemas aplicáveis ao ambiente avaliado;
   vi. Recomendações e controles de segurança necessários para a correção das vulnerabilidades;
   vii. Apresentação das evidências apuradas durante os testes;
   viii. Fontes de pesquisa utilizadas;
   ix. Referências técnicas e ferramentas empregadas;
   x. Informações acessadas pelos especialistas;
   xi. Outras evidências que comprovem o sucesso da invasão ou exploração realizada.

b. Além disso, o relatório deverá contemplar, de forma detalhada, as seguintes informações complementares:
    i. Detalhes da infraestrutura descoberta que foi alvo dos testes de invasão;
    ii. Equipamentos, recursos e insumos utilizados durante a execução do teste;
    iii. Tipos de ataque empregados;
    iv. Prazos e janelas de tempo destinadas à realização dos testes;
    v. Identificação dos pontos de contato da CONTRATADA responsáveis pelo acompanhamento e tratamento de questões decorrentes dos testes;
    vi. Tipos de testes efetivamente realizados pelos especialistas de segurança da informação;
    vii. Confirmação ou refutação da existência de vulnerabilidades;
    viii. Documentação completa sobre o caminho utilizado para exploração, incluindo avaliação do impacto e comprovação da existência das vulnerabilidades;
    ix. Evidências de obtenção de acesso e de possíveis processos de escalada de privilégios;
    x. Detalhamento da metodologia de ataque adotada em cada cenário;
    xi. Recomendações técnicas para mitigação de riscos e correção das vulnerabilidades identificadas.

VIII. **Relatório Final do Teste de Invasão**

a. Após a entrega do Relatório de Teste de Invasão, a CONTRATADA deverá conduzir uma reunião técnica com o objetivo de apresentar detalhadamente todo o conteúdo do documento. Nessa reunião, deverão ser esclarecidas eventuais dúvidas do corpo técnico do CONTRATANTE, garantindo a plena compreensão dos resultados, metodologias utilizadas e vulnerabilidades identificadas.
b. Concluída a apresentação, o CONTRATANTE procederá à análise do relatório, cabendo-lhe solicitar ao Gerente Técnico de Projetos das equipes responsáveis pela administração, operação e manutenção da infraestrutura que adote as medidas necessárias para a correção e/ou mitigação dos apontamentos. Tais medidas deverão contemplar as recomendações

apresentadas pela equipe executora dos testes de invasão, ou ainda outras ações julgadas pertinentes para a eliminação ou redução dos riscos identificados.

c. Nos casos em que houver impedimento técnico que inviabilize a aplicação das medidas de correção pela CONTRATADA, por razões que não lhe sejam atribuíveis, esta deverá comunicar formalmente a situação ao CONTRATANTE. Caberá ao CONTRATANTE, a partir dessa comunicação, decidir sobre a aceitação residual do risco ou sobre a adoção de medidas alternativas.
d. Após a análise dos resultados e a execução das ações de remediação, o CONTRATANTE poderá solicitar à CONTRATADA a realização de um novo teste de invasão, com a finalidade de aferir a eficácia das correções aplicadas. Nessa hipótese, deverá ser emitido um novo relatório técnico, consolidando os resultados obtidos na reavaliação e confirmando a mitigação ou eliminação das vulnerabilidades anteriormente identificadas.

IX. Atividades de Apoio

a. Para auxiliar a execução das atividades previstas, poderão ser requisitados pelo CONTRATANTE, a critério desta, os seguintes documentos a serem elaborados e apresentados pela CONTRATADA:

    i. Plano de Trabalho, contendo o detalhamento do escopo dos testes a serem realizados, bem como o cronograma de execução proposto;
    ii. Apresentação Inicial, com a descrição das ações que serão aplicadas pela CONTRATADA durante a execução dos testes;
    iii. Relatórios de Acompanhamento Semanais, contemplando o andamento do Plano de Trabalho, com registro das atividades executadas, ajustes implementados e eventuais desvios ou ocorrências relevantes.

X. Periodicidade de execução

a. A CONTRATADA deverá executar os Testes de Invasão conforme a quantidade previamente definida em Ordem de Serviço (OS), respeitando o escopo aprovado pelo CONTRATANTE.

b. O prazo para conclusão de cada OS, abrangendo todas as etapas previstas, será estabelecido em conformidade com a natureza e a complexidade da atividade a ser realizada. Esse ciclo de execução deverá contemplar, no mínimo, as seguintes fases:

   i. **Atividades do Pentest**: realização dos testes de invasão, aplicando metodologias e técnicas reconhecidas para identificação de vulnerabilidades nos ambientes relacionados neste documento;
   ii. **Entrega do Relatório "Teste de Invasão"**: apresentação formal dos resultados obtidos na execução do teste, com descrição detalhada das vulnerabilidades identificadas, riscos associados e recomendações iniciais;
   iii. **Ações Corretivas**: implementação, pelo CONTRATANTE, das medidas de correção das vulnerabilidades apontadas pela CONTRATADA, conforme os relatórios técnicos emitidos;
   iv. **Reavaliação do Pentest**: execução de nova rodada de testes, quando necessária, para validar a eficácia das medidas corretivas aplicadas;
   v. **Entrega do Relatório Final do Teste de Invasão**: apresentação consolidada dos resultados após a reavaliação, confirmando a mitigação dos riscos e formalizando a conclusão da Ordem de Serviço.

XI. Grupo Técnico de Teste de Invasão

a. O grupo responsável pela execução do serviço de teste de invasão será o Grupo Técnico de Teste de Invasão.

XII. Certificações do Grupo Técnico de Teste de Invasão

a. Com o objetivo de assegurar a qualidade da execução dos Testes de Invasão e dos relatórios técnicos correspondentes, pelo menos um dos profissionais alocados para a atividade deverá possuir, obrigatoriamente, o grupo de certificações abaixo relacionado (ou equivalente reconhecida no mercado):

Perfis	Certificações	Tipo de Atuação

Analista de Segurança	02 (duas) obrigatórias: • ITCerts - ITC-004 - Ethical Hacking Essentials • ITCerts - ITC-042 - PenTest Essentials 01 (uma) obrigatória: • EC-Council - Certified Ethical Hacker (C|EH); • EC-Council Licensed Penetration Tester – LPT; • IACRB Certified Expert Penetration Tester – CEPT; • GIAC Exploit Researcher and Advanced Penetration Tester – GXPN; • Offensive Security Certified Professional – OSCP; • CompTIA - PenTest+	Remota

b. Em comum acordo com o CONTRATANTE, poderão ser aceitas certificações equivalentes às listadas, desde que comprovada a equivalência em termos de abrangência técnica e requisitos de qualificação.

c. Todos os profissionais envolvidos deverão apresentar certificações válidas, respeitando o prazo de vigência estabelecido pela entidade certificadora. Para certificações que não possuem expiração formal, será aceita, no máximo, até a penúltima versão disponível da credencial em questão.

1.5 Modelo de Execução e Implementação do Contrato

1.5.1 Principais Papéis

I. Durante a execução contratual, deverão ser observados os seguintes papéis e responsabilidades:
   a. **Preposto**: representante legal da empresa contratada, responsável pelo acompanhamento da prestação dos serviços;
   b. **Gestor do Contrato**: servidor do órgão responsável pela gestão da execução contratual, assegurando a aderência do serviço ao previsto neste documento e nos demais instrumentos normativos;
   c. **Fiscal Técnico do Contrato**: servidor lotado na área de Tecnologia da Informação e Comunicação (TIC), incumbido da fiscalização técnica do objeto contratado, com foco na conformidade dos aspectos operacionais e tecnológicos;
   d. **Fiscal Administrativo do Contrato**: servidor lotado na área Administrativa, responsável pela fiscalização sob a perspectiva legal, administrativa e normativa da execução contratual;
   e. **Fiscal Demandante do Contrato**: servidor vinculado à área demandante da solução, responsável pela fiscalização dos aspectos funcionais do objeto contratado e pela validação da aderência do serviço às necessidades da unidade requisitante.

II. As atribuições do Gestor e dos Fiscais do Contrato encontram amparo nos seguintes instrumentos normativos:
   a. Artigos 8º e 117 da Lei Federal nº 14.133/2021;
   b. Resolução CNJ nº 468/2022;
   c. Guia de Contratação de TIC do Poder Judiciário, estabelecido pela Resolução CNJ nº 468/2022.
   d. Ato Normativo Nº 096/2022 do Tribunal de Justiça do Estado do Espírito Santo.

1.5.2 Dinâmica de Execução

I. A vigência contratual terá duração de 02 (dois) anos, estruturada em duas etapas distintas.
   i. Na primeira etapa, correspondente à fase de implantação, o prazo será de 6 (seis) meses, destinados à configuração inicial, parametrização das soluções e à integração dos serviços.

ii. Na segunda etapa, correspondente à fase de execução, serão compreendidos os 18 (dezoito) meses subsequentes, período em que os serviços contratados deverão estar plenamente operacionais e em regime contínuo de funcionamento.

iii. Em caso de prorrogação contratual, não será concedido novo prazo para a etapa de implantação. Nessa hipótese, os quantitativos originalmente previstos serão acrescidos de forma proporcional, de modo a assegurar a continuidade dos serviços, sem prejuízo da faculdade do CONTRATANTE em autorizar acréscimos nos limites legais aplicáveis.

II. A execução dos serviços objeto do contrato será demandada por meio da emissão de **Ordens de Serviço (OS)**, elaboradas pelo CONTRATANTE. Cada item contratado poderá ser solicitado em ordem de serviço própria ou em conjunto com outros itens, de acordo com a conveniência administrativa e a necessidade operacional do SOC.

i. As ordens de serviço deverão conter, no mínimo, a descrição do serviço a ser executado, o prazo de atendimento, as métricas de desempenho a serem observadas e as condições específicas de execução, constituindo-se como instrumento formal de controle e de rastreabilidade contratual.

III. A tabela a seguir traz os principais marcos e eventos relevantes que ocorrerão durante a execução da contratação:

ID	DESCRIÇÃO	QUANDO	PRAZO	ATORES
1	Assinatura do Contrato e do termo de compromisso de manutenção de sigilo	Após homologação do objeto contratado	Até 5 (cinco) dias úteis	CONTRATANTE e CONTRATADA
2	Publicação da equipe de fiscalização (Fiscal Técnico e Fiscal Administrativo do Contrato	Após ID 1	Até 3 (três) dias úteis	STI
3	Reunião de alinhamento – Início do período de transição e implantação.	Após ID 2	Até 10 (dez) dias úteis	Gestor e Fiscais do Contrato e

ID	DESCRIÇÃO	QUANDO	PRAZO	ATORES
	Conforme tópico de Reunião de Alinhamento.			Preposto
4	Início da prestação do serviço de acordo com a Ordem de Serviço emitida pelo TJES	Após ID 3	Imediato	CONTRATANTE e CONTRATADA
5	Diagnóstico inicial de vulnerabilidades existentes, anteriores ao contrato, incluindo recomendações e procedimentos de correção/mitigação. **Conforme tópico Acompanhamento dos prazos de garantia e Nível Mínimo de Serviço – NMS.**	Após ID 3	Até 30 (trinta) dias úteis.	CONTRATADA
6	Apresentação de plano de operacionalização dos serviços, contendo o detalhamento das ações necessárias para a absorção dos conhecimentos e entrega dos serviços. **Conforme tópico Modelo de Execução. (exceto os serviços do Red Team)**	Após ID 3	Até 15 (quinze) dias úteis	CONTRATADA
7	Carta de apresentação, acompanhada da relação de prestadores da CONTRATADA que irão prestar os serviços, juntamente com os	Após ID 3	Até 15 (quinze) dias úteis	CONTRATADA

ID	DESCRIÇÃO	QUANDO	PRAZO	ATORES
	documentos comprobatórios de vínculo empregatício, experiência, qualificação e certificações exigidas para o perfil profissional. **Conforme tópico Modelo da execução. (exceto os serviços do Red Team)**			
8	Carta de apresentação, acompanhada da relação de prestadores da CONTRATADA que irão prestar os serviços, juntamente com os documentos comprobatórios de vínculo empregatício, experiência, qualificação e certificações exigidas para o perfil profissional, **exclusivamente para o serviços Red Team**	Após ID 3	Até 5 (cinco) dias após a Expedição de cada Ordem de Serviço específica.	CONTRATADA
9	Emissão do ROM - Relatório de Operação Mensal. Conforme tópico de Acompanhamento dos prazos de garantia e Nível Mínimo de Serviço - NMS.	Mensalmente	Até o 10º (décimo) dia do mês posterior à prestação do serviço	CONTRATADA
9.1	Apresentação do Emissão do ROM - Relatório de Operação Mensal e emissão da ATA de reunião de apresentação	Mensalmente	Até o 10º (décimo) dia do mês posterior à prestação do serviço	

ID	DESCRIÇÃO	QUANDO	PRAZO	ATORES
10	Análise do Relatório de Operação Mensal e emissão do Termo de Recebimento	Após ID 9.1	Até 10 (dez) dias após o recebimento dos ROM	CONTRATANTE
11	Envio da Nota Fiscal	Após ID 10	Até 5 (dez) dias úteis	CONTRATADA
12	Liquidação e pagamento da nota fiscal	Após ID 11	Até 30 dias corridos	CONTRATANTE

IV. Detalhamento dos Marcos da Vigência Contratual

i. A reunião de alinhamento marcará o início do período de implantação e deverá contemplar a apresentação da equipe que atuará na fase de transição dos serviços. Nesse momento, a CONTRATADA deverá apresentar a documentação comprobatória de qualificação de, pelo menos, um profissional correspondente a cada item de serviço previsto, em observância aos requisitos de qualificação técnica descritos no capítulo de Qualificação Profissional.

ii. Em caso de não atendimento aos requisitos, a CONTRATADA terá prazo de dois dias úteis, a contar da data de comunicação formal da recusa, para apresentar a documentação de um novo profissional que satisfaça integralmente as exigências. O CONTRATANTE poderá, a qualquer tempo, recusar a execução dos serviços por profissionais que não atendam às qualificações estabelecidas.

iii. O período de transição compreenderá 15 dias úteis contados a partir da reunião de alinhamento. Trata-se de etapa integrante do período de implantação, destinada ao reconhecimento do ambiente pela CONTRATADA e à elaboração do Plano de Operacionalização dos Serviços.

V. Plano de Operacionalização dos Serviços

i. A CONTRATADA deverá apresentar, em até 15 dias úteis após a reunião de alinhamento, o Plano de Operacionalização dos Serviços, contendo:

a. Detalhamento das ações necessárias para absorção do ambiente e início da execução contratual;

b. Relação das soluções e ferramentas que serão utilizadas na prestação dos serviços, acompanhadas dos comprovantes de licenciamento com prazo de validade compatível com a vigência contratual.
c. Link e acesso ao Portal de Indicadores, conforme previsto no capítulo que trata do monitoramento dos serviços.
d. Deverá, ainda, ser entregue a documentação definitiva com a relação completa dos profissionais envolvidos, acompanhada de comprovação de qualificação e experiência exigida para cada perfil.

ii. O não atendimento a essas exigências acarretará rescisão contratual, sem prejuízo da aplicação de sanções administrativas e legais.

VI. Período de Implantação

i. O período inicial de 180 dias será considerado como fase de implantação da operação. Durante esse período, os indicadores de desempenho não atingidos estarão sujeitos à aplicação de glosas graduais, conforme os seguintes critérios:
a. Nos primeiros 60 dias: aplicação de 25% dos percentuais previstos para cada ocorrência de indicador não atingido.
b. Do 61º ao 120º dia: aplicação de 50% dos percentuais previstos.
c. Do 121º ao 180º dia: aplicação de 75% dos percentuais previstos.
d. Após o 180º dia, aplicar-se-ão integralmente os percentuais previstos na tabela de níveis mínimos de serviço.
e. Em caso de prorrogação contratual, não será concedido novo período de implantação, permanecendo as condições acima estabelecidas.

VII. Regras Adicionais

i. Sempre que houver necessidade de alteração da equipe, a CONTRATADA deverá apresentar previamente a documentação comprobatória de qualificação do(s) novo(s) profissional(is) antes do início de suas atividades.

VIII. As regras acima descritas são aplicáveis às equipes técnicas de todas as torres de serviço previstas no contrato.

1.5.3 Instrumentos Formais de Solicitação

I. O canal de comunicação entre o CONTRATANTE e a CONTRATADA, para fins de gestão e fiscalização contratual, deverá ocorrer preferencialmente por intermédio do

preposto designado pela CONTRATADA, conforme previsto no instrumento convocatório.

II. As interações oficiais poderão ser realizadas por meio dos seguintes instrumentos:
   a. Correio eletrônico (e-mail): canal formal para envio e recebimento de informações, registros e documentos;
   b. Processo administrativo: utilizado para comunicações que demandem tramitação formal e registro no sistema de gestão documental do CONTRATANTE;
   c. Atas de reunião: elaboradas por colaborador da CONTRATADA, devendo ser validadas pela equipe técnica do CONTRATANTE, assegurando o registro e acompanhamento das deliberações;
   d. Sistema WEB: acesso por procedimentos específicos, mediante controle de login e senha, garantindo a rastreabilidade e segurança das informações trocadas.

1.5.4 Reunião de Alinhamento

I. A reunião de alinhamento entre o CONTRATANTE e a CONTRATADA tem como finalidade identificar expectativas, nivelar entendimentos sobre as condições estabelecidas no contrato, no edital e em seus anexos, além de esclarecer eventuais dúvidas relacionadas à execução dos serviços.

II. A primeira reunião deverá ocorrer no endereço do CONTRATANTE ou de forma remota, dentro do prazo definido no capítulo referente à dinâmica da execução. A realização remota poderá se dar por conveniência do CONTRATANTE ou em razão de condições excepcionais de saúde pública que impeçam ou restrinjam reuniões presenciais.

III. Nessa ocasião, caberá à CONTRATADA:
   a. Apresentar oficialmente o seu preposto, mediante Termo de Designação de Preposto, conforme modelo a ser apresentado;
   b. Apresentar o cronograma de atendimento, em conformidade com o capítulo que trata dos Níveis Mínimos de Serviço (NMS), especificando os serviços a serem prestados e as tecnologias a serem utilizadas, de forma a demonstrar o atendimento integral aos requisitos deste documento.

IV. Todos os aspectos tratados na reunião deverão ser submetidos à aprovação do CONTRATANTE.

V. A CONTRATADA deverá promover, **mensalmente**, reunião de alinhamento com a participação de todos os profissionais certificados vinculados ao contrato, ocasião em que se reunirão com os gestores e fiscais designados pelo CONTRATANTE. Nessas reuniões deverão ser apresentados os resultados alcançados, o andamento das atividades em execução, eventuais não conformidades detectadas, bem como os planos de ação corretivos e preventivos adotados, de forma a garantir a rastreabilidade, a transparência e a conformidade na execução contratual.

1.5.5 Solicitações

I. As solicitações formais de serviços deverão ser realizadas por meio de chamados técnicos ou Ordens de Serviço encaminhadas à CONTRATADA em formato digital, seja por e-mail, seja por ferramenta de registro de chamados. A execução de qualquer atividade dependerá de autorização prévia do CONTRATANTE ou da abertura de chamado na Central de Serviços.

II. Os serviços poderão ser requisitados pelo CONTRATANTE através de diferentes canais: Central de Serviços, Ordens de Serviço, registro de chamados por contato telefônico (inclusive ligação gratuita 0800), correio eletrônico ou site web específico, mediante procedimentos com controle de acesso por senha.

III. As solicitações poderão ser registradas a qualquer momento, 24 horas por dia, em dias úteis, finais de semana, feriados e pontos facultativos. O atendimento deverá observar os Níveis Mínimos de Serviço previstos neste documento.

IV. A CONTRATADA deverá disponibilizar endereços eletrônicos específicos para recebimento de chamados e comunicações, possibilitando a abertura automática de tickets sem intervenção humana. Além disso, chamados – especialmente incidentes – poderão ser abertos automaticamente pelas ferramentas de monitoramento do ambiente do CONTRATANTE ou por soluções que venham a ser implantadas pela própria CONTRATADA.

V. Sempre que um chamado for aberto, uma notificação deverá ser encaminhada aos endereços eletrônicos indicados pelo CONTRATANTE, permitindo o acompanhamento e atualização das informações por meio do sistema de gestão de chamados. O CONTRATANTE poderá, ainda, agendar data e hora específicas para o início do atendimento.

VI. Na hipótese de indisponibilidade do sistema de chamados disponibilizado pela CONTRATADA, os registros deverão ser feitos por meio de número de telefone local

ou ligação gratuita 0800, devendo tais canais ser mantidos ativos pela CONTRATADA.

VII. Todas as solicitações recepcionadas deverão gerar número de protocolo exclusivo, a ser registrado no sistema de gerenciamento de chamados. Esse protocolo permitirá a contabilização posterior de todos os atendimentos e a geração de relatórios gerenciais.

VIII. Cada chamado técnico deverá conter, no mínimo, as seguintes informações:

a. Número de identificação sequencial exclusivo;
b. Data e hora do início da ocorrência;
c. Descrição detalhada da ocorrência;
d. Objetivo da tarefa, com definição das expectativas e justificativas para a sua realização;
e. Nível de severidade atribuído;
f. Providências adotadas para diagnóstico;
g. Indicação de solução provisória e/ou definitiva;
h. Data e hora do encerramento com a solução definitiva;
i. Identificação do técnico do TJES que solicitou e validou o chamado;
j. Identificação da área demandante;
k. Identificação do técnico da CONTRATADA responsável pela execução;
l. Listagem das atividades a serem realizadas, classificadas conforme sua complexidade;
m. Identificação dos responsáveis pela fiscalização e validação, pelo lado do CONTRATANTE;
n. Resultado alcançado e nível de qualidade definido para a tarefa;
o. Outras informações que se mostrem pertinentes.

1.5.6 Validação Técnica das solicitações

I. As solicitações somente poderão ser consideradas encerradas quando todos os objetivos definidos forem integralmente atingidos e quando os produtos ou serviços demandados forem entregues com a qualidade requerida, devidamente avaliados e atestados tanto pelo demandante quanto pelo gestor do CONTRATANTE.

II. Antes do fechamento de cada solicitação, a CONTRATADA deverá obrigatoriamente consultar o representante designado pelo CONTRATANTE. Esse representante será responsável por avaliar a execução e atestar formalmente o serviço prestado, garantindo que os requisitos técnicos e operacionais tenham sido cumpridos.

III. Qualquer solicitação de serviço ou incidente que venha a ser encerrado sem a anuência expressa do CONTRATANTE, ou sem que tenha sido efetivamente resolvido, deverá ser reaberto. Nesses casos, os prazos de atendimento serão recalculados a partir da data da primeira abertura da requisição, inclusive para fins de aplicação das penalidades e sanções previstas no contrato.

1.6 Condições de execução do Serviço

1.6.1 Locais e horários de Prestação dos Serviços

I. A execução dos serviços durante o horário de funcionamento do CONTRATANTE deverá ocorrer de forma presencial, nas dependências indicadas, de segunda a sexta-feira, no período das 07h às 19h.

II. Fora desse intervalo, os serviços deverão ser prestados de maneira remota, em regime de operação contínua 24x7x365, garantindo a disponibilidade ininterrupta.

III. Em ambos os casos, a execução deverá observar rigorosamente os critérios técnicos e operacionais definidos neste documento, assegurando a conformidade com os níveis de serviço estabelecidos.

Purple Team Atendimento de requisições				
Item	**Descrição do Serviço**	**Horário de prestação do serviço**		**Local de Prestação**
		Administrativo	**Contínuo**	
1	Serviço de Administração, Operação, Manutenção e Atendimento às Requisições	X	X	Semipresencial para Torre de Serviço que ficará nas instalações do CONTRATANTE. Entretanto, esta torre de serviços também é composta de equipe remota no SOC da Contratada, nesse caso o serviço é contínuo.
Blue Team - Gestão de incidentes de segurança e monitoramento de ataques cibernéticos				

Item	Descrição do Serviço	Horário de prestação do serviço		Local de Prestação
		Administrativo	Contínuo	
2	Serviço de gestão de vulnerabilidades	X		Remoto
3	Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança		X	Remoto
4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response – SOAR		X	Remoto
5	Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)		X	Remoto
6	Gerenciamento de Patch (Patch Management)		X	Remoto
Red Team – Serviço de Testes de invasão (Também conhecidos como Pentests ou Testes de Intrusão)				
Item	**Descrição do Serviço**	**Horário de prestação do serviço**		**Local de Prestação**
1	Pentest Gray Box	Sob demanda		Remoto
2	Pentest Black Box	Sob demanda		Remoto

Legenda:

Horário Administrativo	Dias úteis das 7h às 19h
Horário Monitoramento	Todos os dias 24x7x365

1.6.2 Acompanhamento dos prazos de garantia e Níveis mínimos de Serviços (NMS)

I. Os Níveis Mínimos de Serviço (NMS) constituem critérios objetivos e mensuráveis, destinados a aferir e avaliar a qualidade, o desempenho, a disponibilidade, a abrangência e a segurança dos serviços contratados.

II. A medição dos serviços será realizada por meio de indicadores vinculados a fórmulas específicas, devendo ser apurados mensalmente conforme a unidade, a periodicidade e a frequência previstas nos requisitos técnicos. Os resultados obtidos deverão ser confrontados com as metas exigidas, de forma a permitir a avaliação transparente da execução.

III. O não atingimento das metas ensejará a aplicação de glosas, entendidas como rejeição ou desconsideração total ou parcial de determinados itens do contrato. Nos casos em que houver múltiplas ocorrências, as glosas por inadimplemento serão cumulativas.

IV. O modelo de medição adotado será híbrido, fundamentado na disponibilidade dos serviços e condicionado ao alcance das metas de desempenho. Nesse modelo, o valor total dos serviços é estabelecido no momento da contratação, considerando a disponibilidade estimada de profissionais. Contudo, o valor mensal a ser faturado será calculado de acordo com os resultados alcançados pela CONTRATADA nos indicadores de NMS.

V. Não serão concedidos bônus ou pagamentos adicionais caso a CONTRATADA supere as metas previstas, nem será admitida compensação entre indicadores. Ou seja, a superação de uma meta não poderá ser utilizada para justificar o não atendimento de outra.

VI. A aferição e avaliação dos NMS ocorrerá mensalmente, devendo a CONTRATADA apresentar ao CONTRATANTE o Relatório de Operação Mensal (ROM) dentro do prazo definido. Esse relatório deverá conter, no mínimo:

   a. indicadores e níveis de serviço alcançados;
   b. descrição e análise dos incidentes ocorridos, incluindo categorias, severidade, tempos de resposta e de solução, bem como ações tomadas;

c. identificação de vulnerabilidades, recomendações de correção e prazos de solução;
d. informações de desempenho das ferramentas mantidas pela CONTRATADA (CPU, memória, disco, aderência ao ambiente e relação de ativos configurados no SIEM);
e. plano de resposta a incidentes (PRI) e plano de comunicação atualizados;
f. documentação técnica e operacional referente à transferência de conhecimento;
g. tabela de comprovação da qualificação técnica dos profissionais;
relatório de *gap analysis*;
h. ata da reunião de apresentação do ROM.

VII. Caberá à equipe de fiscalização do contrato analisar mensalmente o ROM, verificando os indicadores e os NMS atingidos. O não cumprimento das metas acarretará glosas, multas ou outras sanções contratuais.

VIII. A CONTRATADA deverá manter ferramenta única de abertura e acompanhamento de chamados, permitindo ao CONTRATANTE monitorar o andamento, ainda que a demanda transite por diferentes equipes técnicas (Red, Blue ou Purple). Apenas serão aceitas justificativas para o não atendimento em casos de força maior ou quando depender de ações diretas da equipe técnica do CONTRATANTE, desde que formalmente comunicados e previamente aprovados pelo gestor ou fiscal técnico.

IX. Durante a fase de implantação, a CONTRATADA deverá elaborar, em conjunto com o CONTRATANTE, um Plano de Resposta a Incidentes (PRI), contemplando procedimentos claros para identificação, avaliação, mitigação e comunicação de incidentes de segurança. Esse documento deverá ser atualizado continuamente, alinhando-se às mudanças no ambiente tecnológico e às necessidades do negócio.

X. O Plano de Comunicação deverá estabelecer, de forma clara, os setores a serem notificados de acordo com o tipo de serviço, definindo tempos máximos de resposta e os padrões de mensagens que deverão ser adotados.

XI. A CONTRATADA deverá elaborar, no início de sua atuação, um diagnóstico detalhado das vulnerabilidades existentes no ambiente do CONTRATANTE, conforme previsto na dinâmica de execução. Esse diagnóstico deverá ser apresentado em formato de relatório técnico à equipe do CONTRATANTE, contendo a Matriz de Responsabilidades, as recomendações para correção ou mitigação das

vulnerabilidades identificadas e a aprovação formal do CONTRATANTE. O documento servirá como referência inicial para avaliações mensais subsequentes.

XII. Quando identificadas vulnerabilidades que não possam ser totalmente corrigidas, seja por limitações técnicas ou por razões de negócio, a CONTRATADA deverá notificar formalmente o CONTRATANTE. Essa comunicação assegura a transparência e o pleno entendimento das restrições, permitindo que as partes definam, de forma conjunta, a melhor abordagem de mitigação. A atualização contínua do Plano de Resposta a Incidentes (PRI), do Plano de Comunicação e da Matriz de Responsabilidades será essencial para garantir a eficácia das medidas e a adaptação às mudanças tecnológicas e de negócio.

XIII. Será adotado o padrão Common Vulnerability Scoring System – CVSS (v3.1) como base de pontuação para classificação da severidade das vulnerabilidades, em conformidade com o site do Fórum Global de Equipes de Resposta a Incidentes de Segurança – FIRST.org.

XIV. A CONTRATADA deverá monitorar, identificar e reportar imediatamente todas as vulnerabilidades decorrentes de falhas na implantação ou na aplicação de políticas de segurança nos sistemas corporativos. Caso tais vulnerabilidades não possam ser corrigidas integralmente, deverá haver comunicação formal e imediata ao CONTRATANTE, garantindo o acompanhamento e a tomada de decisão conjunta sobre as medidas compensatórias.

XV. Nesses cenários, a colaboração entre CONTRATANTE e CONTRATADA será indispensável para assegurar uma resposta eficaz, devendo contemplar:

a. comunicação aberta e transparente;
b. identificação conjunta de problemas;
c. desenvolvimento de soluções adequadas;
d. compromisso e flexibilidade das partes envolvidas;
e. implementação e monitoramento contínuos.

1.6.2.1 Definição e natureza dos Incidentes de Segurança

I. As tabelas a seguir apresentam a classificação das categorias de acordo com a sua natureza, o impacto no negócio, o impacto nas informações e o esforço necessário para a recuperação.

II. Essa categorização será utilizada como referência para a aplicação dos percentuais de glosa, sempre que o cálculo depender da gravidade ou da relevância da ocorrência classificada.

PERSPECTIVA	CLASSE	DESCRIÇÃO
Quanto à Natureza	Evento	Algo que ocorreu nos Sistemas de Informações, Infraestrutura ou Dados, mas não é necessariamente malicioso ou que requer uma ação.
	Alerta	Algo potencialmente acionável. Uma indicação de um evento acionável.
	Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, mas **sem impacto à missão ou ao negócio da organização.**
	Incidente Grave	Qualquer evento com violação da confidencialidade, integridade, disponibilidade e privacidade, **com impacto à missão ou ao negócio.**
	Invasão e/ou Vazamento	Perda ou comprometimento de sistemas, dados regulados, ou de propriedade empresarial que dispara uma ação ou resposta legal que vá além dos serviços de monitoramento e resposta a incidentes.
Quanto ao Impacto de Negócio	Nenhum	Nenhum efeito na capacidade da organização de oferecer todos os serviços a todos os usuários.
	Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu eficiência.
	Médio	A organização perdeu a capacidade de fornecer um serviço essencial e crítico para um subconjunto de usuários do sistema.

	Alto	A organização não é mais capaz de fornecer alguns serviços essenciais e críticos a nenhum usuário e/ou houve comprometimento de dados institucionais e/ou pessoais.
	Crítico	A organização não é mais capaz de fornecer alguns serviços essenciais e críticos a nenhum usuário e/ou houve comprometimento de dados institucionais e/ou pessoais.
Quanto ao Impacto de Informações	Nenhum	Nenhuma informação foi exfiltrada, alterada, apagada ou, de qualquer outra forma, comprometida
	Quebra de Privacidade	Informações sensíveis pessoalmente identificáveis (PII), foram acessadas ou exfiltradas.
	Quebra de Propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas
	Perda de Integridade	Informações sensíveis ou proprietárias foram alteradas ou excluídas
Quanto ao Impacto de Recuperação	N/A	Não se aplica
	Regular	O tempo para recuperação é previsível com os recursos existentes.
	Complementado	O tempo para recuperação é previsível com recursos adicionais.
	Estendido	O tempo para recuperação é imprevisível; são necessários recursos adicionais e ajuda externa.
	Não Recuperável	A recuperação do incidente não é possível (por exemplo, os dados sensíveis exfiltrados são publicados; lançar investigação para apuração criminal

1.6.2.2 Apuração

I. A apuração do cumprimento dos Níveis Mínimos de Serviço terá como referência o Relatório de Operação Mensal (ROM), emitido pela CONTRATADA, bem como o Relatório de Acompanhamento resultante dos procedimentos de teste e inspeção conduzidos pela Comissão de Fiscalização do Contrato.

II. No primeiro mês de vigência contratual, contado a partir da assinatura, não serão contabilizados os incidentes decorrentes de vulnerabilidades identificadas no relatório de diagnóstico inicial, a ser entregue pela CONTRATADA no prazo previamente estipulado. Exceção será feita aos incidentes cuja severidade seja classificada como Crítica ou Alta, conforme o padrão CVSS v3.1, os quais deverão receber tratamento prioritário e imediato.

III. Não serão consideradas, para fins de glosa, as vulnerabilidades do tipo zero day. Assim, incidentes que explorem falhas recém-descobertas, sem correções ou mitigações disponibilizadas pelos desenvolvedores, não serão computados. Por definição, vulnerabilidade de “dia zero” consiste em falha de segurança ainda desconhecida pelo desenvolvedor e, portanto, sem correção disponível, oferecendo risco imediato de exploração.

IV. Também não serão contabilizados os incidentes cuja origem esteja vinculada a vulnerabilidades previamente relatadas e nas quais a atuação da equipe de SOC/Blue Team não tenha sido autorizada pelo CONTRATANTE, desde que haja comprovação formal da comunicação da CONTRATADA e da recusa explícita do CONTRATANTE.

V. Do mesmo modo, não serão considerados para aplicação de glosas ou penalidades os incidentes comprovadamente originados de fatores totalmente alheios à atuação da CONTRATADA.

VI. Por outro lado, serão contabilizados, para fins de glosa e penalidade, todos os incidentes de segurança efetivamente sofridos em decorrência de ataques bem-sucedidos contra os sistemas ou a infraestrutura do TJES, ressalvados os testes de invasão conduzidos pelo Red Team.

VII. Os chamados técnicos somente poderão ser encerrados, atestados e validados após o atingimento integral dos objetivos propostos e a entrega dos produtos e serviços com a qualidade exigida, devidamente aprovada pela Equipe de Gestão do Contrato.

VIII. A CONTRATADA estará sujeita à aplicação de glosa no percentual de 0,5% (meio por cento) sobre o valor da fatura, a cada 15 (quinze) pontos ou percentual proporcional ao número de pontos apurados, conforme a tabela de mensuração de qualidade dos Níveis Mínimos de Serviço (Indicadores Operacionais).

IX. Tabela de mensuração de qualidade – Níveis Mínimos de Serviços (Indicadores operacionais):

ID	INDICADOR	FÓRMULA DE CÁLCULO	UNID.	META EXIGIDA	GLOSAS (SOBRE O VALOR MENSAL)
IO1	**Mensal – Índice de Monitoramento de Infraestrutura.** (Percentual de ativos devidamente configurados/monitorados nas ferramentas mantidas pela CONTRATADA (SIEM)	[total de ativos monitorados] / [total de ativos homologados pelo CONTRATANTE para serem monitorados] x 100	%	98%	3 (três) pontos por cada ponto percentual abaixo da meta exigida, aplicado sobre o valor mensal do **Item 01**
IO2	**Mensal – Índice de Monitoramento de Infraestrutura.** (Percentual de ativos devidamente configurados/monitorados nas ferramentas mantidas pela CONTRATADA (SOAR)	[total de ativos monitorados] / [total de ativos homologados pelo CONTRATANTE para serem monitorados] x 100	%	98%	3 (três) pontos por cada ponto percentual abaixo da meta exigida, aplicado sobre o valor mensal do **Item 01**
IO3	**Mensal – Índice de Monitoramento de Infraestrutura.** (Percentual de ativos devidamente configurados/monitorados nas	[total de sistemas, serviços, urls, pessoas, present monitorados] / [total de	%	98%	3 (três) pontos por cada ponto percentual abaixo da meta exigida, aplicado sobre o valor mensal do **Item 01**

	ferramentas mantidas pela CONTRATADA (CTI-DRP)	sistemas, serviços, urls, pessoas, presente em operação] x 100			
IO4	**Mensal – Tempo máximo para a requisição de mudança para aplicação dos Patches e Hotfixes de segurança ou indicação de solução para contorno para tratamento de grave vulnerabilidade com classificação de severidade Alta ou Crítica ou Ameaça Emergente.**	Tempo = [hora da conclusão do planejamento e comunicação da requisição de mudança] – [hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente]	tempo	48:00:00	15 (quinze) pontos, adicionados a 15 (quinze) pontos para cada dia violado, aplicados sobre o valor mensal do **Item 02**
IO5	**Mensal – Índice do Plano de Comunicação.** (não cumpra o escopo ou os prazos especificados no Plano de Comunicação para serviços que apresentarem incidentes de segurança da informação)	[total de plano de comunicação com adequado cumprimento de escopo e prazo] / [Total de plano de comunicação entregue] x 100	%	100%	7 (sete) pontos por cada falta constatada, aplicado sobre o valor mensal do **Item 01**
IO6	**Mensal – Índice de eficiência na comunicação de incidentes, feita pela equipe**	[total de comunicações de incidentes	%	100%	2 (dois) pontos por cada falta constatada, aplicado sobre o valor

	local da CONTRATADA à Central de Serviços de Segurança, aos Gestores do Contrato e ao órgão responsável de acordo com o Plano de Comunicação.	feitas em menos de 15 minutos do conhecimento do problema] / [total de comunicações realizadas] x 100			mensal do **Item 01 e Item 03**
IO7	**Mensal – Índice de incidentes cibernéticos detectados.** (incidentes cibernéticos de algum serviço ocorrido que, por não ter sido corretamente configurada, não foi detectado pela plataforma de SIEM / SOAR / NTA / UEBA / CTI-DRP)	[total de incidentes cibernéticos detectados pela Plataforma] / [total de incidentes cibernéticos ocorridos] x 100	%	100%	5 (cinco) pontos por cada falta constatada, aplicado sobre o valor mensal das **Torres 01 e 02**
IO8	Quantidade de Vulnerabilidades não detectadas e posteriormente identificadas e que resultaram em incidente	Soma das quantidades de vulnerabilidades não relatadas e posteriormente identificadas e que resultaram em incidente	Qt.	0	Quando da ocorrência de vulnerabilidade não identificadas, aplicar-se-ão, de acordo com os níveis de severidade, as seguintes glosas a serem aplicadas sobre o valor mensal dos **itens 01 e 02**: 45 (quarenta e cinco) por incidente resultante, de severidade baixa (limitada a 48 ocorrências durante a vigência do contrato)

					75 (setenta e cinco) por incidente resultante, de severidade média (limitada a 24 ocorrências durante a vigência do contrato)
					150 (cento e cinquenta) por incidente resultante, de severidade alta e crítica (limitada a 6 ocorrências durante a vigência do contrato)
IO9	**Mensal – Índice de eficiência na prevenção de ataques. Quantidade de ataques sofridos com sucesso.**	Soma das quantidades dos ataques sofridos com sucesso	Qtd	0	Quando da ocorrência de ataques sofridos com sucesso, a CONTRATADA será glosada nas **Torres 01 e 02**, na forma a seguir:
					150 (cento e cinquenta) pontos por **impacto ao negócio** com classificação **baixa**, por cada evento, limitada a 3 ocorrências durante a vigência contratual.
					300 (trezentos) pontos por **impacto ao negócio** com classificação **média**, por cada evento, limitada a 2 ocorrências durante a vigência contratual.
					450 (quatrocentos e cinquenta) pontos por **impacto ao negócio**

					com classificação alta, por cada evento, limitada a 1 ocorrência durante a vigência contratual.
IO10	**Mensal – Índice de Disponibilidade do SOC** (falha, degradação ou indisponibilidade de operação do SOC fornecido pela CONTRATADA para a prestação dos serviços.) Ou seja, serão mensuradas as disponibilidades das ferramentas que serão fornecidas nas torres 01 e 01 e 02	[Indisponibilidade das ferramentas] / [tempo contratado de monitoramento dos serviços (24x7)]. Equivalente à: Tempo de disponibilidade mensal [Tempo de disponibilidade – tempos de manutenção preventiva – tempo de indisponibilidade causado por terceiros] x 100	%	99,7%	7 (sete) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador até o limite de 98.7%] 15 (quinze) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador, entre os limites de 98,69% até 97,70%] 20 (vinte) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador abaixo do limite de 97,69%] Aplicado sobre o valor mensal do **item 01.** Obs: Os cálculos se referem a todo o ambiente mantido, ou seja, uma ou mais aplicações/serviços monitorados, a fórmula de cálculo é única,

					tendo como o limite total em 30%.
IO11	**Mensal –** Tempo máximo para correção de incidentes nos serviços de segurança, gerenciados pela CONTRATADA, no caso de indisponibilidade.	Tempo = [hora do restabelecimento] – [hora do início da indisponibilidade]	tempo	1:00:00	150 (cento e cinquenta) pontos adicionados a 3 (três) pontos para cada 10 min de indisponibilidade excedente, aplicados sobre o valor mensal do **Item de serviço que apresentou a indisponibilidade**
IO12	**Mensal – Índice de investigação de incidentes (triagem)** com resolução ou requisições abertas ou resolução do problema em até 15 min	[total de investigação de incidentes com resolução ou requisições abertas em até 15 min] / [total de chamados recebidos] x 100	%	98%	3 (três) pontos por impacto no negócio com classificação **baixa;** 6 (seis) pontos por impacto no negócio com classificação **média;** 7 (sete) pontos por impacto do negócio com classificação **alta;** A serem aplicados sobre o valor mensal do **item 1**
IO13	**Mensal – Índice de resposta** a incidentes e / ou requisições abertas, **em até 1 hora**	[total de respostas a incidentes e ou requisições abertas em até 1 hora do recebimento] / [total de chamados recebidos] x 100	%	80%	4 (quatro) pontos por item cujo impacto no negócio recebeu classificação **baixa;** 7 (sete) pontos por item cujo impacto no negócio recebeu classificação **média;**

					15 (quinze) pontos por item cujo impacto no negócio recebeu classificação **alta;**
					A serem aplicados sobre o valor mensal do **item 3**
IO14	**Mensal – Índice de resposta a incidentes e / ou requisições abertas em até 2 horas**	[total de respostas a incidentes e / ou requisições abertas em até 2 horas do recebimento] / [total de chamados recebidos] x 100%	%	90%	4 (quatro) pontos por item cujo impacto no negócio recebeu classificação **baixa**
					7 (sete) pontos por item cujo impacto no negócio recebeu classificação **média**
					15 (quinze) pontos por item cujo impacto no negócio recebeu classificação **alta**
					A serem aplicados sobre o valor mensal do **item 3**, de forma cumulativa com a glosa descrita no item anterior.
IO15	**Mensal – Índice de recorrência de incidentes e / ou requisições abertas.** (Reincidência de abertura de chamados por falta de atuação da CONTRATADA)	[total de requisições e /ou incidentes reabertos] / [total de solicitações] x 100	%	1%	100 (cem) pontos por quantidade de tickets reabertos, que infrinjam a meta de não-reabertura
				do total de requisições ou solicitações / mês	Aplicado sob o valor mensal do **item 3**
IO16	**Mensal – Índice de atendimento para demandas pela equipe da CONTRATADA alocada**	[total de atendimentos a demandas abertas para a	%	1%	100 (cem) pontos por quantidade de tickets, que infrinjam a meta de

	dentro das dependências físicas do TJES <u>com tempo superior à 15 min</u>.	equipe local, classificadas como severidades <u>altas ou críticas em mais 15 min</u>] / [total de atendimentos a demandas abertas para a equipe local, classificadas como severidades altas ou críticas] x100			tempo de atendimento inferior à 15 min
				do total de requisições ou solicitações / mês	Aplicado sobre o valor mensal dos itens 01
IO17	**Índice de ordens de serviço cumpridas dentro do Prazo. (PENTEST)**	[soma da quantidade de dias fora do prazo acordado]	Qtd	0	150 (cento e cinquenta) pontos por dia de atraso, até o limite de 3 dias.
IO18	**Índice de qualidade do relatório de teste de invasão de acordo com o Tópico específico neste documento**	[soma de inconformidades identificadas]	Qtd	0	45 (quarenta e cinco) pontos por constatação de inconformidade por item, até o limite de 50% dos itens da Ordem de Serviço.
					Aplicado sobre o valor da OS
IO19	**Mensal – Índice de Disponibilidade dos Links de Dados**	[Indisponibilidade do link] / [tempo contratado para fornecimento do link de dados (24x7)].	%	99%	7 (sete) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador até o limite de 98%]
	(falha, degradação ou indisponibilidade de operação do SOC fornecido pela				

	CONTRATADA para a prestação dos serviços.)				
		Equivalente à:			15 (quinze) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador, entre os limites de 97 e 97,9%]
		Tempo de disponibilidade mensal [Tempo de disponibilidade – tempos de manutenção preventiva – tempo de indisponibilidade causado por terceiros] x 100			20 (vinte) pontos [para cada décimo percentual ou fração menor que a meta definida por indicador abaixo do limite de 96,9%]
					Aplicado sobre o valor mensal da fatura.
					Obs: Os cálculos se referem a todo o ambiente mantido, ou seja, uma ou mais aplicações/serviços monitorados, a fórmula de cálculo é única, tendo como o limite total em 30%.
IO20	**Mensal - Índice de Rotatividade da Equipe Técnica (Turnover)**	Quantidade de técnicos que deixaram o contrato ou foram substituídos /	%	<10%	100 pontos caso seja igual ou superior a 10%, incidindo sobre o valor mensal da fatura.

		Quantidade total de técnicos x 100 (cem)			
IO21*	**Mensal - Índice de Aderência dos Profissionais Certificados** ***Este indicador será aferido a partir do 6º mês**	Total de Certificações Apresentadas / Total de Certificações Exigidas em Contrato) × 100	%	100%	100 pontos (90% a 99,9%); 200 pontos (80% a 90%); 300 pontos (abaixo de 80%). A glosa para este item incidirá sobre o valor mensal da fatura.

X. Tabela de mensuração de Indicadores não operacionais

Índice	**Descrição**	**Referência**	**Pontuação (glosa) aferida mensalmente**
INO01	Suspender ou interromper os serviços solicitados, salvo por motivo de força maior ou caso fortuito.	Por ocorrência	5
INO02	Finalizar a requisição de serviço ou incidente sem a anuência do solicitante ou sem que o mesmo tenha sido solucionado, ou deixar de realizar os testes para aferir a efetiva resolução.	Por ocorrência	5
INO03	Deixar de notificar incidentes repetitivos para a equipe de governança de serviços de TI, quer tenham sido conhecidos através do monitoramento ou por notificações de usuários.	Por ocorrência	5

INO04	Registrar, em um chamado, uma solução que não condiz com o solicitado inicialmente, ou registrá-la de forma incompleta sem a descrição das atividades realizadas.	Por ocorrência	5
INO05	Deixar de registrar qualquer ocorrência significativa para o histórico do chamado na ferramenta de Requisição de Serviço e Gerenciamento de TI.	Por ocorrência	2
INO06	Deixar de documentar todas as ocorrências (incidentes, requisições, mudanças, problemas, indisponibilidades) na Ferramenta de Requisição de Serviço e Gerenciamento de TI.	Por ocorrência	10
INO07	Realizar cancelamento de chamado na ferramenta de Gerenciamento de Serviço sem justificativa aceita pelo CONTRATANTE.	Por ocorrência	5
INO08	Fraudar, manipular ou descaracterizar indicadores/metas de níveis de serviço e de desempenho por quaisquer subterfúgios.	Por ocorrência de indicador manipulado	100
INO09	Permitir a presença de profissional sem crachá nos locais onde há prestação de serviço para o CONTRATANTE, após reincidência formalmente notificada.	Por ocorrência	5
INO10	Manter profissionais sem formação ou sem a qualificação exigida para executar os serviços contratados.	Por dia, para cada profissional.	5
INO11	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50
INO12	Causar qualquer dano aos equipamentos do contratante por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50

INO13	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10
INO14	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo CONTRATANTE.	Por ocorrência	50
INO15	Incluir, excluir ou alterar regras dos dispositivos de segurança sem autorização do CONTRATANTE ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	30
INO16	Deixar de comunicar ao contratante a substituição de profissionais responsáveis pela execução das atividades	Por ocorrência	10
INO17	Deixar de cumprir as Políticas de Segurança e de Continuidade de Negócios de TI.	Por ocorrência	10
INO18	Deixar de apresentar os relatórios consolidados para a fiscalização contratual, conforme exigências deste documento, dentro do prazo definido	Por dia de atraso	3
INO19	Deixar de apresentar relatórios, levantamentos e inventários no prazo determinado em comum acordo.	Por ocorrência	10
INO20	Deixar de documentar os Ics e de manter completa e atualizada a Base de Dados de Configuração, inclusive no que diz respeito aos diagramas e desenhos, imediatamente após sua inclusão ou exclusão do ambiente.	Por ocorrência	5
INO21	Deixar de analisar a viabilidade e o impacto da instalação de novas soluções e correções.	Por ocorrência	5

INO22	Deixar de aplicar as políticas de controle de acesso e de gestão da identidade de usuários de TI.	Por ocorrência	5
INO23	Deixar de operar e monitorar proativamente o ambiente de segurança de TIC, que esteja diretamente aos cuidados da CONTRATADA.	Por ocorrência	5
INO24	Deixar de realizar avaliação de impacto, criação de cronograma, monitoramento e controle do processo de mudança ou presen-los de forma deficiente ou incompleta.	Por ocorrência	10
INO25	Deixar de apresentar a proposta de execução de atividades na data acordada com o CONTRATANTE quando de uma Requisição Planejada, ou apresentá-la de forma incompleta.	Por ocorrência	10
INO26	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada.	Por ocorrência	10
INO27	Deixar de comunicar a realização de mudança programada que poderá gerar indisponibilidade em sistemas ou serviços.	Por ocorrência	10
INO28	Deixar de participar de reunião solicitada e previamente agendada com a equipe de gestão de TI do CONTRATANTE	Por ocorrência	5
INO29	Deixar de retirar profissional que se conduza de modo inconveniente, que não respeite as normas do CONTRATANTE ou que não atenda às necessidades, em no máximo 12 horas após a notificação formal.	Por dia incompleto	10
INO30	Deixar de zelar pelas máquinas, equipamentos e instalações do CONTRATANTE utilizados pela CONTRATADA.	Por ocorrência	5

INO31	Deixar de apresentar no prazo definido por este documento as comprovações das capacidades técnicas dos colaboradores da CONTRATADA.	Por mês incompleto de atraso	10
INO32	Deixar de apresentar ao CONTRATANTE o impacto e o cronograma da Solução do Problema no Tempo Máximo para Solução do Incidente do respectivo Incidente que deu origem ao Problema.	Por ocorrência	5
INO33	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	200
INO34	Deixar de zelar pela segurança orgânica das instalações do contratante fornecendo crachá ou credenciais de acesso a pessoas não autorizadas ou, ainda, não verificando o correto fechamento das portas das áreas restritas.	Por ocorrência	40
INO35	Deixar de cumprir, de forma reincidente, qualquer outra obrigação estabelecida no edital e não prevista nesta tabela, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10
INO36	Deixar de buscar a causa raiz de incidentes repetitivos	Por ocorrência	50
INO37	Deixar de implementar soluções definitivas para problemas identificados, que não sejam erros conhecidos e aceitos	Por ocorrência	50
INO38	Deixar de realizar o acompanhamento dos patches a serem aplicados	Por ocorrência	10
INO39	Deixar de aplicar patch de segurança causando algum incidente.	Por ocorrência	200
INO40	Deixar de cumprir o prazo de implantação previsto na Ordem de Serviço sem justificativa aceita pelo CONTRATANTE	Por ocorrência	200

XI. Os chamados técnicos somente poderão ser encerrados, atestados e validados quando todos os objetivos inicialmente propostos tiverem sido plenamente atingidos,

e todos os produtos e serviços realizados e entregues com a qualidade demandada, devidamente aprovada pela Equipe de Gestão do Contrato.

XII. Caso qualquer dos limites de ocorrência, estabelecidos como metas na tabela de mensuração dos Níveis Mínimos de Serviço, seja ultrapassado de forma reincidente, a Administração poderá optar pela rescisão unilateral do contrato, aplicando as sanções previstas no instrumento contratual, ou, alternativamente, aplicar a glosa máxima permitida no mês da constatação do descumprimento.

XIII. As glosas incidirão sobre o valor total da fatura mensal, observados os limites máximos de 30%, tanto para o valor de cada item individualizado, quanto para o valor total a ser faturado no período.

XIV. Será caracterizada inexecução parcial do contrato quando a aplicação de glosas por descumprimento dos Níveis Mínimos de Serviço ocorrer dentro dos limites estabelecidos, por 3 (três) meses consecutivos ou por 5 (cinco) meses intercalados. Nessa hipótese, a CONTRATADA ficará sujeita às sanções previstas no instrumento contratual.

XV. Igualmente, será considerada inexecução parcial do contrato quando a CONTRATADA descumprir de forma recorrente qualquer um dos itens constantes dos Acordos de Níveis de Serviço (ANS) definidos neste documento. Para este fim, entende-se como recorrência os descumprimentos verificados em 5 (cinco) meses consecutivos ou em 7 (sete) meses intercalados, no período de 12 (doze) meses, relativamente ao mesmo item do ANS.

XVI. A ausência de apresentação das certificações exigidas contratualmente, dentro dos prazos estipulados e sem a devida justificativa, poderá configurar inexecução total do contrato.

2.1 Acompanhamento da Execução

I. O preposto indicado pela CONTRATADA atuará como Gerente do Contrato, sendo o responsável direto pelo acompanhamento da execução contratual e pelo papel de interlocutor principal junto ao CONTRATANTE. Caberá a este profissional receber, diligenciar, encaminhar e responder a todas as questões técnicas, administrativas e correlatas relacionadas ao andamento do contrato. O serviço de gerenciamento do contrato e dos diversos serviços nele contemplados será prestado sem ônus adicional.

II. Pela parte do CONTRATANTE, as decisões operacionais ficarão a cargo da Secretaria de Tecnologia da Informação, por intermédio da Coordenadoria de

Infraestrutura e Operações, responsável por fiscalizar a execução contratual e emitir as notificações cabíveis. Esta unidade poderá exigir da CONTRATADA, a qualquer tempo, esclarecimentos, demonstrações e documentos comprobatórios da regularidade da execução.

III. Com o objetivo de facilitar o planejamento e o controle da execução dos serviços, o Gerente do Contrato e o Coordenador da Coordenadoria de Infraestrutura e Operações realizarão reuniões periódicas. O Coordenador poderá, em situações específicas, dispensar reuniões programadas ou, em caso de necessidade, convocar reuniões extraordinárias, às quais o Gerente do Contrato deverá comparecer em até dois dias úteis, ou a critério do CONTRATANTE, poderá participar de forma remota.

IV. Como meios oficiais de comunicação entre CONTRATANTE e CONTRATADA, serão admitidos:
   a. Portal de atendimento (com usuário e senha);
   b. E-mail institucional;
   c. Termo de Notificação

V. Os documentos emitidos por meio desses canais terão plena validade legal para aferição de resultados, comprovação, contestação e demais fins administrativos.

VI. A emissão de aceite dos serviços pelo CONTRATANTE não isenta a CONTRATADA da responsabilidade pela correção de erros identificados durante a execução. Em caso de deficiências, o CONTRATANTE poderá solicitar formalmente sua resolução, cabendo à CONTRATADA providenciar, inclusive junto ao fabricante, todas as medidas necessárias para recompor o nível de serviço exigido nesta contratação, sem ônus adicional.

3.1 Requisitos de Qualificação

I. Durante toda a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com as qualificações específicas previstas no tópico de Requisitos Técnicos. A manutenção das qualificações deverá ser comprovada de forma contínua, assegurando que a equipe técnica esteja permanentemente em conformidade com as exigências contratuais.

II. Nos primeiros seis meses após a assinatura do contrato, período correspondente à fase de implantação, será admitida a apresentação parcial da equipe quanto às qualificações. Essa flexibilização tem como objetivo possibilitar a transição gradual e

estruturada, garantindo que a CONTRATADA organize sua força de trabalho e cumpra as metas estabelecidas para a plena operação do serviço.

III. Para esta fase de implantação, estabelece-se uma gradação progressiva no atendimento às exigências de qualificação, nos seguintes termos:
   a. Nos dois primeiros meses, a equipe deverá apresentar comprovação de, no mínimo, 20% das qualificações requeridas.
   b. Entre o terceiro e o quarto mês, deverá estar comprovado, no mínimo, 40% das qualificações exigidas.
   c. Entre o quinto e o sexto mês, a equipe deverá demonstrar, no mínimo, 60% das qualificações previstas.

IV. Ao término da fase de implantação, a CONTRATADA deverá garantir que a equipe técnica esteja completamente constituída e que 100% das qualificações obrigatórias tenham sido devidamente atendidas, em estrita observância às especificações técnicas estabelecidas neste documento.

3.1.1 Da Qualificação Técnico-Profissional

I. A composição da equipe técnica deverá ser integralmente provida e dimensionada pela CONTRATADA, devendo esta assegurar a adequada relação entre o quantitativo de profissionais alocados, sua produtividade individual e os prazos definidos no contrato. Caberá à CONTRATADA garantir que a força de trabalho disponibilizada seja suficiente para atender, de forma contínua e eficiente, às demandas previstas neste documento.

II. Adicionalmente, a CONTRATADA deverá prover aos profissionais todos os recursos necessários ao desempenho adequado das funções, incluindo ferramentas, equipamentos e insumos, de modo a assegurar a plena execução dos serviços sem ônus adicional para o CONTRATANTE.

3.1.2 Da comprovação dos Requisitos de Qualificação

I. Para fins de comprovação do atendimento aos requisitos de qualificação profissional, serão aceitos certificados ou diplomas apresentados em cópia simples acompanhada do documento original, ou em cópia autenticada, desde que comprovem a conclusão dos cursos exigidos.

II. Todos os documentos fornecidos pela CONTRATADA estarão sujeitos à diligência do CONTRATANTE, que poderá adotar os meios necessários para confirmar a veracidade das informações apresentadas.

III. Nos casos em que determinada certificação não possua mais validade, será admitida a certificação que oficialmente a substitua, desde que emitida por entidade reconhecida.

IV. Poderão ainda ser utilizadas certificações equivalentes às listadas nas tabelas de certificados previstas neste Termo de Referência, desde que comprovada a equivalência técnica. Nessas situações, o pedido de análise deverá ser formalizado junto ao CONTRATANTE, acompanhado da documentação comprobatória pertinente.

V. As certificações técnicas exigidas deverão permanecer válidas durante todo o período de execução contratual.

VI. Para efeito de comprovação das formações acadêmicas, deverão ser observadas as disposições da Portaria MEC nº 70, de 24 de janeiro de 2025.

3.1.3 Da comprovação do Vínculo Empregatício

I. Todos os profissionais envolvidos na execução dos serviços deverão possuir vínculo formal com a CONTRATADA, seja por meio da Consolidação das Leis do Trabalho (CLT), seja mediante contratação de pessoa física por meio de empresa individual, em conformidade com a jurisprudência consolidada pelo Tribunal de Contas da União (TCU).

II. O Acórdão nº 1189/2025 - Plenário do TCU consolidou o entendimento de que não é admissível a imposição absoluta de vínculo celetista em todas as contratações de tecnologia da informação. O Tribunal reconheceu como válida a contratação de profissionais por meio de pessoa física constituída em empresa individual, desde que não caracterizada fraude trabalhista, consignando expressamente nos itens 42 e 43:

> *"42. Na área de tecnologia da informação essa modalidade ganhou espaço significativo, principalmente em contratações sem dedicação exclusiva de mão de obra, como as aqui tratadas, que permitem uma maior autonomia do profissional, que comumente exerce suas funções de forma remota, permitindo a liberdade na prestação de serviço para diferentes contratantes e sua alocação somente nas etapas do projeto em que se faz necessário, diminuindo a ociosidade do trabalhador e os custos para as empresas*

> *contratantes. Não se pode ignorar a realidade do mercado e as novas formas de contratação existentes, desde que, é claro, não impliquem em práticas fraudulentas, que, todavia, não podem ser presumidas pela simples adoção do modelo, mas devidamente comprovadas pelas circunstâncias de cada caso concreto."*
> *43. Assim, contratar uma pessoa física para prestar serviços por meio de uma empresa individual, por ser essa uma prática comum do mercado de tecnologia da informação, não é o mesmo que subcontratar uma determinada empresa para assumir uma parte do serviço devido à falta de capacidade técnica da contratada para isso, ou por uma maior especialização da subcontratada. Entende-se, portanto, que a vedação à subcontratação não implica a obrigatoriedade de contratação pelo vínculo celetista, não impedindo outras formas de contratação admitidas pelo Direito e pela jurisprudência." (BRASIL. Tribunal de Contas da União. Acórdão nº 1189/2025 – Plenário. Relator: Ministro Walton Alencar Rodrigues. Sessão de 29 de maio de 2025. Brasília, DF: TCU, 2025).*

III. Assim, a comprovação do vínculo poderá se dar por qualquer uma dessas duas modalidades, cabendo sempre à CONTRATADA a responsabilidade integral pelas obrigações legais, contratuais e trabalhistas aplicáveis.

IV. A CONTRATADA deverá comprovar mensalmente perante a fiscalização do contrato o vínculo profissional de todos os colaboradores alocados na execução dos serviços, mediante apresentação de documentação idônea que demonstre a regularidade trabalhista ou contratual da relação mantida, garantindo transparência e segurança jurídica na execução do objeto. Essa comprovação deverá ocorrer, preferencialmente, em conjunto com a entrega do relatório mensal da operação.

4.1 Garantia dos Serviços

I. Durante toda a vigência contratual, a CONTRATADA deverá assegurar suporte técnico permanente para todos os serviços objeto do contrato, abrangendo tanto atividades consultivas quanto operacionais, de modo a garantir o pleno funcionamento das soluções e a efetividade dos mecanismos de monitoramento e segurança implantados.

II. O suporte deverá contemplar a correção de falhas, inconsistências ou interrupções que venham a afetar a continuidade dos serviços, observando os níveis de serviço (SLAs) previamente pactuados. O atendimento será prestado diretamente pela equipe designada da CONTRATADA, com a devida especialização técnica, sem que haja repasse de custos adicionais ao CONTRATANTE, respeitadas as condições estabelecidas no contrato.

III. O serviço deverá estar disponível em regime contínuo (24x7x365), com prazo máximo de quatro horas para resposta inicial em situações críticas, garantindo pronta atuação diante de incidentes e acompanhamento integral das soluções até sua completa normalização.

IV. A CONTRATADA deverá ainda disponibilizar múltiplos canais de atendimento, tais como telefone, e-mail, portal de chamados e recursos de acesso remoto, de forma a facilitar a comunicação, agilizar o registro de ocorrências e reduzir a burocracia no processo de suporte.

V. O escopo do suporte incluirá, no mínimo:
   a. análise e resolução de falhas operacionais e técnicas;
   b. diagnóstico e tratamento de incidentes relacionados às ferramentas de monitoramento e segurança contratadas;
   c. aplicação de correções, atualizações e upgrades necessários ao bom funcionamento das soluções utilizadas;
   d. realização periódica de relatórios sobre desempenho e conformidade das ferramentas;
   e. implementação de medidas preventivas que evitem a reincidência de falhas e assegurem a continuidade operacional.

VI. Na hipótese de se constatar a necessidade de adequação ou substituição de componentes essenciais, caberá à CONTRATADA adotar, em prazo célere, as medidas corretivas, sem prejuízo da manutenção da operação regular do ambiente tecnológico do CONTRATANTE.

VII. Por fim, a CONTRATADA deverá atuar em conformidade com as políticas institucionais de segurança da informação, garantindo que todas as recomendações de melhoria e planos de ação corretiva sejam formalmente registrados e submetidos ao acompanhamento da fiscalização contratual.

5.1 Requisitos de Segurança da Informação

I. São requisitos exigidos com relação à Política de Segurança da Informação, na forma da Resolução nº 079/2024, do Ato Normativo nº 41/2018 e do Ato Normativo nº 42/2018, do Ato Normativo nº 161/2024, do Ato Normativo nº 124/2024, do Ato Normativo nº 143/2024, Ato normativo nº 240/2024, Ato normativo nº 139/2024, Ato normativo nº 145/2024 todos deste PJES, devendo a CONTRATADA:

a. Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo CONTRATANTE
b. Executar todos os testes de segurança necessários e definidos nas legislações pertinentes, bem como executar seus trabalhos dentro das diretrizes ali estabelecidas.
c. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do PJES ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar seus empregados nesse sentido.
d. Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos eventualmente disponibilizados para a execução dos serviços, não cabendo ao PJES qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer, cabendo à CONTRATADA o seu ressarcimento, em quantidade e qualidade, sem prejuízo das penalidades cabíveis.
e. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do PJES.
f. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou de rescisão do Contrato, as informações relativas:
    i. À Política de Segurança adotada pelo PJES e as configurações de hardware e de softwares decorrentes;
    ii. Ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos;
    iii. Ao processo de implementação, no ambiente do PJES, dos mecanismos de criptografia e autenticação.
g. A Lei Geral de Proteção de Dados será obedecida, em todos os seus termos, pela CONTRATADA, obrigando-se ela a tratar os dados da CONTRATANTE que forem eventualmente coletados, conforme sua necessidade ou obrigatoriedade. (art. 7º, LGPD).
h. Conforme prevê a Lei Geral de Proteção de Dados, obriga-se a CONTRATADA a executar os seus trabalhos e tratar os dados da CONTRATANTE respeitando os princípios da finalidade, adequação, transparência, livre acesso, segurança, prevenção e não discriminação (art. 6º, LGPD).

i. A CONTRATADA obriga-se a garantir a confidencialidade dos dados coletados da CONTRATANTE por meio de uma política interna de privacidade, a fim de respeitar, por si, seus funcionários e seus prepostos, o objetivo do presente termo (art. 50, LGPD).

j. Eventuais dados coletados pela CONTRATADA serão arquivados por esta somente pelo tempo necessário para a execução dos serviços contratados. Ao seu fim, os dados coletados serão permanentemente eliminados, excetuando-se os que se enquadrarem no disposto no artigo 16, I da Lei Geral de Proteção de Dados (art. 15, LGPD).

k. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

l. O Adendo I - Termo de Confidencialidade, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada e por seus empregados diretamente envolvidos na contratação, encontra-se disponível neste documento.

5.1.2 Requisitos de Segurança Institucional

I. Durante a execução do contrato, a CONTRATADA deverá zelar pelo cumprimento da Resolução nº 21/2017 do PJES, dando ciência do seu conteúdo a todos os seus respectivos técnicos.

II. O CONTRATANTE deverá cientificar a CONTRATADA sobre as normas internas vigentes relativas à segurança, inclusive aquelas relacionadas ao controle de acesso de pessoas e veículos, bem como sobre a Política de Segurança da Informação.

III. Para que a CONTRATADA atenda aos requisitos exigidos com relação à Política de Controle de Acesso, deverá:

IV. Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências do PJES, assumindo quaisquer prejuízos porventura causados por dolo ou culpa de seus profissionais.

V. Solicitar, por escrito, credenciamento e autorização de acesso para os recursos humanos da CONTRATADA.

VI. Informar e solicitar ao GESTOR ou FISCAL TÉCNICO do CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas, o descredenciamento dos recursos desvinculados da prestação de serviços com o CONTRATANTE.

VII. Devolver para o CONTRATANTE todos os recursos e equipamentos eventualmente disponibilizados, como crachás, cartões certificadores, “pendrives” e outros, de propriedade do CONTRATANTE, juntamente com a solicitação de descredenciamento.

6.1. Requisitos Sociais, Ambientais e Culturais

I. A CONTRATADA deverá orientar sua equipe técnica sobre as boas práticas voltadas ao consumo consciente, redução de desperdício dos recursos naturais e coleta seletiva, inclusive à adequada destinação dos resíduos porventura gerados na execução do contrato, com o objetivo de contribuir para a preservação do meio ambiente, quando aplicável;

II. Os profissionais da CONTRATADA que desempenharão as atividades em contato direto junto ao CONTRATANTE, deverão cumprir os seguintes requisitos:

   a. Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando vestuário que comprometa a imagem institucional do CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;

   b. Respeitar todos os servidores e demais colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

   c. Atuar nas dependências do CONTRATANTE, se necessário, com urbanidade e cortesia.

III. Quanto aos critérios ambientais, a CONTRATADA deverá cumprir os seguintes requisitos de uso racional de recursos:

   a. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em em atendimento ao Art. 9º

da Política de Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);

b. As configurações de hardware e software deverão ser realizadas visando ao alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;
c. Utilizar de forma eficiente o espaço de armazenamento virtual e oferecer o máximo de desempenho de processamento com o menor impacto ou comprometimento da capacidade de processamento dos recursos tecnológicos do CONTRATANTE.

7.1 Requisitos Legais

I. A pretensa contratação tem como referência os seguintes instrumentos legais: Constituição Federal de 1988; Lei nº 14.133/2021; Resolução nº 468/2022 do CNJ; Instrução Normativa nº 94/2022 do ME; e demais instrumentos correlatos.

7.1.1 Do Sigilo

I. São consideradas confidenciais informações ou dados armazenados a que a CONTRATADA tenha acesso, e também aqueles transmitidos oralmente, por escrito ou eletronicamente, em razão da execução deste objeto, independentemente de expressa menção à sua confidencialidade.
II. A CONTRATADA, para fins de sigilo, se obriga por seus administradores, empregados, prepostos a qualquer título, sucessores e comissários.
III. A CONTRATADA deverá seguir os protocolos de segurança e envidará os melhores esforços para evitar backdoors e vulnerabilidades nos serviços objeto deste contrato. Na hipótese de vazamento de informações, a CONTRATADA se responsabilizará por eventuais perdas e danos causados ao CONTRATANTE.
IV. Sem prejuízo das disposições relativas à Segurança da Informação previstas neste documento, quaisquer incidentes de segurança, incluídos, mas não limitados aos ataques por hackers e/ou invasões de qualquer natureza e/ou vulnerabilidades técnicas que exponham ou tenham o potencial de expor o ambiente onde se encontram hospedados informações e dados do PJES, deverão ser imediatamente comunicados pela CONTRATADA ao CONTRATANTE, mesmo que se trate de meros indícios, guardando todos os registros (inclusive logs, metadados e outras

evidências dos incidentes e providências correspondentes) visando subsidiar a realização de eventual auditoria.

V. Caso a CONTRATADA receba uma solicitação de acesso emitida por uma autoridade governamental, do Brasil ou do exterior, aos dados do PJES armazenados em decorrência da execução deste objeto, a CONTRATADA deverá dar ciência imediata ao CONTRATANTE, ressalvadas as hipóteses legais de sigilo na investigação e desde que expressamente exigido, por escrito, pela autoridade.

VI. A CONTRATADA envidará seus melhores esforços para questionar, administrativa ou judicialmente, às suas próprias expensas, solicitações de acesso por autoridades governamentais que não possuam inequívoco respaldo legal, antes de conceder o acesso requerido.

VII. O descumprimento pela CONTRATADA da obrigação de sigilo, revelando informações e dados confidenciais ou facilitando sua revelação, poderá ensejar na rescisão do contrato.

8.1 Atendimento da Demanda

8.1.1 Portal do Software Público Brasileiro

Após análise, verifica-se que os serviços de segurança da informação previstos neste documento, como Gestão de Vulnerabilidades, Gestão de Patches, Cofre de Senhas, Monitoramento de Ataques Cibernéticos, Resposta a Incidentes, Pentests, SIEM, SOAR e Threat Intelligence, não encontram correspondência no catálogo do Portal do Software Público Brasileiro (SPB). Tais soluções exigem ferramentas de classe Enterprise, com suporte especializado, certificações internacionais de conformidade (ISO 27001, SOC 2, FIPS, entre outras) e capacidade de integração em ambientes críticos, requisitos que não são contemplados por softwares disponíveis no SPB, os quais se concentram em aplicações administrativas, de gestão documental e de participação social.

Ressalta-se, contudo, que ferramentas do SPB poderiam ser utilizadas de forma complementar em áreas de apoio, como gestão de processos, protocolos eletrônicos ou fluxos de comunicação interna, mas não substituem as soluções específicas de segurança da informação exigidas no objeto contratual. Dessa forma, para a prestação dos serviços aqui previstos, permanece de responsabilidade da CONTRATADA o fornecimento, operação e sustentação das soluções adequadas, em conformidade com os requisitos técnicos e regulatórios estabelecidos.

8.1.2 Soluções de TIC

I. Tendo em vista as necessidades identificadas e considerando que foi afastada a possibilidade de atendimento da demanda com recursos humanos e tecnológicos internos, procedeu-se à análise das soluções atualmente disponíveis no mercado de TIC. A partir desse levantamento preliminar, foram selecionadas duas alternativas que se mostraram mais compatíveis com os requisitos do TJES, levando-se em conta, especialmente, a relação custo-benefício e a aderência técnica às necessidades institucionais.

II. Essas alternativas serão objeto de estudo mais aprofundado, com vistas à verificação detalhada de sua viabilidade, abrangência funcional, requisitos de integração, sustentabilidade e conformidade com os marcos regulatórios aplicáveis. Tal análise permitirá fundamentar a decisão final de contratação com maior segurança e transparência, em alinhamento às diretrizes estratégicas da administração.

Solução 1 - Estruturação de Equipe Própria de Segurança da Informação

Nesta alternativa, o Tribunal optaria por estruturar uma equipe própria para desempenhar diretamente as funções de monitoramento, gestão de vulnerabilidades, resposta a incidentes e demais serviços de segurança da informação. O modelo prevê a contratação de profissionais especializados, aquisição de ferramentas e licenciamento de softwares necessários, além da criação de rotinas internas de operação e governança.

A adoção de uma equipe interna permitiria maior autonomia na execução das atividades de segurança, reduzindo a dependência de fornecedores externos e garantindo domínio pleno sobre processos e dados sensíveis. Haveria ainda maior flexibilidade para adequar procedimentos às especificidades do TJES, com possibilidade de consolidar uma equipe estratégica para médio e longo prazo, alinhada às políticas institucionais e às demandas do Poder Judiciário.

Contudo, para viabilizar esse modelo, seriam necessárias adequações relevantes. O TJES enfrenta um cenário de escassez de pessoal técnico, agravado pela alta rotatividade decorrente de vínculos precários, como contratações temporárias, que dificultam a consolidação do conhecimento institucional. A constituição de uma equipe robusta demandaria concurso público, o que não se mostra viável em curto prazo. Além disso, os

custos fixos com pessoal, capacitação contínua e licenciamento de ferramentas tenderiam a ser elevados, reduzindo a flexibilidade orçamentária.

Nesse contexto, embora a solução de equipe própria apresente benefícios em termos de soberania e autonomia, seu sucesso dependeria de um plano consistente de gestão de pessoas, com investimentos em capacitação, manutenção de certificações técnicas, políticas de retenção de talentos e previsão de orçamento para a renovação tecnológica. Sem tais condições, o risco de fragilidade operacional e de descontinuidade dos serviços seria elevado.

Solução 2 - Serviços Gerenciados de Segurança da Informação

A primeira alternativa avaliada corresponde à contratação de Serviços Gerenciados de Segurança da Informação, ofertados sob a forma de um portfólio de serviços destinados a complementar as competências da equipe técnica do TJES. Essa abordagem contempla a atuação como provedor especializado em detecção e resposta a ameaças, assumindo, ainda, a responsabilidade pelo monitoramento e gerenciamento de dispositivos de segurança já existentes no ambiente institucional. Tais dispositivos podem ser de diferentes fabricantes e arquiteturas, abrangendo Firewalls, Sistemas de Prevenção de Intrusão (IPS) e soluções de Gerenciamento Unificado de Ameaças (UTM), entre outros.

O objetivo central desta solução é reduzir os riscos associados a alterações não autorizadas em informações sensíveis, bem como mitigar ataques capazes de comprometer a segurança de ativos críticos da infraestrutura tecnológica. Para isso, a empresa contratada deve disponibilizar equipe qualificada e processos estruturados, assegurando a continuidade e a qualidade da prestação dos serviços.

A remuneração, por sua vez, está vinculada a um valor mensal fixo, condicionado ao atingimento das metas estabelecidas nos Níveis Mínimos de Serviço (NMS). O modelo prevê, ainda, a aplicação de glosas como mecanismo de controle financeiro em caso de descumprimento dos indicadores pactuados, garantindo maior previsibilidade e transparência no acompanhamento contratual.

8.1.3 Contratações Públicas Similares

Órgão 1 - Banco do Nordeste - BNB

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	ESTRATÉGIA / FASE / DATA	EMPRESA VENCEDORA	QUANTIDADE	PREÇO TOTAL DO CONTRATO
Serviços Gerenciados de Segurança da Informação	Pregão Eletrônico nº 127/2020	Homologado	ISH Tecnologia S/A	1	5.998.000,00

Órgão 2 - Supremo Tribunal Federal - STF

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	ESTRATÉGIA / FASE / DATA	EMPRESA VENCEDORA	QUANTIDADE	PREÇO TOTAL DO CONTRATO
Serviços Gerenciados de Segurança da Informação	Pregão Eletrônico nº 08/2023	Homologado	Kryptus Segurança da Informação Central It Tecnologia da Informacão S/A Harpia Tecnologia LTDA	3 lotes	R$ 3.522.999,92

Órgão 3 - Tribunal de Justiça do Rio de Janeiro

SOLUÇÃO	IDENTIFICAÇÃO DA CONTRATAÇÃO	ESTRATÉGIA / FASE / DATA	EMPRESA VENCEDORA	QUANTIDADE	PREÇO TOTAL DO CONTRATO

Serviços Gerenciados de Segurança da Informação	Pregão Eletrônico nº 50/2022	Homologado	Future Technologies Informática Ltda.	1	R$ 45.607.999,92

8.1.4 Orçamento Estimado

I. A elaboração do orçamento estimado enfrentou limitações relevantes quanto ao uso de contratações similares como parâmetro comparativo. Os serviços relativos à operação de um Centro de Operações de Segurança (SOC) apresentam alto grau de personalização, o que dificulta a obtenção de referências uniformes de preços no âmbito da Administração Pública.

II. Diversos fatores influenciam diretamente a precificação desses serviços, tais como: o tipo de fornecimento adotado, o número de ativos contemplados, a inclusão ou não de licenças no escopo, a eventual incorporação de equipamentos, a quantidade de ativos monitorados, bem como a existência prévia de licenças parciais em poder do órgão contratante. Cada um desses elementos gera variações expressivas nos valores praticados, tornando inviável a comparação direta com contratos já celebrados por outros entes públicos.

III. Outro aspecto que agrava a impossibilidade de comparação é a forma de descrição do objeto nas licitações anteriores. Frequentemente, os itens são agrupados, fracionados ou redigidos com nomenclaturas distintas para designar serviços equivalentes, o que compromete a identificação de similaridades efetivas com o objeto ora pretendido. Essa diversidade terminológica e técnica impede a construção de um paralelo seguro e juridicamente defensável.

IV. Diante desse cenário, para viabilizar a pesquisa de mercado e assegurar maior fidedignidade às estimativas, optou-se por considerar exclusivamente as cotações apresentadas por fornecedores especializados que se dispuseram a elaborar propostas com base nas especificações técnicas gerais estabelecidas neste Estudo Técnico Preliminar, as quais passam a compor a cesta de preços utilizada para formação do valor de referência, conforme segue:

LOTE 01									
ITEM	**Quantidade**	**ISH - Unit.**	**ISH - Total**	**BI4.0 - Unit.**	**BI4.0 - Total**	**Future - Unit.**	**Future - Total**	**GC - Unit.**	**GC - Total**
1 - Serviço de Administração, Operação, Manutenção e Atendimento de Requisições	24 meses	R$ 110.577,89	R$ 2.653.869,36	R$ 57.600,00	R$ 1.382.400,00	R$ 79.166,66	R$ 1.899.999,84	-	-
2 - Serviço de gestão de vulnerabilidades	24 meses	R$ 323.476,01	R$ 7.763.424,24	R$ 72.000,00	R$ 1.728.000,00	R$ 95.416,66	R$ 2.289.999,84	-	-
3- Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança	24 meses	R$ 781.052,60	R$ 18.745.262,40	R$ 120.000,00	R$ 2.880.000,00	R$ 262.500,00	R$ 6.300.000,00	-	-
4 - Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security	24 meses	R$ 110.936,22	R$ 2.662.469,28	R$ 96.000,00	R$ 2.304.000,00	R$ 150.000,00	R$ 3.600.000,00	-	-

Orchestration, Automation and Response – SOAR)									
5 - Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)	24 meses	R$ 23.260,23	R$ 558.245,52	R$ 38.400,00	R$ 921.600,00	R$ 45.833,33	R$ 1.099.999,92	-	-
6 - Gerenciamento de Patches (Patch Management)	24 meses	R$ 61.525,79	R$ 1.476.618,96	R$ 48.000,00	R$ 1.152.000,00	R$ 95.208,33	R$ 2.284.999,92	-	-
TOTAL LOTE 01	-	**R$ 33.859.889,76**		**R$ 10.368.000,00**		**R$ 17.474.999,52**		-	-

LOTE 02									
ITEM	**Quantidade**	**ISH - Unit.**	**ISH - Total**	**BI4.0 - Unit.**	**BI4.0 - Total**	**Future - Unit.**	**Future - Total**	**GC - Unit.**	**GC - Total**
1 - Gray Box (Caixa Cinza)	500	R$ 767,14	R$ 383.570,00	R$ 320,00	R$ 160.000,00	R$ 380,00	R$ 190.000,00	R$ 849,95	R$ 424.975,00

2 - Black Box (Caixa Preta)	1500	R$ 767,14	R$ 1.150.710,00	R$ 320,00	R$ 480.000,00	R$ 280,00	R$ 420.000,00	R$ 850,70	R$ 1.276.050,00
TOTAL LOTE 02	-	**R$ 1.534.280,00**		**R$ 640.000,00**		**R$ 610.000,00**		**R$ 1.701.025,00**	

8.1.5 Da Metodologia da Cálculo para Custo Estimado

I. A definição do valor estimado da contratação observou critérios estatísticos de aferição de tendência central e dispersão, aplicados aos valores unitários coletados junto aos fornecedores que apresentaram propostas.

II. Inicialmente, para cada item do objeto foram calculadas as seguintes métricas:

   a. **Média aritmética ($\bar{x}$)**: obtida pela soma dos valores unitários ofertados dividida pelo número de observações. Representa a tendência central quando os dados são homogêneos.
   b. **Mediana (med)**: corresponde ao valor central da amostra, separando-a em duas metades iguais. É uma medida mais robusta, adequada em cenários de elevada dispersão ou presença de valores extremos.
   c. **Desvio padrão (s)**: expressa a variação absoluta dos dados em relação à média, indicando o grau de dispersão dos preços cotados. Quanto maior o desvio padrão, maior a distância dos valores em relação à média.
   d. **Coeficiente de variação (CV):** resulta da divisão entre o desvio padrão e a média, expresso em percentual. Essa métrica permite avaliar a homogeneidade relativa dos preços coletados.

III. Em conformidade com a literatura estatística e com boas práticas aplicadas na formação de preços públicos, adotou-se a seguinte regra metodológica:

   a. **Para CV inferior ou igual a 25%**, considera-se que os dados apresentam homogeneidade, de modo que a média aritmética é utilizada como valor de referência.
   b. **Para CV superior a 25%**, considera-se que os dados apresentam heterogeneidade ou elevada dispersão, devendo-se adotar a mediana como valor de referência, por ser menos sensível a valores extremos e mais representativa do conjunto de preços coletados.

IV. Essa metodologia assegura que o orçamento estimado seja construído com base em critérios técnicos e estatísticos objetivos, preservando a razoabilidade dos valores de referência e mitigando distorções que poderiam advir da simples adoção de uma média aritmética em cenários de grande dispersão dos dados.

V. Na tabela abaixo, se observa a cálculo para obtenção do coeficiente de variação (CV), conforme segue:

Lote	Item	Média ($\bar{x}$)	Mediana (med)	Desvio padrão (s)	CV (%)	Método recomendado
Lote 01	1 - Serviço de Administração, Operação, Manutenção e Atendimento de Requisições	R$ 82.448,18	R$ 79.166,66	R$ 26.640,96	32,3%	**Mediana**
	2 - Serviço de gestão de vulnerabilidades	R$ 163.630,89	R$ 95.416,66	R$ 138.924,19	84,9%	**Mediana**
	3- Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança	R$ 387.850,87	R$ 262.500,00	R$ 347.896,92	89,7%	**Mediana**
	4 - Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response – SOAR)	R$ 118.978,74	R$ 110.936,22	R$ 27.883,89	23,4%	**Média**
	5 - Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)	R$ 35.831,19	R$ 38.400,00	R$ 11.503,71	32,1%	**Mediana**
	6 - Gerenciamento de Patches (Patch Management)	R$ 68.244,71	R$ 61.525,79	R$ 24.310,79	35,6%	**Mediana**
Lote 02	1 - Gray Box (Caixa Cinza)	R$ 579,27	R$ 573,57	R$ 268,01	46,3%	**Mediana**
	2 - Black Box (Caixa Preta)	R$ 554,46	R$ 543,57	R$ 296,25	53,4%	**Mediana**

8.1.6 Do Valor Estimado da Contratação

I. Após a aplicação da metodologia estatística descrita anteriormente, foram consolidados os valores de referência para cada item do objeto da contratação. O critério adotado considerou, para cada serviço, o método mais adequado entre a média e a mediana, conforme a análise do coeficiente de variação (CV), assegurando maior fidedignidade aos resultados.

II. Dessa forma, apenas os itens cujo CV apresentou homogeneidade relativa (igual ou inferior a 25%) tiveram o valor de referência definido pela média aritmética. Para os demais, em que se constatou elevada dispersão (CV superior a 25%), adotou-se a mediana como medida representativa.

III. O resultado deste processamento foi a composição de uma tabela final, que apresenta o custo estimado de cada item do contrato, bem como os subtotais por lote e o valor global da estimativa de referência. Esse valor global servirá de base para a condução do processo licitatório, garantindo transparência, previsibilidade e observância ao princípio da economicidade.

ORÇAMENTO ESTIMADO DA CONTRATAÇÃO					
Lote	**Item/Serviço**	**Método adotado**	**Valor unitário (R$)**	**Quantidade**	**Valor total estimado (R$)**
Lote 01	1 - Serviço de Administração, Operação, Manutenção e Atendimento de Requisições	Mediana	R$ 79.166,66	24 meses	R$ 1.899.999,84
	2 - Serviço de gestão de vulnerabilidades	Mediana	R$ 95.416,66	24 meses	R$ 2.289.999,84
	3- Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança	Mediana	R$ 262.500,00	24 meses	R$ 6.300.000,00
	4 - Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response – SOAR)	Média	R$ 118.978,74	24 meses	R$ 2.855.489,76
	5 - Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)	Mediana	R$ 38.400,00	24 meses	R$ 921.600,00
	6 - Gerenciamento de Patches (Patch Management)	Mediana	R$ 61.525,79	24 meses	R$ 1.476.618,96

SUBTOTAL LOTE 1					**R$ 15.743.708,40**
Lote 02	1 - Gray Box (Caixa Cinza)	Mediana	R$ 573,57	500	R$ 286.785,00
	2 - Black Box (Caixa Preta)	Mediana	R$ 543,57	1.500	R$ 815.355,00
SUBTOTAL LOTE 2					**R$ 1.102.140,00**
TOTAL GLOBAL					**R$ 16.845.848,40**

8.1.7 Modelos de Aquisição/Prestação do Serviço

I. **Equipe Própria (Aquisição de Softwares de Segurança da Informação e Capacitação Interna)**

Este modelo prevê que o TJES invista na formação de uma equipe própria de profissionais especializados em segurança da informação. Para tanto, seria necessário realizar concurso público ou processos seletivos, adquirir as ferramentas e soluções de mercado requeridas e promover o treinamento contínuo dos servidores, incluindo a obtenção e renovação de certificações técnicas.

A adoção desse formato traria maior autonomia ao Tribunal no controle direto das atividades de segurança, além de favorecer a consolidação do conhecimento técnico dentro da instituição. Entretanto, tal modelo exigiria esforço expressivo em recursos humanos e orçamentários, com riscos relacionados à escassez de mão de obra qualificada, alta rotatividade de profissionais e custos elevados para manter a capacitação e atualização tecnológica constantes.

II. **Serviços Gerenciados de Segurança da Informação (Empresa Especializada)**

Neste modelo, o TJES contrata uma empresa especializada para a prestação dos serviços de segurança, englobando operação, monitoramento, sustentação e resposta a incidentes, de acordo com os níveis mínimos de serviço (NMS) e indicadores de desempenho acordados contratualmente. A responsabilidade pela gestão de equipe, atualização tecnológica e operação contínua das ferramentas de segurança recairia sobre a contratada, cabendo ao TJES a supervisão e fiscalização técnica do contrato.

Essa alternativa possibilita o acesso imediato a profissionais experientes e certificados, com menor risco de descontinuidade dos serviços, já que a contratada assume o compromisso de garantir a disponibilidade de especialistas conforme o escopo. O modelo, contudo, implica maior dependência do fornecedor e menor autonomia interna, ainda que mitigado pelo acompanhamento rigoroso por parte do contratante.

III. **Equipe Própria (Aquisição de Softwares de Segurança da Informação e Capacitação Interna)**
    a. **Vantagens**

i. Maior autonomia do TJES na execução das atividades de segurança da informação.
ii. Retenção e consolidação de conhecimento técnico dentro da instituição.
iii. Possibilidade de alinhar diretamente as práticas de segurança às prioridades estratégicas do Tribunal.
iv. Redução de dependência externa e de eventuais riscos contratuais.

b. **Desvantagens**

i. Necessidade de realização de concurso público ou processos seletivos, o que demanda tempo e recursos.
ii. Escassez de mão de obra qualificada no mercado, dificultando a formação de equipe própria em tempo hábil.
iii. Custos elevados para aquisição de ferramentas, treinamentos e certificações contínuas.
iv. Risco de rotatividade e evasão de profissionais capacitados para o setor privado, que oferece remuneração mais competitiva.
v. Maior tempo necessário para alcançar plena maturidade operacional e técnica.

IV. Serviços Gerenciados de Segurança da Informação (Empresa Especializada)

a. **Vantagens**

i. Acesso imediato a equipe qualificada e certificada, com experiência consolidada em segurança da informação.
ii. Rapidez na implementação e na operacionalização dos serviços.
iii. Redução dos riscos de indisponibilidade devido à obrigação contratual de manter equipe dimensionada.
iv. Atualização contínua de ferramentas, processos e metodologias, sob responsabilidade da contratada.
v. Possibilidade de mensuração clara de desempenho por meio de Níveis Mínimos de Serviço (NMS) e indicadores de qualidade.

b. **Desvantagens**

i. Dependência do fornecedor para a execução de atividades críticas de segurança.
ii. Menor internalização de conhecimento técnico dentro do TJES.
iii. Necessidade de acompanhamento e fiscalização rigorosa por parte do contratante.
iv. Riscos associados à eventual troca ou descontinuidade do prestador de serviço.
v. Potenciais limitações de customização da solução, já que a contratada pode adotar práticas padronizadas.

V. Matriz Comparativa de Modelos

Aspecto	Solução 1 – Equipe Própria (Aquisição e Capacitação Interna)	Solução 2 – Serviços Gerenciados de Segurança da Informação (Empresa Especializada)
Custo Inicial	Alto: aquisição de ferramentas, capacitação, concurso ou contratações temporárias.	Médio/Alto: depende da abrangência do contrato, mas diluído ao longo da vigência.
Custo de Manutenção	Elevado: treinamentos contínuos, certificações, atualização de tecnologia.	Incluído no contrato: atualização, suporte e dimensionamento de equipe ficam sob responsabilidade da contratada.
Tempo de Implementação	Longo: exige estruturação da equipe, capacitação e adaptação ao ambiente.	Curto: execução imediata após assinatura e implantação do contrato.
Risco de Continuidade	Alto: risco de evasão de profissionais para o setor privado e perda de conhecimento.	Médio: mitigado por obrigação contratual, mas sujeito à troca de fornecedor.
Flexibilidade	Alta: equipe interna atua conforme diretrizes estratégicas do TJES.	Média: depende do escopo contratual e da capacidade de customização da empresa.

Maturidade Técnica	Baixa a médio prazo: demanda tempo para consolidação.	Alta: acesso imediato a expertise consolidada e certificada.
Dependência Externa	Baixa: maior autonomia institucional.	Alta: dependência direta da contratada para execução das atividades.
Governança e Controle	Elevado: gestão totalmente interna, com maior alinhamento institucional.	Médio: exige fiscalização e monitoramento dos níveis de serviço.
Risco de Não Atendimento	Alto: dificuldade em reter e formar equipe pode comprometer prazos e qualidade.	Médio/Baixo: riscos mitigados pelos Acordos de Nível de Serviço (NMS) e penalidades contratuais.

8.1.8. Capacidade e alternativas do mercado de TIC

Alternativas do mercado de TIC avaliadas no item de Análise dos Custos Totais da Demanda.

8.1.9. Contratações correlatas e/ou interdependentes

Não é aplicável.

8.1.10 Análise dos Custos Totais da Demanda

Nota explicativa para Solução 1 - Equipe Própria

I. Considerando que nenhum outro Órgão da administração pública adotou a solução apresentada, realizou-se um levantamento estimado de custos para abarcar um valor aproximado caso a administração optasse por essa solução.

   a. **Custo de Pessoal**

      i. O principal custo de um SOC interno está associado à formação da equipe técnica. Para um SOC de porte adequado ao TJES, estima-se a necessidade de 15 profissionais entre analistas de diferentes níveis e perfis técnicos especializados.

a) O salário-base médio de analista foi estimado em R$ 9.900,00, acrescido de auxílios obrigatórios (alimentação, saúde, creche), totalizando aproximadamente R$13.580,00 por colaborador/mês.
b) Considerando a contribuição patronal de 22%, o custo mensal por profissional alcança cerca de R$15.378,00.
c) Para uma equipe de 15 pessoas, o custo mensal é de R$230.670,00, resultando em R$ 2.768.040,00 ao ano e R$5.536.080,00 em dois anos.
d) Além disso, estima-se um custo adicional de R$375.000,00 em certificações e treinamentos, para manter a equipe alinhada às exigências técnicas.
e) Subtotal Pessoal (2 anos): R$5.911.080,00

b. **Infraestrutura e Licenciamento**

i. A implementação e operação de um Centro de Operações de Segurança (SOC) em ambiente interno exige a disponibilidade de um ecossistema tecnológico de caráter corporativo, em padrão Enterprise, capaz de assegurar escalabilidade, resiliência e confiabilidade no tratamento contínuo de incidentes.

a) SIEM (Security Information and Event Management)

(1) O núcleo funcional de um SOC é o SIEM (Security Information and Event Management), solução responsável pela ingestão massiva de logs, análise de eventos, correlação de dados e geração de alertas acionáveis, constituindo-se como ferramenta indispensável para a gestão de riscos cibernéticos e para a conformidade com normativos nacionais e internacionais de segurança da informação.
(2) No atual estágio, não é possível afirmar com precisão o número de eventos por segundo (EPS) que serão processados no ambiente do Tribunal, cabendo à empresa contratada realizar a devida mensuração, considerando as particularidades da infraestrutura em produção. Todavia, estimativas baseadas em tribunais

de porte equivalente indicam métricas médias na ordem de 12.000 EPS, parâmetro que serve de referência para cálculos preliminares de licenciamento. À luz desses indicadores, os valores praticados no mercado situam-se em torno de R$ 1.500.000,00 por ano, alcançando aproximadamente R$ 3.000.000,00 em um período contratual de dois anos. Esse investimento reflete não apenas a criticidade do componente SIEM, mas também a necessidade de licenciamento aderente às demandas institucionais de alta disponibilidade, escalabilidade e interoperabilidade com as demais camadas tecnológicas de proteção.

b) Ferramenta de Gestão de Vulnerabilidades

(1) A efetividade de um SOC depende, de forma estruturante, da capacidade de identificar, priorizar e mitigar vulnerabilidades em todos os ativos tecnológicos sob sua esfera de monitoramento. Nesse contexto, mostra-se imprescindível a disponibilização de uma solução corporativa de Gestão de Vulnerabilidades, apta a realizar varreduras contínuas, análises de risco, priorização baseada em criticidade e integração com os demais componentes de segurança cibernética.

(2) Considerando o inventário atual da instituição, estima-se a necessidade de cobertura de aproximadamente 10.000 endpoints adicionais, o que torna necessário o complemento de licenciamento de uma plataforma de mercado robusta e consolidada, como o Tenable One ou outra solução equivalente que assegure aderência às melhores práticas internacionais. Tal ferramenta constitui pilar essencial para a manutenção da postura de segurança da informação, permitindo a detecção tempestiva de exposições críticas, a geração de relatórios executivos e técnicos e a integração com sistemas de resposta a

incidentes, de forma a conferir maior eficácia ao processo decisório e à proteção do ambiente institucional.

(3) Para a cobertura integral do parque e a integração com os demais componentes do SOC, projeta-se investimento na ordem de R$ 3.000.000,00 no horizonte de dois anos, abrangendo licenciamento, suporte e atualizações.

c) Infraestrutura complementar (hardware, storage, appliances, links)

(1) A plena operacionalização de um Centro de Operações de Segurança (SOC) requer infraestrutura tecnológica dedicada, de alta disponibilidade e com redundância em todos os níveis críticos. Tal infraestrutura deve contemplar servidores de alto desempenho, sistemas de armazenamento (storage) escaláveis, appliances de segurança especializados (como firewalls de última geração, balanceadores e dispositivos de inspeção profunda de pacotes) e redundância de links de comunicação, de modo a garantir continuidade operacional, resiliência a falhas e suporte adequado ao elevado volume de dados de segurança processados em tempo real.

(2) Esse arcabouço tecnológico constitui o alicerce sobre o qual se apoiam as demais camadas de defesa cibernética, permitindo o correto funcionamento de soluções de SIEM, gestão de vulnerabilidades, resposta a incidentes e orquestração de segurança. Sua ausência ou dimensionamento inadequado comprometeria diretamente a capacidade do SOC de detectar, correlacionar e responder a ameaças em tempo hábil.

(3) Considerando os custos de mercado para aquisição, manutenção e suporte de tais ativos, projeta-se um investimento estimado em R$ 2.000.000,00 para o

horizonte de dois anos, valor que contempla tanto a aquisição de equipamentos quanto os contratos de suporte técnico, atualização de firmware e garantias estendidas necessárias à sustentação da operação em nível corporativo.

c. Tabela Resumo – Estimativa de Custos da Solução 1 (Equipe Própria)

ITEM	DESCRIÇÃO	CUSTO ESTIMADO (2 ANOS)
Pessoal	15 profissionais SOC (salários, encargos, auxílios) + certificações	R$ 5.911.080,00
SIEM	Licenciamento para ~12.000 EPS	R$ 3.000.000,00
Gestão de Vulnerabilidades	Complementação ao Tenable One (14.200 endpoints adicionais)	R$ 1.500.000,00
Infraestrutura complementar	Servidores, storage, appliances, links redundantes	R$ 2.000.000,00
Total Geral (2 anos)		**R$ 12.411.080,00**

A implementação de um SOC interno, com equipe própria e dedicada, representa uma alternativa robusta, porém onerosa e de alta complexidade para o TJES. Além dos custos já estimados com pessoal, infraestrutura, licenciamento e treinamento, é importante destacar que essa solução, mesmo sendo abrangente, **não contempla integralmente todas as frentes de segurança cibernética necessárias**.

Entre os serviços que ficariam descobertos ou exigiriam contratações adicionais, destacam-se:

I. **Testes de Penetração (Pentests):** fundamentais para validar de forma prática as vulnerabilidades exploráveis no ambiente. Uma equipe SOC interna, ainda que qualificada, não substitui a atuação independente de um time de Red Team especializado.
II. **Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP):** envolve monitoramento contínuo em surface, deep e dark web, bem como ações de takedown de conteúdos fraudulentos, falsos perfis e domínios maliciosos, atividades geralmente terceirizadas a empresas especializadas.
III. **Serviços de inteligência de ameaças avançadas e consultorias específicas:** apoio em investigações forenses, resposta a incidentes complexos, análises avançadas de malware, entre outros.

Ou seja, ainda que o custo estimado da Solução 1 seja de R$12.400.00,00 em dois anos, permanece a necessidade de novas contratações complementares para assegurar a cobertura plena do escopo de segurança definido neste documento.

Seq.	Soluções Identificadas	Especificação do produto/serviço	Catmat/Catser	Quantificação do Produto ou Serviço	Órgão (s) que adotou a solução	Vantagens e Benefícios	Desvantagens e riscos	Custo (s) envolvido (s)
1	Equipe própria	Aquisição de Softwares de Segurança da Informação e Capacitação Interna	-	1	Nenhum	• Maior autonomia institucional e domínio interno dos processos de segurança da informação. • Acúmulo de conhecimento e experiência dentro da equipe técnica do TJES. • Possibilidade de adaptação direta às necessidades específicas da instituição.	• Necessidade de realização de concursos públicos ou contratações específicas, o que demanda tempo e enfrenta restrições orçamentárias e legais. • Alto custo de capacitação continuada e dificuldade de retenção de profissionais qualificados diante da concorrência do mercado privado. • Risco de obsolescência tecnológica pela demora na formação da equipe e pela necessidade de constante atualização. • Prazo de maturidade elevado para atingir nível adequado de resposta a	R$ 12.411.080,00

							incidentes. ●	
2	Empresa Especializada	Prestação de Serviços Gerenciados de Segurança da Informação	27014	1	STF CNJ TJRJ TJBA BNB TJSP	● Acesso imediato a equipe altamente qualificada e certificada, com experiência consolidada em diversos ambientes institucionais. ● Redução do tempo de implementação e maior maturidade operacional desde o início da execução contratual. ● Previsibilidade financeira, com pagamento condicionado ao cumprimento de Níveis Mínimos de Serviço (NMS). ● Transferência de responsabilidade pela atualização de ferramentas, manutenção de certificações e atendimento a requisitos regulatórios.	● Dependência da contratada para manutenção da operação e da continuidade dos serviços. ● Necessidade de gestão contratual rigorosa para garantir o cumprimento dos níveis de serviço e a qualidade das entregas. ● Risco de custos adicionais em caso de necessidade de serviços fora do escopo contratado.	R$ 16.845.848,40

						• Mitigação de riscos de descontinuidade e vulnerabilidades críticas, assegurando maior resiliência cibernética.		

8.2 Escolha e Justificativa da Solução

8.2.1 Descrição da Solução Escolhida

Solução 2 - Empresa Especializada (Solução Viável)

A escolha da solução a ser adotada pelo Tribunal de Justiça do Estado do Espírito Santo deve considerar não apenas o custo direto de implantação, mas também a maturidade técnica, a velocidade de execução, a amplitude de serviços cobertos e a sustentabilidade ao longo da vigência contratual. A análise comparativa das duas alternativas estudadas, qual seja, a constituição de uma estrutura interna (Solução 1) e a contratação de empresa especializada em serviços gerenciados de segurança da informação (Solução 2), revelou diferenças significativas que fundamentam a decisão em favor da segunda.

A constituição de um SOC próprio, ainda que possa conferir maior controle administrativo e certa autonomia sobre os processos, mostrou-se uma alternativa de elevado custo e baixa viabilidade operacional. Para sua efetiva implementação seria necessária a contratação de aproximadamente quinze profissionais especializados em segurança cibernética, todos em regime de dedicação exclusiva e com qualificações técnicas certificadas em padrões internacionais. Além do elevado custo salarial e dos encargos trabalhistas associados, o Tribunal teria que arcar com benefícios e gratificações, bem como com um programa contínuo de capacitação, de modo a manter a equipe atualizada frente à rápida evolução das ameaças cibernéticas.

Essa equipe, ainda que numerosa, não seria capaz de abranger integralmente todos os serviços necessários a um SOC moderno. Faltariam, por exemplo, serviços de Digital Risk Protection (DRP), que exigem equipes especializadas em investigação em ambientes de deep e dark web, além de provedores com acordos internacionais de cooperação para a execução de serviços de takedown. Do mesmo modo, os testes de penetração especializados, que demandam profissionais certificados em metodologias específicas como OSSTMM, NIST e OWASP, dificilmente poderiam ser realizados de forma contínua com equipe própria, implicando em novas contratações. Soma-se a isso a necessidade de aquisição de ferramentas de mercado de classe enterprise, tais como o Tenable One ou solução equivalente para gestão de vulnerabilidades, plataformas SIEM licenciadas para volumes expressivos de eventos por segundo (EPS), soluções de SOAR para orquestração de resposta a incidentes e ferramentas de análise avançada de riscos digitais. Esses

custos, somados aos já elevados gastos com pessoal, tornariam o modelo insustentável financeiramente e de alto risco operacional.

Outro ponto crítico da Solução 1 refere-se ao tempo necessário para alcançar maturidade. A contratação de equipe própria esbarraria em dificuldades de mercado, considerando a escassez de profissionais altamente qualificados em segurança cibernética e a forte competição com a iniciativa privada, que oferece remunerações atrativas. Mesmo que fosse possível atrair tais profissionais, haveria uma curva de aprendizado natural até que a equipe estivesse plenamente integrada aos processos do Tribunal, o que implicaria risco de falhas, atrasos e vulnerabilidades não endereçadas durante os primeiros meses – ou até anos – de operação. A experiência de outros órgãos demonstra que a maturidade de um SOC próprio é resultado de longo prazo, exigindo investimentos constantes e nem sempre compatíveis com a realidade orçamentária do setor público.

A Solução 2, por sua vez, afasta tais limitações ao transferir para uma empresa especializada a responsabilidade integral pela implantação, operação e sustentação dos serviços de segurança cibernética. Diferentemente do SOC próprio, essa alternativa garante ao Tribunal o acesso imediato a profissionais experientes e certificados, com conhecimento acumulado em múltiplos clientes e setores, capazes de aplicar metodologias atualizadas de resposta a incidentes, gestão de vulnerabilidades e monitoramento contínuo. A amplitude da cobertura é notadamente superior: além de monitoramento por SIEM e gestão de vulnerabilidades, estão incluídos serviços de DRP, testes de penetração, orquestração e automação de resposta a incidentes (SOAR), monitoramento em 24x7x365 e relatórios técnicos e executivos em tempo real, todos já integrados em uma única proposta contratual.

Sob a ótica financeira, a contratação de empresa especializada proporciona previsibilidade orçamentária, uma vez que os custos são consolidados em valor mensal fixo, condicionado ao atingimento de Níveis Mínimos de Serviço (NMS). Esse modelo elimina a necessidade de aquisição direta de licenças de ferramentas de segurança, pois a contratada assume a responsabilidade de prover e sustentar tais soluções, liberando o Tribunal de investimentos iniciais milionários em licenciamento e manutenção. Além disso, a existência de mecanismos contratuais de glosa assegura que o serviço somente seja remunerado quando o desempenho esperado for efetivamente alcançado, o que não ocorreria em uma estrutura própria, onde os custos com pessoal e licenças permaneceriam inalterados independentemente da qualidade da entrega.

Comparando os dois cenários, percebe-se que a Solução 1, além de financeiramente mais onerosa, apresenta lacunas técnicas relevantes que impedem a composição de um SOC completo e moderno. Faltariam serviços críticos como testes de penetração especializados e monitoramento de riscos digitais em ambientes obscuros da internet, indispensáveis no atual contexto de ameaças. A Solução 2, ao contrário, apresenta-se como alternativa de maior abrangência, menor risco e custo mais eficiente, garantindo ao Tribunal não apenas a execução dos serviços, mas também o alinhamento imediato a padrões internacionais de segurança da informação e conformidade regulatória.

Diante desse comparativo, a opção pela Solução 2 é justificada de maneira inequívoca. A contratação de empresa especializada em serviços gerenciados de segurança cibernética assegura a entrega integral do escopo requerido, dentro dos parâmetros de eficiência, economicidade e efetividade exigidos pelo contrato BID nº 5883/OC-BR, ao passo que a constituição de um SOC próprio implicaria em elevados custos, prazos extensos de maturação e lacunas técnicas que comprometeriam a segurança institucional. Assim, considerando o interesse público, a proteção dos ativos críticos de informação do TJES e a necessidade de resultados imediatos, opta-se pela Solução 2 como a mais adequada, segura e sustentável.

8.2.2 Benefícios Esperados

A adoção da solução escolhida para a gestão integrada de segurança da informação no PJES traz consigo um conjunto de benefícios diretos e indiretos que se alinham tanto às necessidades imediatas da instituição quanto às diretrizes estratégicas do Poder Judiciário.

Em primeiro lugar, a contratação de serviços especializados viabiliza a estruturação de um Centro de Operações de Segurança (SOC) robusto e em conformidade com padrões internacionais de boas práticas. Ao contrário da alternativa de composição de equipe própria, que demandaria investimentos elevados em contratações, capacitações, certificações e ferramentas, a solução adotada permite a entrega imediata de um ambiente maduro, sustentado por profissionais já certificados e com experiência consolidada em ambientes de missão crítica.

Do ponto de vista técnico, a solução garante maior abrangência e especialização. Enquanto a formação de equipe própria ficaria restrita a determinadas frentes de atuação, a contratação especializada engloba serviços adicionais que são indispensáveis para a plena defesa cibernética, como os testes periódicos de penetração (pentests), a gestão de

vulnerabilidades com uso de ferramentas Enterprise (a exemplo do Tenable), a orquestração de respostas (SOAR) e o Gerenciamento de Proteção contra Riscos Digitais (Digital Risk Protection - DRP). Dessa forma, o TJES terá à sua disposição um portfólio completo de serviços, abrangendo desde a detecção precoce até a resposta estruturada e documentada a incidentes.

Outro benefício relevante refere-se à eficiência na gestão de riscos e conformidade regulatória. A solução contratada possibilita a implementação de processos de monitoramento e resposta em aderência a frameworks como NIST, SANS e MITRE ATT&CK, bem como a observância das exigências da LGPD, da Resolução CNJ nº 468/2022 e de normas internacionais de segurança da informação. Essa aderência contribui para elevar a maturidade institucional e garantir segurança jurídica e técnica ao Tribunal, mitigando riscos de sanções administrativas e de comprometimento da imagem institucional.

Adicionalmente, espera-se como benefício a otimização de custos e recursos internos. Ao centralizar a gestão da segurança da informação em um contrato de serviços especializados, o TJES evita dispersão de esforços na formação e retenção de equipes próprias, que historicamente enfrentam elevada rotatividade devido à concorrência do setor privado. Esse modelo permite que os servidores do TJES concentrem sua atuação em atividades de planejamento, governança e alinhamento estratégico, enquanto a execução operacional de segurança é desempenhada por profissionais dedicados, com alta disponibilidade (24x7x365).

Outro aspecto central é a garantia de continuidade e evolução tecnológica. O contrato prevê a atualização contínua das ferramentas e metodologias utilizadas, incluindo feeds de inteligência de ameaças, frameworks atualizados e integração com novas tecnologias que venham a surgir. Isso assegura que o Tribunal não ficará defasado frente ao avanço constante das técnicas de ataque cibernético, beneficiando-se de uma proteção dinâmica e atualizada.

Por fim, a solução escolhida trará ganhos em transparência, rastreabilidade e controle, por meio de indicadores de desempenho (KPIs) e relatórios consolidados que permitem acompanhar a efetividade das ações de segurança. Esses relatórios, discutidos em reuniões mensais de alinhamento, permitem que a alta administração do TJES tenha clareza sobre os riscos enfrentados, os incidentes tratados e a eficácia das medidas aplicadas, fortalecendo a governança institucional.

Assim, os benefícios esperados da solução vão muito além da proteção técnica do ambiente de TIC. Eles abrangem a sustentabilidade da operação, o cumprimento de marcos regulatórios, a otimização de custos, a mitigação de riscos reputacionais e a consolidação do TJES como uma instituição moderna, resiliente e preparada para os desafios da transformação digital.

8.2.3 Resultados Esperados

Tipo	Detalhamento
(X) Ganho de Produtividade	A centralização das atividades de monitoramento, resposta a incidentes e gestão de vulnerabilidades em uma estrutura de SOC permite eliminar dispersões de esforço e retrabalho, otimizando a utilização dos recursos humanos do TJES. A atuação de uma equipe dedicada e certificada garante maior velocidade no tratamento de eventos, reduzindo o tempo de resposta e permitindo que os servidores internos concentrem-se em atividades de planejamento e governança de TIC.
(X) Redução de Esforço Operacional	A automação de processos, proporcionada por ferramentas de SIEM, SOAR e gestão de vulnerabilidades, reduz a necessidade de intervenções manuais. Atividades complexas, como coleta de logs, correlação de eventos e orquestração de respostas, passam a ser executadas automaticamente, diminuindo o esforço humano e evitando falhas decorrentes de operações repetitivas.
(X) Melhoria na Segurança e Conformidade	A implementação de processos estruturados e baseados em frameworks reconhecidos internacionalmente (NIST, SANS, MITRE ATT&CK) permite maior eficácia na identificação e mitigação de riscos cibernéticos. Isso fortalece a resiliência institucional frente a ataques, além de assegurar conformidade com legislações como a LGPD e com normativos do CNJ (Resolução 468/2022).
(X) Aumento da Confiabilidade das Informações	Com a utilização de ferramentas Enterprise de monitoramento e detecção de ameaças, todos os eventos de segurança passam a ser rastreados e registrados de forma precisa e auditável. Esse processo garante maior confiabilidade nos relatórios de incidentes e

	fornece insumos para auditorias internas e externas, contribuindo para a governança e a tomada de decisão estratégica.
(X) Continuidade dos Serviços Críticos	A rápida detecção e contenção de incidentes de segurança reduz a probabilidade de indisponibilidade dos sistemas judiciais críticos, assegurando que serviços como o PJe, portais e sistemas administrativos permaneçam ativos e com performance adequada. Isso resulta em maior estabilidade para magistrados, servidores e usuários externos.
(X) Redução de Riscos Reputacionais	O fortalecimento da defesa cibernética mitiga a ocorrência de incidentes que possam resultar em exposição de dados sensíveis ou indisponibilidade de sistemas, preservando a credibilidade institucional do TJES perante a sociedade e órgãos de controle.
(X) Transparência e Governança	A disponibilização de indicadores de desempenho em portal dedicado e a apresentação periódica de relatórios executivos e técnicos proporcionam maior visibilidade sobre a efetividade das ações de segurança. Isso assegura transparência no uso dos recursos e fortalece os mecanismos de governança digital.

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

Lote	Item	Descrição	CATSER	Unidade	Qtd unitária	Qtd total
1	1	Serviço de Administração, Operação, Manutenção e Atendimento de Requisições	27014	Serviço	1	24
	2	Serviço de gestão de vulnerabilidades	27014	Serviço	1	24
	3	Serviço Gerenciado	27014	Serviço	1	24

		de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança				
	4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response – SOAR)	27014	Serviço	1	24
	5	Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection - DRP)	27014	Serviço	1	24
	6	Gerenciamento de Patches (Patch Management)	27014	Serviço	1	24
2	1	Gray Box (Caixa Cinza)	27014	Unidade	1	500
	2	Black Box (Caixa Preta)	27014	Unidade	1	1500

8.2.5 Estimativa do Custo Total da Solução Escolhida

Lote	Item	Descrição	Qtd total	Valor unitário	Valor total

1	1	Serviço de Administração, Operação, Manutenção e Atendimento de Requisições	24 meses	R$ 79.166,66	R$ 1.899.999,84
	2	Serviço de gestão de vulnerabilidades	24 meses	R$ 95.416,66	R$ 2.289.999,84
	3	Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança	24 meses	R$ 262.500,00	R$ 6.300.000,00
	4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and Response – SOAR)	24 meses	R$ 118.978,74	R$ 2.855.489,76
	5	Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)	24 meses	R$ 38.400,00	R$ 921.600,00
	6	Gerenciamento de Patches (Patch Management)	24 meses	R$ 61.525,79	R$ 1.476.618,96
SUBTOTAL LOTE 1					**R$ 15.743.708,40**
2	1	Gray Box (Caixa Cinza)	500	R$ 573,57	R$ 286.785,00
	2	Black Box (Caixa Preta)	1500	R$ 543,57	R$ 815.355,00
SUBTOTAL LOTE 2					**R$ 1.102.140,00**
TOTAL GLOBAL					**R$ 16.845.848,40**

8.3 Declaração de Viabilidade da Contratação

A equipe responsável pelo planejamento da contratação, após a conclusão dos estudos técnicos preliminares, declara ser viável e adequada a contratação pretendida.

9. SUSTENTAÇÃO DO CONTRATO

9.1. Adequação do Ambiente

Não é aplicável.

9.2 Recursos Materiais e Humanos

Não é aplicável.

9.3 Continuidade do Fornecimento

Situação	Ação Preventiva	Responsável
Encerramento abrupto do contrato	Não aplicável preventivamente, pois trata-se de evento imprevisto.	Secretaria de Tecnologia da Informação (STI)
	Ação de Contingência: Providenciar a contratação direta, se as empresas remanescentes da licitação não aceitarem as mesmas condições oferecidas pelo licitante vencedor, atendida a ordem de classificação, conforme legislação vigente. Caso não seja possível, deverá ser realizado o planejamento e abertura de nova licitação em caráter emergencial.	Seção de Contratação / STI
Esgotamento do contrato pelo término da vigência	**Ação Preventiva**: Iniciar o planejamento de nova contratação com antecedência mínima de 12 (doze) meses antes do término do contrato, assegurando tempo hábil para tramitação processual, análise técnica e homologação.	Equipe de Planejamento da Contratação
	Ação de Contingência: Caso a nova contratação não seja concluída em tempo hábil, adotar providências para prorrogação do contrato vigente, em caráter excepcional, dentro dos limites legais, mediante justificativa técnica e aprovação da autoridade competente.	Gestor do Contrato

9.4 Transição Contratual e Encerramento do Contrato

I. A transição contratual constitui etapa essencial para garantir a continuidade e a integridade da prestação dos serviços de tecnologia da informação e segurança cibernética do TJES, evitando descontinuidade, perda de conhecimento ou falhas nos processos críticos. Nesse sentido, a CONTRATADA deverá elaborar e executar um **Plano de Transição Contratual**, aprovado previamente pelo CONTRATANTE, contemplando as ações necessárias para assegurar a transferência ordenada das atividades, processos, dados, acessos, ferramentas e responsabilidades, seja em caso de término natural da vigência contratual ou de rescisão antecipada.

II. Durante o período de transição, a CONTRATADA deverá manter a plena execução dos serviços contratados, respeitando integralmente os Acordos de Nível de Serviço (ANS/NMS), sem que o processo de substituição de profissionais, de tecnologias ou de ferramentas impacte a operação. A CONTRATADA também deverá prestar suporte e repassar informações às equipes técnicas do CONTRATANTE ou à nova empresa contratada, mediante reuniões técnicas, relatórios detalhados, registros de chamados, documentação de processos, manuais e inventários de ativos.

III. Ao final do contrato, a CONTRATADA deverá entregar relatório de encerramento contendo:
    a. descrição das atividades executadas;
    b. status dos serviços em operação;
    c. incidentes em aberto e respectivas tratativas;
    d. recomendações de continuidade e melhoria;
    e. registros técnicos e administrativos relacionados à execução contratual;
    f. documentação atualizada de topologia, configuração, integrações, manuais de operação e acessos.

IV. Fica vedada a retenção de informações, credenciais, registros ou quaisquer artefatos que comprometam a continuidade operacional do ambiente do TJES. A CONTRATADA deve garantir a devolução integral de todos os ativos físicos e lógicos que lhe tenham sido disponibilizados, sob pena de responsabilização civil e administrativa.

V. No caso de rescisão contratual abrupta, a CONTRATADA deverá prestar suporte imediato ao processo de contingência, assegurando que as informações e registros sejam devidamente entregues ao CONTRATANTE, de modo a mitigar os impactos da interrupção.

VI. O período de transição contratual terá um prazo máximo de 03 (três) meses, podendo variar conforme a complexidade dos serviços e o tempo necessário para a absorção pela nova contratada ou equipe interna. A CONTRATADA deverá manter profissionais qualificados até a conclusão da transição, sob pena de glosas e sanções contratuais.

VII. A assistência de que trata o item anterior se refere a todo e qualquer esforço necessário para a migração das cargas de trabalho para outro provedor de nuvem, fornecendo, inclusive, informações técnicas que auxiliem a transição, além da disponibilização dos especialistas da CONTRATADA para acompanhamento e assessoramento durante a transição, dentre outros de igual complexidade e importância.

VIII. A CONTRATADA deverá destruir ou eliminar as informações do CONTRATANTE apenas após concluída a assistência prevista acima, condicionada à autorização expressa e por escrito do CONTRATANTE.

IX. A CONTRATADA deverá emitir um termo informando que os dados foram destruídos, de acordo com o padrão NIST 800-88.

X. Reversão: Arquitetura Física e Lógica

a. Dos pilares para a reversão:

1. Arquitetura Física: Refere-se aos componentes tangíveis da rede.

A CONTRATADA deverá:

- Reinstalar os equipamentos de rede originais que foram removidos ou substituídos durante o contrato, nos locais de origem.
- Restabelecer a fiação e a patcheagem conforme o layout anterior, removendo quaisquer cabos ou conexões adicionais implementadas.
- Desinstalar e remover todos os equipamentos, softwares e acessórios que foram incorporados à infraestrutura da CONTRATANTE para fins exclusivos da execução deste contrato, salvo se houver acordo de compra ou cessão em contrário.

XI. Licenciamento: Em caso de rescisão ou término do contrato, a CONTRATADA se compromete a desvincular seu acesso e a entregar à CONTRATANTE todas as

credenciais de acesso e informações necessárias para que esta mantenha o controle total e irrestrito ao ambiente. A CONTRATADA não terá qualquer direito de retenção sobre os dados, que são de propriedade exclusiva da CONTRATANTE.

1. Arquitetura Lógica: Refere-se à configuração e ao software que define o funcionamento da rede.

   A CONTRATADA deverá:

   - Reaplicar as configurações originais nos equipamentos de rede (roteadores, switches, firewalls), incluindo:
   - Esquema de endereçamento IP anterior (sub-redes, gateways).
   - Configurações de VLAN (Virtual Local Area Network) preexistentes.
   - Regras de ACL (Access Control List) e políticas de firewall originais.
   - Protocolos de roteamento e configurações de DNS/DHCP, se aplicável.

   Garantir a funcionalidade completa da rede no estado revertido, assegurando que todos os serviços dependentes (conectividade, acesso à internet, acesso a servidores) estejam operantes conforme estavam antes do início do contrato.

XII. Aceitação pós-Readequação:

a. Plano de Reversão: A CONTRATADA deverá apresentar um Plano de Reversão detalhado para aprovação da CONTRATANTE com a antecedência do término do contrato.
b. Execução: A reversão será executada em data e horário previamente acordados entre as Partes, preferencialmente fora do horário comercial crítico, para minimizar impactos.
c. Testes e Aceitação Final: Após a conclusão dos trabalhos, as partes realizarão testes conjuntos para verificar se a rede foi restabelecida em sua condição original e está plenamente funcional. A formalização de um Termo de Aceitação será obrigatória para o encerramento das obrigações deste item.

9.4.1 Ações para o Encerramento Contratual

Ação	Responsável	Prazo
Destruição ou eliminação das informações do CONTRATANTE	Contratada	Após conclusão da assistência prevista na transição contratual, condicionada à autorização expressa e por escrito do CONTRATANTE
Emissão de um termo informando que os dados foram destruídos, de acordo com o padrão NIST 800-88.	Contratada	Após a conclusão do item imediatamente anterior
Cancelamento de contas, senhas e permissões concedidas e utilizadas nos provedores de nuvem	Contratada	Ao final do contrato
Reversão da Arquitetura Física e Lógica	Contratada	Ao final do contrato

9.5 Estratégia de Independência Tecnológica

I. Transferência de Conhecimento
   a. A CONTRATADA deverá realizar treinamentos sob demanda, sempre que requisitado pelo CONTRATANTE, a fim de garantir que a equipe técnica interna possua conhecimento suficiente para acompanhar, fiscalizar e, quando necessário, assumir a gestão mínima dos serviços contratados.
   b. Para o repasse de conhecimento relacionado aos serviços de segurança da informação e operação do SOC, a CONTRATADA deverá fornecer ao CONTRATANTE manuais, roteiros técnicos e documentação detalhada, preferencialmente em idioma português brasileiro, viabilizando a utilização

efetiva das soluções contratadas, independentemente da execução de treinamentos formais.

c. A CONTRATADA deverá disponibilizar ao CONTRATANTE, sem custos adicionais, materiais de apoio, guias operacionais, acesso a ambientes de treinamento disponibilizados pelos fabricantes das soluções e relatórios técnicos que permitam à equipe do CONTRATANTE consolidar sua capacidade de supervisão e auditoria dos serviços.

II. Repasse Final de Informações

a. Ao término do contrato, a CONTRATADA deverá repassar ao CONTRATANTE todas as informações necessárias à continuidade da operação dos serviços, incluindo, no mínimo:

i. Todos os artefatos técnicos e operacionais, incluindo dados, registros de incidentes, workflows, scripts, catálogos de serviço, manuais de configuração e documentação das integrações estabelecidas.

ii. Listagem completa e atualizada de todas as contas, perfis de acesso, permissões administrativas e credenciais utilizadas nas soluções e ferramentas do contrato.

iii. Relatório consolidado das lições aprendidas e recomendações para continuidade dos serviços, elaborado pela equipe da CONTRATADA em conjunto com a equipe técnica do CONTRATANTE.

iv. Backups de todos os produtos que fazem parte da solução ofertada em formato universal compatível com outras soluções.

v. Entregar relatório e base de dados com todos os registros, tratativas e demais informações relacionados a todos os chamados durante a execução do contrato.

9.6 Encerramento Abrupto do Contrato

I. A operação de um Centro de Operações de Segurança (SOC) é atividade contínua, crítica e ininterrupta, de modo que eventual encerramento abrupto do contrato celebrado com a CONTRATADA deve estar disciplinado em cláusula específica, resguardando a integridade, a disponibilidade e a confidencialidade dos ativos e informações institucionais.

II. Assim, deverá ser estabelecida a obrigatoriedade de que, em caso de rescisão contratual, independentemente de sua motivação, a CONTRATADA entregue à Administração todas as appliances, equipamentos, bases de dados, logs e backups,

em formato universalmente reconhecido e compatível, de forma a não exigir o uso de softwares proprietários ou de terceiros para acesso às informações, assegurando plena autonomia do CONTRATANTE no manuseio e gestão dos dados.

9.6.1 Da Hipótese de Falência ou Encerramento das Atividades da CONTRATADA

I. Na hipótese de falência, dissolução ou encerramento das atividades da CONTRATADA, esta deverá, sem qualquer ônus adicional ao CONTRATANTE:

   a. disponibilizar todas as licenças de software já contratadas e ativas até o término de seus respectivos períodos de vigência;
   b. transferir integralmente os acessos administrativos, incluindo credenciais de administrador, root ou equivalentes, que permitam o gerenciamento pleno das soluções em uso;
   c. repassar integralmente a documentação técnica, relatórios de configuração e de arquitetura, bem como os mecanismos de autenticação vinculados à operação;

II. Tais previsões têm caráter essencial para resguardar o interesse público, a continuidade dos serviços críticos de segurança da informação e a observância dos princípios da eficiência, economicidade e da supremacia do interesse público.

10 ESTRATÉGIA PARA A CONTRATAÇÃO

10.1 Natureza do Objeto

O objeto em questão, qual seja, a pretensa contratação de Serviços de Segurança da Informação, com foco na implantação e operação de um Centro de Operações de Segurança (SOC), caracteriza-se como um **serviço de natureza contínua**, tendo em vista sua especificidade e essencialidade à manutenção da integridade, disponibilidade, confidencialidade e rastreabilidade dos ativos de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado do Espírito Santo.

A continuidade decorre do fato de que a segurança cibernética não admite interrupções, já que ameaças, vulnerabilidades e incidentes ocorrem de forma ininterrupta, exigindo monitoramento constante (24x7x365) para garantir resposta tempestiva e mitigação de riscos. Trata-se de uma atividade que não se exaure em uma única execução, mas que deve ser mantida de forma permanente, com atualizações, correções e acompanhamento

contínuo da infraestrutura tecnológica, de modo a assegurar o funcionamento regular dos serviços judiciais eletrônicos e demais sistemas críticos do Tribunal.

Além disso, a própria natureza do SOC pressupõe a execução cíclica e reiterada de atividades de coleta, análise e correlação de logs, triagem e tratamento de incidentes, emissão de relatórios e apoio às áreas técnicas, compondo um serviço essencialmente rotineiro e permanente. Portanto, justifica-se sua classificação como serviço de natureza contínua, em consonância com a doutrina e jurisprudência administrativa que reconhecem essa característica em serviços cuja paralisação pode comprometer a segurança institucional e a continuidade da prestação jurisdicional.

10.2 Parcelamento do Objeto e Adjudicação

Em função dos aspectos técnicos e requisitos que envolvem a contratação dos serviços e, também considerando o grau de interação entre alguns itens dos serviços técnicos descritos no presente Termo de Referência, a natureza específica, o caráter contínuo, aliada à alta criticidade e complexidade do ambiente de TIC do TJES foi identificado que o agrupamento em 2 lotes distintos é o que melhor atende a presente contratação. O parcelamento proposto é viável pelos seguintes aspectos:

I. simplificação da conduta das atividades de gestão, fiscalização e controle do contrato;
II. minimização de potenciais conflitos internos entre equipes do mesmo fornecedor; e
III. atingimento de níveis de desempenho em razão da continuidade dos serviços executados.

Assim será, portanto, parcelamento do objeto desta contratação:

Lote 01	
Item	**Descrição**
1	Serviço de Administração, Operação, Manutenção e Atendimento às Requisições
2	Serviço de gestão de vulnerabilidades
3	Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança

4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (Security Orchestration, Automation and response – SOAR)
5	Gerenciamento de Proteção Contra Riscos Digitais (Digital Risk Protection – DRP)
6	Gerenciamento de Patches (Patch Management)
Lote 02	
1	Pentest Gray Box
2	Pentest Black Box

10.2.1 Da subcontratação

Não será admitida a subcontratação.

10.2.2 Do Consórcio

Não serão admitidos, como participantes desta licitação, consórcios de empresas, independentemente de sua forma de constituição. A execução dos serviços de um Centro de Operações de Segurança (SOC) demanda elevado nível de integração técnica e operacional, com plena interoperabilidade entre os módulos de monitoramento, resposta a incidentes, gestão de vulnerabilidades, inteligência de ameaças, automação e relatórios de conformidade. A fragmentação decorrente da atuação conjunta de múltiplas empresas poderia comprometer a coesão da solução e gerar dificuldades na responsabilização, no suporte contínuo e na manutenção da qualidade do serviço prestado. Assim, a vedação ao consórcio justifica-se por razões de ordem técnica, em conformidade com os princípios que regem as licitações públicas.

10.3 Modalidade e Tipo de Licitação

Considerando a natureza do objeto e o disposto na Lei nº 14.133/2021, a modalidade de licitação a ser adotada será o Pregão Eletrônico do tipo Menor Preço, por se tratar de serviço comum e contínuo de tecnologia da informação, definido em função de padrões de desempenho e qualidade que podem ser objetivamente especificados neste documento.

10.4. Vigência do Contrato

I. O Contrato terá vigência de 02 (dois) anos, a contar de sua assinatura, podendo ser prorrogado até o limite de 120 (cento e vinte) meses, após a verificação da real necessidade e com vantagens à Administração, nos termos do art. 107 da Lei 14.133/2021

II. A vigência contratual de 02 (dois) anos justifica-se em razão da natureza continuada do serviço de Segurança da Informação, notadamente a operação do Centro de Operações de Segurança (SOC), que exige atuação ininterrupta, processos estáveis e manutenção de equipe especializada ao longo do tempo, sob pena de comprometer a efetividade da proteção cibernética do Tribunal. O prazo proposto garante a consolidação das rotinas operacionais, a amortização dos investimentos necessários à implantação inicial e a previsibilidade contratual.

10.5 Da Visita Técnica

I. A visita técnica constitui requisito importante para a participação no certame, uma vez que a formação de preços e a compreensão integral do objeto dependem de informações específicas sobre o ambiente tecnológico do CONTRATANTE, de natureza sigilosa e não passíveis de divulgação neste documento.

II. Com o intuito de assegurar a igualdade de condições entre os licitantes e garantir a apresentação de propostas adequadas e compatíveis com a realidade do TJES, a visita técnica deverá ser realizada exclusivamente por videoconferência, em data e horário previamente agendados junto ao CONTRATANTE. Nessa ocasião, serão fornecidas as informações essenciais para o correto dimensionamento da solução, condicionadas à assinatura prévia do Anexo E - Declaração de Compromisso de Confidencialidade da Visita Técnica.

III. As empresas licitantes poderão realizar a visita técnica junto ao Tribunal de Justiça do Estado do Espírito Santo (TJES), a qual ocorrerá exclusivamente de forma virtual, por meio da plataforma Google Meet, mediante link disponibilizado pela Administração após o devido agendamento. O agendamento da visita deverá ser solicitado com antecedência mínima de 48 (quarenta e oito) horas da data de realização do certame, e a visita deverá ocorrer no intervalo entre 11h e 18hrs, em até 72 (setenta e duas) horas da abertura do processo licitatório, sempre acompanhada por servidor formalmente designado pelo TJES. Tal procedimento é recomendável para que as empresas obtenham pleno conhecimento das características técnicas do ambiente, garantindo melhor preparação para a execução contratual e adequado balizamento das propostas.

IV. As empresas deverão encaminhar o Anexo E para o email sti@tjes.jus.br contendo as seguintes informações:
   a. Razão social e CNPJ da empresa;
   b. Nome, telefone e e-mail do responsável pelo contato;
   c. Nome completo, documento de identificação e e-mail dos representantes técnicos que participarão da visita;
   d. Cópia digitalizada da declaração de confidencialidade devidamente preenchida e assinada.

V. A realização da visita será acompanhada por representante designado pelo TJES e, ao final, será emitido o Anexo G - Declaração de Visita Técnica, documento que deverá ser anexado à documentação de habilitação como prova da efetiva participação na visita técnica.

VI. A licitante que não participar da visita técnica deverá apresentar o Anexo F - Declaração de Não Comparecimento à Visita Técnica, no qual declarará ciência aos riscos de não conhecer o ambiente do TJES em sua integralidade.

VII. Este procedimento visa assegurar que todas as empresas participantes tenham pleno entendimento das condições operacionais e de segurança do ambiente, permitindo a formulação de propostas realistas e reduzindo riscos de inconsistência técnica ou de subdimensionamento dos serviços a serem prestados.

10.6 Equipe de Apoio à Contratação

Integrante Demandante: Marcianne Ribeiro Antunes Lima
Email: mrlima@tjes.jus.br

Integrante Técnico: Robson Limaverde Valenca da Silva
Email: rlsilva@tjes.jus.br

Integrante Técnico: Luciano Carlos do Nascimento
Email: lucnascimento@tjes.jus.br

Integrante Administrativo: Marcia Marion Ballarini
Email: mmballarini@tjes.jus.br

10.7. Equipe de Gestão do Contrato

Gestor Titular: Robson Limaverde Valenca da Silva
Email: rlsilva@tjes.jus.br

Gestor Substituto: Luciano Carlos do Nascimento
Email: lucnascimento@tjes.jus.br

Fiscal: Witini Kelli Rodrigues Pinheiro
Email: wkpinheiro@tjes.jus.br

11. ANÁLISE DE RISCOS

11.1. Riscos Mapeados

Risco 01	**Risco:**		Demora no trâmite do processo, na forma da norma correlata
	Probabilidade:		Muito Alta
	Impacto:		Médio
	Dano 1:		Atraso na contratação do objeto
	Tratamento:		Acompanhar
	Id	**Ação Preventiva**	**Responsável**
	01	Acompanhar	Setores envolvidos na contratação
	Id	**Ação de Contingência**	**Responsável**
	01	Solicitar o devido cumprimento dos prazos estabelecidos na Norma de Procedimentos nº 01.01	Setores envolvidos na contratação

Risco 02	**Risco:**	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito,o fornecimento dos

		serviços solicitados, e que não sejam justificados e aceitos pelo Contratante	
	Probabilidade:	Baixa	
	Impacto:	Muito Alto	
	Dano 1:	Suspensão do Objeto contratado	
	Tratamento:	Fiscalizar	
	Id	**Ação Preventiva**	**Responsável**
	01	Fiscalizar	Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Notificar a empresa contratada e aplicar as sanções previstas em contrato e na legislação vigente	Gestor
	02	Rescindir o contrato e providenciar a contratação de nova empresa, se for o caso	Gestor

Risco 03	**Risco:**	Atraso na disponibilização da equipe técnica contratada	
	Probabilidade:	Alta	
	Impacto:	Alta	
	Dano 1:	Comprometimento da fase de implantação do SOC e atraso na operacionalização dos serviços	
	Tratamento:	Fiscalizar documentação e cronograma de alocação	
	Id	**Ação Preventiva**	**Responsável**

	01	Exigir comprovação de vínculo e certificações já na fase de implantação.	Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Notificar a empresa contratada e aplicar as sanções previstas em contrato e na legislação vigente	Gestor

Risco 04	**Risco:**	Indisponibilidade ou falha crítica da plataforma SIEM/monitoramento	
	Probabilidade:	Média	
	Impacto:	Alta	
	Dano 1:	Interrupção do monitoramento em tempo real e falha na detecção de incidentes	
	Tratamento:	Exigir alta disponibilidade, redundância e plano de continuidade	
	Id	**Ação Preventiva**	**Responsável**
	01	Testes de carga e redundância antes da produção.	Fiscal Técnico
	Id	**Ação de Contingência**	**Responsável**
	01	Acionar suporte do fabricante e usar backup/infra redundante.	Contratada / Gestor

Risco 05	**Risco:**	Vazamento de informações sigilosas
	Probabilidade:	Baixa
	Impacto:	Muito Alto
	Dano 1:	Comprometimento da confidencialidade e risco

		jurídico/institucional	
	Tratamento:	Exigir cláusulas de confidencialidade e LGPD	
	Id	**Ação Preventiva**	**Responsável**
	01	Assinatura de Termo de Confidencialidade, segregação de funções e logs de auditoria.	Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Abertura de incidente, comunicação formal e apuração de responsabilidades.	Gestor

Risco 06	**Risco:**	Não atingimento dos Níveis Mínimos de Serviço (NMS)	
	Probabilidade:	Média	
	Impacto:	Alto	
	Dano 1:	Redução da efetividade do SOC e aumento da vulnerabilidade	
	Tratamento:	Acompanhamento mensal dos KPIs e aplicação de glosas	
	Id	**Ação Preventiva**	**Responsável**
	01	Monitorar KPIs via Portal de Indicadores.	Fiscal Técnico / Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Aplicar glosas e sanções previstas em contrato.	Gestor

Risco 07	**Risco:**	Atraso na entrega de relatórios técnicos e executivos

	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Dificuldade na tomada de decisão e resposta a incidentes
	Tratamento:		Fiscalização periódica dos prazos
	Id	**Ação Preventiva**	**Responsável**
	01	Estabelecer cronograma rígido de entregas e reuniões quinzenais.	Fiscal Técnico / Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Aplicação de glosa contratual em caso de atraso reincidente.	Gestor

Risco 08	**Risco:**		Dependência excessiva do fornecedor
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Dificuldade de substituição e risco de continuidade
	Tratamento:		Exigir estratégias de independência
	Id	**Ação Preventiva**	**Responsável**
	01	Previsão contratual de transferência de conhecimento e portabilidade.	Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Execução da Estratégia de Independência prevista nos Estudos da Solução.	Gestor / STI

Risco 09	**Risco:**		Rotatividade elevada da equipe contratada
	Probabilidade:		Alta
	Impacto:		Alta
	Dano 1:		Perda de conhecimento acumulado e falhas operacionais
	Tratamento:		Atuar através de indicadores rígidos, de modo a estimular a retenção de profissionais
	Id	**Ação Preventiva**	**Responsável**
	01	Monitorar turnover e exigir substituição rápida.	Fiscal Técnico / Gestor
	Id	**Ação de Contingência**	**Responsável**
	01	Reposição imediata do profissional sem custo adicional.	Contratada

12. APROVAÇÃO E ASSINATURA

Equipe de Planejamento da Contratação, instituída pelo Ato nº 229/2025, publicado em 02 de Outubro de 2025, bem como pela autoridade competente da área de TIC, aprovam o Estudo Técnico Preliminar (ETP) e atestam sua conformidade às disposições da Resolução CNJ nº 468/2022.

Integrante Demandante: Marcianne Ribeiro Antunes Lima
Email: mrlima@tjes.jus.br

gov.br
Documento assinado digitalmente
MARCIANNE RIBEIRO ANTUNES LIMA
Data: 03/10/2025 13:47:45-0300
Verifique em https://validar.iti.gov.br

Integrante Técnico: Robson Limaverde Valenca da Silva
Email: rlsilva@tjes.jus.br

gov.br
Documento assinado digitalmente
ROBSON LIMAVERDE VALENCA DA SILVA
Data: 02/10/2025 19:03:19-0300
Verifique em https://validar.iti.gov.br

Integrante Técnico: Luciano Carlos do Nascimento
Email: lucnascimento@tjes.jus.br

gov.br
Documento assinado digitalmente
LUCIANO CARLOS DO NASCIMENTO
Data: 02/10/2025 19:09:45-0300
Verifique em https://validar.iti.gov.br

Integrante Administrativo: Marcia Marion Ballarini
Email: mmballarini@tjes.jus.br

gov.br
Documento assinado digitalmente
MARCIA MARION BALLARINI
Data: 02/10/2025 18:55:03-0300
Verifique em https://validar.iti.gov.br

Integrante Administrativo: David Sudre de Andrade
Email: dasandradei@tjes.jus.br

gov.br
Documento assinado digitalmente
DAVID SUDRE DE ANDRADE
Data: 02/10/2025 18:41:37-0300
Verifique em https://validar.iti.gov.br

13. CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

Confirmo o recebimento do presente estudo, no qual tomo ciência de forma integral de seu conteúdo.

Para prosseguimento, encaminho à Secretaria Geral para as providências cabíveis.

Secretária (o) de Tecnologia da Informação:

Anexo A – Lista de Potenciais Fornecedores

Razão social do fornecedor 1: **ISH Tecnologia S/A**
Site: www.ish.com.br
E-mail: vitor.costa@ish.com.br (Vitor Teixeira Costa - Diretor Executivo)
E-mail: comercial.df@ish.com.br (Comercial)
Telefone: (27) 3334-8900 / (27) 3334-8905

Razão social do fornecedor 2: **Future Technologies Informática Ltda**
Site: www.future.com.br
E-mail: licitacao@future.com.br
E-mail: contato@future.com.br
E-mail: alexandre.seibert@future.com.br (Comercial)
Telefone: (24) 2232-5850

Razão social do fornecedor 3: **Telebrás**
Site: www.bi40.com.br
E-mail: rodrigo@bi40.com.br (CTO BI4.0 Solutions)
E-mail: luizalberto.passos@bi40.com.br (CBO BI4.0 Solutions)
Telefone: (21) 99986-2937

Razão social do fornecedor 4: **GC Sistemas de Tecnologia e Segurança S.A**
Site: www.vultuscyber.com.br
E-mail: felipe.lopes@gcsec.com.br
Telefone:(11)2972-8999

Razão social do fornecedor 5: **Trust Cybersecurity**
Site: www.trustcybersecurity.com
E-mail: enzorodrigues@trustcybersecurity.com.br
Telefone: (21) 99368-0025 / (11) 3512- 6000

Razão social do fornecedor 6: **Falconi**
Site: www.falconi.com
E-mail: andreparanhos@falconi.com
Telefone: (31) 3289-7200 / (31) 99368-4700

Razão social do fornecedor 7: **THS Tecnologia**
Site: www.ths.inf.br
E-mail: comercial@ths.inf.br
Telefone: (61) 98324-1661 / (61) 3256-4484

Razão social do fornecedor 8: **Kryptus Segurança da Informação S.A**
Site: www.kryptus.com
E-mail: cabral@kryptus.com (Diretor Administrativo)
Telefone: (19) 3112-5000

Razão social do fornecedor 9: **Yssy Soluções S.A**
Site: www.yssy.com.br
E-mail: licitacao@yssy.com.br
E-mail: fernanda.teixeira@yssy.com.br (Comercial)
Telefone: (11) 4134-8000 / (61) 99935-5372 / (61) 99991-3433

Razão social do fornecedor 10: **Central IT Tecnologia da Informação S/A**
Site: www.centralit.com.br
E-mail: comercial@centralit.com.br
Telefone: (61) 3030-4000 / (61) 3030-4020

Razão social do fornecedor 11: **Globalweb Outsourcing do Brasil S/A**
Site: www.globalweb.com.br
E-mail: licita@globalweb.com.br
Telefone: (61) 98402-1626 / (61) 99277-5570

Anexo B – Propostas Comerciais

Anexo C – Contratações Públicas Similares

A identificação das contratações públicas similares foi realizada no item 7.1.3 deste documento.

Anexo D - Modelo de Proposta Comercial

PREGÃO ELETRÔNICO	Número ___/2025

Nome Fantasia:			
Razão Social:			
CNPJ:		Inscrição Estadual:	
Endereço:		Cidade:	
Estado:	CEP:	Telefone:	Fax:

Lote 01				
Item	**Descrição**	**Preço unitário (A)**	**Quantidade (B)**	**Valor Total (A x B)**
1	Serviço de Administração, Operação, Manutenção e Atendimento às Requisições		24	
2	Serviço de gestão de vulnerabilidades		24	
3	Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança		24	
4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (*Security Orchestration, Automation and Response* – SOAR)		24	
5	Gerenciamento de Proteção Contra Riscos Digitais (*Digital Risk Protection* – DRP)		24	
6	Gerenciamento de Patches (Patch Management)		24	
Total Lote 1				
Lote 02				
1	Pentest Gray Box		500	
2	Pentest Black Box		1500	
Total Lote 2				
VALOR TOTAL				

*Proposta Válida por 90 dias, incluídos todos os tributos, custos e despesas diretas ou indiretas.

_____ ____de _____ de 202__.

_____

RAZÃO SOCIAL CNPJ, NOME DO REPRESENTANTE LEGAL E ASSINATURA

Anexo E - DECLARAÇÃO DE COMPROMISSO DE CONFIDENCIALIDADE DA VISITA TÉCNICA

DECLARAÇÃO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

A empresa _____, inscrita no CNPJ sob nº _____, com sede na _____, neste ato representada por seu responsável legal abaixo assinado, vem, por meio da presente, declarar para os devidos fins que:

1. Reconhece que, durante a realização da **Visita Técnica** referente ao processo licitatório nº _____, cujo objeto é a contratação de serviços de _____, poderá ter acesso a informações, dados e documentos de natureza **sigilosa e restrita**, relacionados ao ambiente tecnológico do Tribunal de Justiça do Estado do Espírito Santo.

2. Compromete-se a tratar todas as informações recebidas como **estritamente confidenciais**, abstendo-se de divulgá-las, reproduzi-las, compartilhá-las ou utilizá-las para qualquer fim que não seja a participação no referido certame.

3. Declara ciência de que o descumprimento deste compromisso poderá implicar na aplicação das sanções administrativas, civis e criminais previstas em lei, bem como nas disposições do edital e demais normativos aplicáveis.

4. Compromete-se a adotar todas as medidas cabíveis para garantir que seus representantes técnicos designados para a visita também observem integralmente os termos desta declaração.

5. Declara, ainda, que a presente obrigação de sigilo permanecerá válida **mesmo após a conclusão da visita técnica e do processo licitatório**, independentemente de eventual adjudicação ou contratação.

Por ser a expressão da verdade, firma a presente declaração em duas vias de igual teor e forma.

Local e Data: _____

Razão Social da Empresa: _____
CNPJ: _____

Representante Legal: _____
Cargo: _____
Assinatura: _____

Anexo F - DECLARAÇÃO DE NÃO COMPARECIMENTO À VISITA TÉCNICA

DECLARAÇÃO DE NÃO COMPARECIMENTO À VISITA TÉCNICA

A empresa _____, inscrita no CNPJ sob o nº_____, com sede na _____, neste ato representada por seu(sua) representante legal infra-assinado(a), DECLARA, para os devidos fins, que:

1. Está ciente de que **não realizará a visita técnica** prevista no Termo de Referência e demais documentos que compõem o processo licitatório nº _____, promovido pelo Tribunal de Justiça do Estado do Espírito Santo.

2. Reconhece que, ao abrir mão da visita técnica, **deixa de ter acesso às informações detalhadas e específicas sobre o ambiente tecnológico do TJES**, incluindo, mas não se limitando a: dados de arquitetura, infraestrutura, soluções tecnológicas em uso, processos internos, restrições operacionais e demais elementos relevantes à adequada composição de preços e à execução do objeto licitado.

3. Declara estar plenamente ciente de que **não poderá, em nenhuma hipótese, alegar desconhecimento do ambiente tecnológico do TJES ou das condições técnicas necessárias à execução contratual** como justificativa para eventual descumprimento de obrigações assumidas na proposta ou no contrato.

4. Reconhece, ainda, que, caso venha a ser vencedora do certame, **deverá cumprir integralmente todas as obrigações assumidas em sua proposta comercial e no contrato a ser firmado**, não lhe sendo facultado pleitear aditamentos, reequilíbrios ou revisões em decorrência da ausência de participação na visita técnica.

5. Declara, finalmente, que tem plena ciência das responsabilidades decorrentes de sua opção, assumindo integralmente os riscos relacionados ao não comparecimento, nos termos da legislação aplicável e das regras editalícias.

Por ser a expressão da verdade e para que produza seus jurídicos e legais efeitos, firma a presente declaração.

Local e Data: _____

Razão Social da Empresa: _____
CNPJ: _____

Representante Legal: _____
Cargo: _____
Assinatura: _____

Anexo G - DECLARAÇÃO VISITA TÉCNICA

DECLARAÇÃO DE VISITA TÉCNICA

A empresa _____, inscrita no CNPJ sob o nº _____, com sede na _____, neste ato representada por seu(sua) representante legal infra-assinado(a), DECLARA, para os devidos fins, que:

1. Compareceu à visita técnica prevista neste documento que compõe o processo licitatório nº _____, promovido pelo Tribunal de Justiça do Estado do Espírito Santo.

2. A visita técnica foi realizada no ambiente tecnológico do TJES, especificamente nas áreas vinculadas à implantação e operação do **Centro de Operações de Segurança (SOC)**, oportunidade em que foram prestadas as informações necessárias para o pleno conhecimento das condições de execução do objeto.

3. Declara, ainda, ter ciência integral das condições técnicas e operacionais observadas durante a visita, comprometendo-se a cumpri-las rigorosamente no caso de adjudicação do objeto à sua empresa, não podendo, em nenhuma hipótese, alegar desconhecimento do ambiente tecnológico do TJES como justificativa para eventual inadimplemento contratual.

4. Compromete-se a manter em sigilo todos os dados, informações, documentos e elementos técnicos a que teve acesso durante a visita, utilizando-os exclusivamente para subsidiar sua participação no certame licitatório.

Por ser a expressão da verdade e para que produza seus jurídicos e legais efeitos, firma a presente declaração.

Local e Data: _____

Razão Social da Empresa: _____
CNPJ: _____

Representante Legal: _____
Cargo: _____
Assinatura: _____

ADENDO I - TERMO DE CONFIDENCIALIDADE

TERMO DE CONFIDENCIALIDADE E MANUTENÇÃO DO SIGILO

Pelo presente instrumento, a empresa _____, inscrita no CNPJ sob o nº _____, neste ato representada por seu representante legal infra-assinado, doravante denominada CONTRATADA, declara que, em razão da execução dos serviços contratados no âmbito do Centro de Operações de Segurança - SOC do Tribunal de Justiça do Estado do Espírito Santo (TJES), assume as seguintes obrigações:

I. Manutenção de Sigilo: Compromete-se a resguardar, em caráter confidencial, todas as informações, documentos, registros, dados, configurações, scripts, códigos, credenciais, relatórios, procedimentos, incidentes de segurança e quaisquer outros elementos técnicos e administrativos a que tiver acesso em decorrência da execução do contrato, abstendo-se de divulgar, reproduzir, ceder ou utilizar tais informações para finalidades diversas daquelas estritamente necessárias ao cumprimento do objeto contratual.

II. Proteção das Informações: Assegura que todas as informações obtidas no âmbito do SOC, independentemente de sua classificação, serão tratadas como confidenciais, adotando as medidas técnicas e administrativas necessárias à sua proteção, em conformidade com as normas de segurança da informação vigentes no TJES, com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), e com demais legislações aplicáveis.

III. Responsabilidade dos Colaboradores: Declara que todos os colaboradores, empregados e prepostos diretamente envolvidos na execução do contrato assinarão este Termo, comprometendo-se pessoalmente ao cumprimento das obrigações aqui estabelecidas.

IV. Duração da Obrigação: O dever de sigilo ora assumido permanecerá vigente durante toda a execução contratual e subsistirá mesmo após o término do contrato, por prazo indeterminado, até que as informações eventualmente venham a se tornar públicas por ato oficial da Administração.

Penalidades - O descumprimento de qualquer obrigação estabelecida neste Termo sujeitará a CONTRATADA e seus representantes às penalidades administrativas, civis e criminais cabíveis, conforme legislação vigente, sem prejuízo das sanções previstas no contrato e na Lei Federal nº 14.133/2021.

Representante Legal da CONTRATADA

Cargo: _____

Assinatura: _____