ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Termo de Referência – TR

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

1. OBJETO DA CONTRATAÇÃO

1.1. Esta contratação tem como objeto a contratação de serviços necessários para a implantação, funcionamento e manutenção de um *Security Operations Center* (SOC) pelo prazo mínimo de 36 meses. O SOC será composto por: Serviço de gestão de incidentes de segurança (Blue Team); Serviço de gestão testes de invasão (Red Team) e Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação, incluindo demais especificações e características consignados neste Termo de Referência.

1.2. Quantitativo

ID	Demanda Prevista	Quantitativo a ser contratado
1	Serviço de gestão de incidentes de segurança (Blue Team)	1 Unidade/Serviço
2	Serviço de gestão testes de invasão (Red Team)	1 Unidade/Serviço
3	Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação	1 Unidade/Serviço
4	Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.	10 Unidade/Serviço
5	Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.	10 Unidade/Serviço
6	Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.	10 Unidade/Serviço

1.2.1. As demandas previstas com IDs 4, 5 e 6 da Tabela mostrada acima poderão ser contratadas opcionalmente, sob demanda de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual.

1.2.2. Não haverá obrigação do TJCE, na utilização do quantitativo parcial ou total dos pacotes de extra que são apresentadas nas demandas previstas com IDs 4, 5 e 6 apresentadas na Tabela anterior.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Motivação

2.1.1. Realizar coleta, análise e gerenciamento de informações de segurança em tempo real. Monitorar a rede do Tribunal de Justiça do Estado do Ceará (TJCE) e detectar possíveis ameaças e vulnerabilidades de maneira centralizada, garantindo a segurança da informação e a integridade dos sistemas. Além disso, fornecer informações e recomendações para a tomada de decisões estratégicas relacionadas à segurança da informação.

2.1.2. Identificar e responder a ameaças em tempo real. Coletar, analisar e correlacionar informações de segurança de vários dispositivos e sistemas do TJCE, permitindo que a equipe de segurança possa responder prontamente a possíveis ataques ou vulnerabilidades.

2.1.3. Lidar com incidentes de segurança cibernética. Ter expertise para identificar, isolar e solucionar possíveis problemas de segurança, minimizando o impacto e os danos causados por um possível ataque. Sendo essencial para garantir a continuidade dos serviços do TJCE, mantendo a integridade da informação.

2.1.4. Automatizar processos e fluxos de trabalho relacionados à segurança da informação. Simplificar e agilizar a resposta a incidentes de segurança, permitindo que a equipe de segurança possa lidar com mais eficiência e rapidez com possíveis ameaças ou vulnerabilidades.

2.1.5. Capacidade de testar a segurança do sistema simulando um ataque real. Defender a rede e os sistemas, respondendo aos ataques simulados e implementando medidas de segurança para evitar possíveis violações de segurança.

2.2. Resultados a serem alcançados com a contratação

2.2.1. Vinculados às necessidades de negócios.

2.2.1.1. Contar com sistemas especializados de tratamento de dados de segurança da informação para melhorar a confidencialidade, integridade e disponibilidade

dos dados que trafegam na rede do TJCE.

2.2.1.1.1. Dados processuais: informações relacionadas a processos judiciais.

2.2.1.1.2. Dados pessoais: informações pessoais dos envolvidos nos processos, como nomes, endereços, números de documentos, registros criminais, dados biométricos, entre outros.

2.2.1.1.3. Documentos digitais: documentos eletrônicos utilizados no ambiente de trabalho do Tribunal.

2.2.1.1.4. Comunicações internas: e-mails, mensagens instantâneas, chamadas de voz e videoconferências realizadas pelos funcionários do Tribunal.

2.2.1.1.5. Dados de segurança: registros de acesso, logs de eventos, informações de autenticação, registros de monitoramento e outras informações relacionadas à segurança da rede e dos sistemas do Tribunal.

2.2.1.1.6. Dados de sistemas administrativos: informações relacionadas à gestão interna do Tribunal, como recursos humanos, finanças, compras, contratos, licitações, entre outros.

2.2.1.2. Contar com uma equipe especializada e dedicada exclusivamente a atividades de segurança da informação e resposta a incidentes, também conhecida como Centro Operacional de Segurança (Security Operations Center – SOC), para elevar o nível de proteção dos serviços utilizados pelos usuários da rede do TJCE e atender as seguintes necessidades de negócio:

2.2.1.2.1. Proteção da informação: Um Tribunal de Justiça lida com uma grande quantidade de informações confidenciais, sensíveis e sigilosas. A equipe de resposta a incidentes é fundamental para proteger essas informações contra ameaças cibernéticas, violações de segurança e acesso não autorizado.

2.2.1.2.2. Preservação da integridade dos sistemas: Os sistemas de um Tribunal de Justiça são essenciais para o funcionamento adequado das atividades judiciais. A equipe de resposta a incidentes contribui a mentar a integridade dos sistemas, prevenindo e mitigando incidentes que possam comprometer a disponibilidade e o desempenho dos sistemas.

2.2.1.2.3. Continuidade dos serviços: A equipe de resposta a incidentes

desempenha um papel fundamental na garantia da continuidade dos serviços do Tribunal de Justiça. Eles estão preparados para lidar com incidentes de segurança, minimizando o impacto e assegurando que os serviços sejam restabelecidos o mais rápido possível em caso de interrupções ou ataques cibernéticos.

2.2.1.3. Contar com serviços especializados em soluções de tratamento e resposta a incidentes de redes, com o objetivo de atender os seguintes artigos da RESOLUÇÃO No 396, DE 7 DE JUNHO DE 2021 do CNJ:

2.2.1.3.1. Art. 6º, Inciso IV: permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

2.2.1.3.2. Art. 9º, Inciso II: elevar o nível de segurança das infraestruturas críticas.

2.2.1.3.3. Art. 11º, Inciso I: estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão.

2.2.1.3.4. Art. 11º, Inciso II: instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

2.2.1.3.5. Art. 11º, Inciso III: elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa.

2.2.1.3.6. Art. 11º, Inciso XI: realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo.

2.2.1.3.7. Art. 12º, Inciso V: possibilitar a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança cibernética.

2.2.1.4. Contar com serviços especializados em soluções de testes de segurança de invasão de redes, com o objetivo de atender os seguintes artigos da RESOLUÇÃO No 396, DE 7 DE JUNHO DE 2021 do CNJ:

2.2.1.4.1. Art. 6º, Inciso II: aumentar a resiliência às ameaças cibernéticas.

2.2.1.4.2. Art. 11º, Inciso X: realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos.

2.2.1.4.3. Art. 12º, Inciso IV: estabelecer rotinas de verificações de conformidade em segurança cibernética.

2.2.1.5. Maior visibilidade, fortalecimento, inteligência e a maturidade em de segurança da informação.

2.2.1.6. Melhoria da conformidade regulatória. Mantendo o TJCE em conformidade com as leis e regulamentações de segurança, minimizando o risco de penalidades ou multas.

2.2.1.7. Treinamento especializado para repasse de conhecimento do serviço técnico especializado.

2.2.2. Vinculados às necessidades tecnológicas.

2.2.2.1. Contar com serviços especializados em soluções tecnológicas de monitoramento e correlação de dados de redes de computadores com o objetivo de atender os seguintes artigos da RESOLUÇÃO No 396, DE 7 DE JUNHO DE 2021 do CNJ:

2.2.2.1.1. Art. 11º, Inciso IV: utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

2.2.2.1.2. Art. 11º, Inciso VI: providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes.

2.2.2.2. Contar com serviços especializados em solução tecnológica SIEM para manutenção, monitoramento e análise de logs de auditoria no TJCE, conforme os seguintes tópicos do Inciso “8 Checklist para utilização dos Controles Mínimos Recomendados” do Manual de Referência – Proteção de Infraestruturas Críticas de TIC (ANEXO IV DA PORTARIA No 162, DE 10 DE JUNHO DE 2021):

2.2.2.2.1. Inciso 6.5: Garantir que os logs apropriados sejam agregados em um sistema central de gerenciamento de logs para análises e revisões.

2.2.2.2.2. Inciso 6.6: Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs.

2.2.2.2.3. Inciso 6.7: Em uma base regular, revisar os logs para identificar

anomalias ou eventos anormais.

2.2.2.2.4. Inciso 6.8: Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes.

2.2.2.3. Solução tecnológica SIEM para gerenciar os eventos e incidentes nos ativos de rede do TJCE de maneira normalizada, padronizada e sincronizada na modalidade 24 horas do dia, nos 7 dias da semana, no período de vigência contratual.

2.2.2.4. Solução tecnológica SIEM como ferramenta homogeneizada que evite a sobrecarga da análise desses eventos e incidentes em cada um dos ativos heterogêneos de rede (diversos fabricantes, sistemas operacionais ou firmware), os quais são apresentados na Tabela 4. do documento TRF ANEXO I.

2.2.2.5. Atender às exigências regulatórias de governança e boas práticas, estabelecidas pelos Frameworks de segurança da informação (NIST, SANS, ISO 27000, OWASP, MITRE ATT&CK, etc), os quais estão relacionados a detecção e resposta de incidentes (Blue Team), testes de invasão (Red Team) e monitoramento e correlação de eventos com a ferramenta SIEM.

2.2.2.6. Treinamento especializado para repasse de conhecimento do serviço técnico especializado.

2.2.2.7. Automação dos processos de tarefas repetitivas e rotineiras, permitindo que a equipe de segurança se concentre em atividades mais críticas e aumentando a confiança dos usuários nos serviços prestados pelo TJCE.

2.2.2.8. Serviço técnico especializado ininterrupto (24h x 7d x 365d) de monitoramento, controle e visibilidade de ataques cibernéticos no tráfego de rede do TJCE (aplicações em nuvem ou on-premise, servidores bare-metal ou virtualizados, equipamentos de roteamento/switch de redes e equipamentos ou aplicações de segurança de redes), com processos de triagem e respostas/tratamento a incidentes de segurança.

2.2.2.9. Serviço técnico especializado de testes de invasão por meio da identificação, mapeamento e documentação de possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica, com o objetivo de avaliar a eficácia das medidas de segurança existentes, assim como analisar, remediar, conter e documentar os eventos de segurança da informação que podem ser transformados em incidentes de segurança para implementação de medidas

de proteção.

2.3. Referência aos Estudos Técnicos Preliminares

2.3.1. Os documentos que resultaram dos Estudos Técnicos Preliminares desta contratação seguem acostados nos respectivos autos do Processo Administrativo que trata da demanda exposta neste Termo de Referência.

2.4. Alinhamento estratégico

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da SETIN
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

ID	Iniciativa Elencada no PDTIC 2023
N23003	Aquisição e Implantação de SOC (“Security Operations Center” - Centro de Operações de Segurança).

2.5. Critérios Ambientais

2.5.1. A contratada deverá providenciar o recolhimento e o adequado descarte de produto(s) e material(is) inservível(is) originário(s) da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA n° 01, de 18/03/2010, da Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA n° 416, de 30/09/2009, e legislação correlata.

2.5.2. A contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 11º da Lei n.º 14.133/21.

2.5.3. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

2.5.4. Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

2.5.5. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva ROHS (*restriction of certain hazardous substances*), tais como mercúrio (hg), chumbo (pb), cromo hexavalente (cr(vi)), cádmio (cd), bifenil-polibromados (pbbs), éteres difenil-polibromados (pbdes).

2.5.6. Os serviços prestados e os bens fornecidos pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela Contratante.

2.6. Análise das soluções possíveis

2.6.1. Soluções viáveis.

2.6.1.1. Serviços Gerenciados de Segurança da Informação.

2.6.1.1.1. Também conhecido como Managed Security Services (MSS), consiste em um conjunto de serviços terceirizados de segurança da informação e gerenciamento de risco fornecidos por um provedor especializado, incluindo o uso de software e hardware da contratada como serviço. Esses serviços abrangem monitoramento contínuo, detecção e resposta a incidentes de segurança, gerenciamento de vulnerabilidades, análise de logs e eventos de segurança, além de consultoria e suporte técnico. O objetivo principal do MSS é ajudar as organizações a fortalecerem sua postura de segurança, reduzir riscos e proteger seus ativos críticos, permitindo que elas se concentrem em suas principais atividades comerciais.

2.6.1.1.2. Nesta solução, cabe à empresa contratada gerenciar a quantidade de profissionais necessários para a realização das atividades. É de responsabilidade da empresa contratada adequar a composição da equipe de acordo com os parâmetros estabelecidos para os níveis mínimos de serviço.

2.6.1.1.3. A proposta da solução é reduzir os riscos relacionados a modificações acidentais ou intencionais, acessos não autorizados ou ataques maliciosos que possam comprometer a segurança de ativos críticos.

2.6.2. Soluções inviáveis: Outras soluções consideradas inviáveis estão listadas no item 5 do documento Estudos Técnicos Preliminares desta contratação. Esse documento se encontra nos respectivos autos do Processo Administrativo que trata da demanda

exposta neste Termo de Referência.

2.6.3. Pesquisa de preços de mercado das soluções viáveis.

2.6.3.1. A pesquisa de mercado está presente no documento acostado aos autos do processo.

2.7. Identificação da Solução Escolhida

2.7.1. Solução 1: - Serviços Gerenciados de Segurança da Informação.

2.8. Justificativa da Solução Escolhida

2.8.1. No contexto da Solução 1, os pagamentos estão relacionados ao cumprimento dos Níveis Mínimos de Serviço (NMS) estabelecidos. Caso ocorra o descumprimento de algum NMS, serão aplicados redutores no faturamento por meio de glosas. A solução 1, que utiliza Níveis Mínimos de Serviço (NMS) e possui uma remuneração mensal fixa com base nos resultados alcançados e verificados, é uma opção tecnicamente viável. No entanto, é necessário fornecer informações sobre o ambiente tecnológico, incluindo hardware, software, histórico de consumo e todos os serviços relacionados à gestão da segurança da informação. Essas informações estão presentes no item 4 deste TRF.

2.8.2. É importante ressaltar que a solução 1 está em conformidade com as recomendações legais, estabelecendo padrões de qualidade e indicadores facilmente mensuráveis, resultando em melhorias na qualidade e produtividade dos serviços. Além disso, ela simplifica a gestão e fiscalização contratual, facilitando as ações orçamentárias. Dessa forma, a solução 1, que se baseia nos Níveis Mínimos de Serviço (NMS), é considerada uma opção viável tanto do ponto de vista técnico quanto administrativo, atendendo integralmente às necessidades e requisitos estabelecidos no item 4.

2.8.3. O objetivo do TJCE ao escolher essa solução é obter prestação de serviços especializados que lidem com as tarefas e rotinas de segurança de forma mais eficiente e/ou com menor custo do que o uso da própria força de trabalho, servidores ou serviços acessórios que não possuem a mesma capacidade técnica necessária para garantir a integridade dos recursos e ativos tecnológicos, além de aprimorar as boas práticas de segurança.

2.8.4. Benefícios do Serviço de gestão de incidentes de segurança (Blue Team).

2.8.4.1. Atualmente o TJCE não conta com serviços profissionais especializados em detecção e resposta a incidentes. Essa lacuna de profissionais faz com que o TJCE não conte com capacidade de resposta rápida e precisa na detecção e resposta a incidentes de segurança. Por exemplo, problemas de

disponibilidade, como lentidão nos sistemas, poderiam ser resolvidos com perícia técnica de análise e configuração de sistemas. Sendo assim, há uma necessidade prioritária de contar com uma equipe especializada em detecção e resposta a todo tipo de incidentes de segurança da informação. A equipe necessária é conhecida na literatura de segurança da informação como Blue Team.

2.8.4.2. O Blue Team contará com profissionais altamente qualificados e trará ao TJCE maturidade de detecção e resposta a incidentes de segurança da informação. As principais vantagens de contar com o Blue Team no TJCE são:

2.8.4.2.1. Proteção contra ciberataques: o Blue Team possui conhecimento e habilidades para identificar, prevenir e mitigar ataques cibernéticos. Eles estão constantemente monitorando e analisando a infraestrutura de TI para detectar qualquer atividade maliciosa e responder de forma rápida e eficiente.

2.8.4.2.2. Resposta rápida a incidentes: com um Blue Team atuante, o TJCE pode responder de maneira mais ágil a incidentes de segurança cibernética. A equipe possui protocolos e procedimentos estabelecidos para lidar com violações de segurança, minimizando o impacto e reduzindo o tempo de inatividade dos sistemas.

2.8.4.2.3. Monitoramento contínuo: o Blue Team realiza monitoramento contínuo dos sistemas e redes de TI do órgão governamental. Isso permite identificar comportamentos suspeitos, padrões incomuns e vulnerabilidades potenciais antes que sejam exploradas por atacantes.

2.8.4.2.4. Análise de riscos: A equipe Blue Team avalia regularmente os riscos de segurança cibernética enfrentados pelo órgão governamental. Isso inclui a identificação e análise de vulnerabilidades, a realização de testes de penetração e a implementação de medidas de segurança adequadas para reduzir os riscos.

2.8.4.2.5. Conformidade regulatória: com a equipe Blue Team, o TJCE poderá garantir a conformidade com regulamentações de segurança cibernética aplicáveis. Isso é especialmente relevante para lidar com informações sensíveis e confidenciais dos

cidadãos.

2.8.4.2.6. Conscientização e treinamento: o Blue Team desempenhará um papel fundamental na conscientização e treinamento em segurança cibernética para os funcionários do TJCE. Isso ajuda a promover uma cultura de segurança, educando os usuários sobre boas práticas, políticas de segurança e a importância de manter a segurança das informações.

2.8.4.2.7. Inteligência de ameaças: a equipe Blue Team está constantemente atualizada sobre as últimas ameaças e tendências em segurança cibernética. Isso permitirá ao TJCE estar ciente das ameaças emergentes e adotar medidas proativas para se proteger contra ataques.

2.8.4.2.8. Parceria com outras equipes: o Blue Team trabalhará em colaboração com outras equipes de TI e de resposta a incidentes no TJCE. Essa parceria fortalece a segurança geral, promovendo a troca de informações e o compartilhamento de melhores práticas entre as equipes.

2.8.5. Benefícios do Serviço de gestão de testes de invasão (Red Team), por 36 meses.

2.8.5.1. Atualmente o TJCE não conta com serviços profissionais especializados em testes de invasão e detecção de falhas. Essa lacuna de profissionais faz com que o TJCE não conte com um setor responsável por simular ataques e explorar vulnerabilidades em sistemas, aplicativos e infraestrutura, identificando falhas e pontos fracos antes que sejam explorados por adversários reais. Por exemplo, problemas de disponibilidade, como lentidão nos sistemas, poderiam ter sido detectados e previstos como falhas existentes para terem sua correção aplicada antes que apareça o incidente. Sendo assim, há uma necessidade prioritária de contar com uma equipe especializada em testes de invasão e prevenção de vulnerabilidades para todo tipo de incidentes de segurança da informação. A equipe necessária é conhecida na literatura de segurança da informação como Red Team.

2.8.5.2. O Red Team contará com profissionais altamente qualificados e trará ao TJCE maturidade de detecção e prevenção de incidentes de segurança da informação. As principais vantagens de contar com o Red Team no TJCE são:

2.8.5.2.1. Avaliação de segurança abrangente: o Red Team realizará testes de penetração e simulações de ataques realistas e controlados para

identificar vulnerabilidades e pontos fracos nos sistemas do TJCE. Isso permite uma avaliação abrangente da postura de segurança, indo além das análises teóricas e identificando áreas que precisam de melhorias.

2.8.5.2.2. Identificação de vulnerabilidades ocultas: o Red Team utilizará técnicas avançadas para identificar vulnerabilidades ocultas que podem não ser detectadas pelos sistemas de segurança convencionais ou mesmo pelo pessoal interno do TJCE. Isso ajuda a revelar falhas de segurança desconhecidas e a corrigi-las antes que sejam exploradas por atacantes reais.

2.8.5.2.3. Teste de resiliência: o Red Team realizará testes práticos para avaliar a resiliência do TJCE em cenários de ataque realistas. Isso permite testar a eficácia dos processos de resposta a incidentes, a capacidade de recuperação e a coordenação entre as equipes de segurança.

2.8.5.2.4. Melhoria da conscientização em segurança: As atividades do Red Team ajudarão a aumentar a conscientização sobre segurança cibernética entre os funcionários do TJCE. Os testes de penetração e os incidentes simulados fornecem exemplos concretos dos riscos e das consequências de violações de segurança, incentivando a adoção de práticas de segurança mais robustas e a conformidade com políticas e diretrizes.

2.8.5.2.5. Tomada de decisão embasada: as avaliações do Red Team fornecem informações valiosas para a tomada de decisões estratégicas em relação aos investimentos em segurança cibernética. Os resultados dos testes ajudam a priorizar as áreas de melhoria e a alocar recursos de forma mais eficiente, garantindo que os esforços de segurança estejam alinhados com as ameaças reais.

2.8.5.2.6. Preparação para incidentes de segurança: ao simular ataques e explorar vulnerabilidades, o Red Team ajudará a preparar o TJCE para lidar com incidentes de segurança cibernética reais. Isso inclui a identificação de gaps nos planos de resposta a incidentes, o treinamento das equipes de resposta e a melhoria dos processos de comunicação e coordenação durante uma crise de segurança.

2.8.5.2.7. Aumento da confiança pública: a presença de um Red Team no TJCE demonstrará um compromisso com a segurança cibernética e a proteção das informações confidenciais dos usuários. Isso ajuda a aumentar a confiança do público no TJCEl e em suas práticas de segurança.

2.8.5.2.8. Benefícios dos Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação por 36 meses.

2.8.5.3. Atualmente, o TJCE não conta com uma solução que permita coletar, analisar e correlacionar eventos de segurança de várias fontes em tempo real. Com a aquisição da ferramenta SIEM, assim como, no mínimo, um profissional para sua gestão, o TJCE contará com as seguintes vantagens:

2.8.5.3.1. Detecção de ameaças avançadas: uma ferramenta SIEM é capaz de coletar e correlacionar informações de logs e eventos de segurança de diversas fontes, permitindo a detecção de ameaças avançadas que poderiam passar despercebidas de forma isolada. Com a análise em tempo quase real e histórica dos dados, é possível identificar padrões e comportamentos anormais, indicando possíveis ataques ou violações de segurança.

2.8.5.3.2. Resposta rápida a incidentes: o profissional especializado em SIEM tem a capacidade de interpretar os alertas e informações gerados pela ferramenta de forma rápida e eficiente. Isso permite uma resposta ágil a incidentes de segurança, minimizando o tempo de detecção e reduzindo o impacto causado por ataques cibernéticos. O profissional pode tomar as medidas necessárias para conter a ameaça e iniciar as investigações pertinentes.

2.8.5.3.3. Monitoramento abrangente: uma ferramenta SIEM permitirá o monitoramento abrangente de toda a infraestrutura de TI do TJCE, incluindo redes, servidores, aplicativos e dispositivos. Isso possibilita a identificação de atividades suspeitas ou não autorizadas em tempo real, auxiliando na proteção dos sistemas e informações sensíveis.

2.8.5.3.4. Análise forense e investigação: o SIEM armazenará os registros de eventos de segurança por até 6 meses (conforme PORTARIA No 162, DE 10 DE JUNHO DE 2021 do CNJ), permitindo uma análise forense detalhada em caso de incidentes. O profissional

especializado em SIEM é capaz de investigar e rastrear as origens das ameaças, analisando logs e correlacionando dados para obter uma visão mais completa do incidente. Isso é fundamental para entender a extensão do ataque, identificar pontos de entrada e melhorar as medidas de segurança.

2.8.5.3.5. Conformidade regulatória: o uso de uma ferramenta SIEM e a presença de um profissional especializado auxiliam no cumprimento de regulamentações e normas de segurança cibernética impostas ao TJCE. A capacidade de coletar, analisar e relatar eventos de segurança em conformidade com os requisitos regulatórios é facilitada pela utilização de um SIEM adequado e pela expertise do profissional.

2.8.5.3.6. Alertas e notificações em tempo real: a ferramenta SIEM emite alertas e notificações em tempo quase real para indicar eventos de segurança relevantes. O profissional pode configurar e personalizar esses alertas de acordo com as necessidades do órgão governamental, garantindo que incidentes sejam prontamente identificados e tratados.

2.8.5.3.7. Melhoria da visibilidade e tomada de decisões: a utilização de uma ferramenta SIEM aliada ao conhecimento do profissional permite uma visibilidade abrangente dos riscos de segurança cibernéticas enfrentados pelo órgão governamental. Isso facilita a tomada de decisões informadas em relação a investimentos em segurança, implementação de medidas preventivas e melhoria contínua dos controles de segurança.

2.8.6. Viabilidade financeira:

2.8.6.1. A segurança cibernética é uma área de extrema importância para o TJCE, uma vez que lida com informações confidenciais e sensíveis, além de desempenhar um papel crítico na proteção e bem-estar dos cidadãos. Nesse contexto, é fundamental contar com Blue/Red Team e um serviço gerenciado de monitoramento e correlação de eventos de segurança da informação, por meio de uma ferramenta SIEM.

2.8.6.2. Considerando que o orçamento anual de aproximadamente 2,6 milhões de reais disponíveis para este edital foi aprovado no Plano Anual de Contratações de 2023, e que há histórico de órgãos e empresas que conseguem atender

técnica e financeiramente as três demandas, a implementação do projeto de Blue/Red Team e Serviço gerenciado de SIEM é altamente justificável pelos seguintes motivos:

2.8.6.2.1. Maximização dos recursos humanos e tecnológicos: a contratação de serviços via NMS efetuado por equipes de especialistas de Blue Team e Red Team, juntamente com o serviço gerenciado de SIEM, permite uma utilização eficiente dos recursos disponíveis. A externalização do serviço de SIEM garante acesso à expertise e tecnologia avançada de uma empresa especializada, sem a necessidade de investimentos significativos em infraestrutura e treinamento interno.

2.8.6.2.2. Conformidade com as regulamentações: a implementação do projeto atende às exigências regulatórias em relação à segurança cibernética no ambiente governamental. Ao contar com um Blue/Red Team dedicado e um serviço gerenciado de SIEM, o TJCE demonstrará seu compromisso com a proteção das informações confidenciais e o cumprimento das normas de segurança cibernética.

2.8.6.2.3. Mitigação de riscos e prejuízos financeiros: a detecção precoce e a resposta eficiente a incidentes de segurança ajudam a minimizar os riscos e prejuízos financeiros decorrentes de violações de dados e interrupções nos serviços do TJCE. A implementação do projeto contribui para a mitigação desses riscos, protegendo a reputação do TJCE e evitando possíveis perdas financeiras decorrentes de incidentes de segurança.

2.9. Justificativa para o não parcelamento do objeto

2.9.1. Os serviços gerenciados de segurança da informação serão compostos pelos serviços mostrados na seguinte Tabela.

LOTE	SERVIÇO	DESCRIÇÃO DO SERVIÇO	QTD
1	**1**	**Serviço de gestão de incidentes de segurança (Blue Team), por 36 meses.**	**1**
	2	**Serviço de gestão testes de invasão (Red Team), por 36 meses.**	**1**
	3	**Serviços gerenciados de monitoramento e correlação**	**1**

		de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS por 36 meses.	
	4	**Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.**	**10**
	5	**Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.**	**10**
	6	**Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.**	**10**

2.9.2. Os serviços devem ser prestados por equipes dotadas de competências técnicas especializadas, e que devem buscar, de forma conjunta e compartilhada, o alcance dos seguintes objetivos:

2.9.2.1. Solucionar, de forma precisa e conforme prazos estabelecidos, as demandas pertencentes ao escopo de atividades delegadas por esta contratação.

2.9.2.2. Permitir que grupos especializados concentrem sua atuação em atividades que proporcionem maior fluxo de valor à instituição.

2.9.3. A execução do serviço por equipes distintas dispersaria a responsabilidade pelo alcance dos objetivos. Essa dispersão acarretaria diluição do comprometimento com os processos de trabalho e traria riscos de sobreposição de atividades. Além disso, a comunicação direta e contínua entre as equipes é essencial para a qualidade da prestação do serviço, haja vista que os objetivos são comuns e a fronteira de atuação é muito tênue, dada a forte interconexão das atividades no que concerne aos aspectos técnicos (caráter generalista) e metodológicos (registro, investigação e diagnóstico).

2.9.4. A contratação deve ser realizada via lote único pela existência de interdependência de trabalho entre os profissionais do SOC (Blue Team, Red Team e de Serviços gerenciados de monitoramento e correlação de eventos), em conjunto com o uso da ferramenta SIEM, e pelas seguintes características de funcionamento de serviço unificado em somente uma empresa contratada:

2.9.4.1. Coesão e integração: Ao ter os três serviços fornecidos por uma única empresa, a comunicação e colaboração entre as equipes podem ser mais eficientes e coesas. Permitindo uma melhor coordenação de esforços e uma abordagem mais unificada na resposta a incidentes de segurança.

2.9.4.2. Conhecimento aprofundado do ambiente: A empresa que fornece todos os serviços terá um conhecimento mais aprofundado do ambiente de segurança da organização, incluindo a infraestrutura de rede, sistemas e vulnerabilidades.

Resultando em uma melhor compreensão dos riscos específicos e à identificação mais precisa de ameaças.

2.9.4.3. Integração das soluções: Uma empresa que oferece todos os serviços pode garantir que as ferramentas de segurança utilizadas em cada etapa (Blue Team, Red Team e SIEM) estejam bem integradas e trabalhem em conjunto de maneira mais eficiente. Resultando em melhoria na detecção, resposta e correlação de eventos de segurança.

2.9.4.4. Melhoria contínua: A empresa que fornece todos os serviços terá uma visão mais holística da segurança da organização e, assim, oferecer soluções mais abrangentes e personalizadas. Resultando em melhoria contínua na segurança cibernética e a uma abordagem proativa para mitigar riscos.

2.9.4.5. Responsabilidade única: Ao contratar uma única empresa, a organização tem uma responsabilidade única para relatar, gerenciar e solucionar qualquer problema ou incidente relacionado aos serviços contratados.

2.9.5. Ante o exposto, a adjudicação do serviço a uma única empresa mitigará os riscos em comento e proporcionará melhor gestão e maior qualidade na execução dos serviços contratados. Sendo assim, não há parcelamento do objeto.

2.10. Natureza do Objeto

2.10.1. A natureza do objeto a ser licitado é comum de acordo com o inciso XIII do art. 6°, da Lei 14.133, de 1º de abril de 2021, que considera bens e serviços comuns, com fornecimento de equipamento, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais.

2.11. Natureza do Serviço

2.11.1. Os serviços especializados a serem contratados (item 1.2) devem ser contínuos pelo período contratado. A continuidade do SOC é crucial devido à natureza em constante evolução das ameaças cibernéticas e à necessidade contínua de manter a postura de segurança da organização. A complexidade e sofisticação das ameaças cibernéticas exigem uma abordagem constante e vigilante para identificar, prevenir e responder a incidentes de segurança. O serviço de gestão de incidentes de segurança (Blue Team) precisa ser mantido ao longo do tempo para garantir uma detecção precoce e uma resposta eficaz a ameaças em constante mutação. Da mesma forma, os serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta SIEM são essenciais para monitorar constantemente os ambientes de TI em busca de atividades suspeitas ou anomalias. Portanto, a continuidade desses serviços ao longo do período de contratação é justificada pela necessidade de adaptação constante às ameaças

cibernéticas em constante evolução e pela garantia de uma postura de segurança sólida e sustentável ao longo do tempo.

2.11.2. O período de 36 meses é adequado para a implementação e consolidação dos serviços contratados considerando que o prazo de implantação inicial é de 3 meses e a melhoria contínua de procedimentos de resposta a incidentes e de configuração do SIEM pode levar entre 18 e 24 meses. Sendo assim, o período de 36 meses mínimos de contratação tem coimo objetivo garantir uma maior eficiência e eficácia na prestação dos serviços. Um contrato com duração de no mínimo 36 meses, proporcionará maior estabilidade e previsibilidade tanto para a CONTRATANTE quanto para a CONTRATADA, permitindo um planejamento mais adequado e uma gestão mais eficiente dos recursos. Este período é uma prática adotada nas pesquisas realizadas de contrato do tipo em outros órgãos públicos (ver item 2.6.2).

2.11.3. Os serviços poderão ser renovados até o limite máximo de tempo conforme a Nova Lei de Licitações e Contratos - Lei nº 14.133/2021 (10 anos).

2.12. Justificativa para Aplicação do Direito de Preferência (Lei complementar nº 123/06 e Lei nº 8.248/91)

2.12.1. Nos termos do art. 48, III da Lei Complementar n. 123, de 2006 (atualizada pela LC n. 147/2014), a Administração deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte. Por essa razão, parcela de até 25% (vinte e cinco por cento) dos quantitativos divisíveis deverão ser destinados exclusivamente a ME/EPP/COOP beneficiadas pela LC n. 123/2006. Essas “cotas reservadas” deverão ser definidas em função de cada item separadamente ou, nas licitações por preço global, em função do valor estimado para o grupo ou o lote da licitação que deve ser considerado como um único item (art. 9º, inciso I do Decreto n. 8.538, de 2015).

2.12.2. In casu, a licitação que se pretende deverá ocorrer pelo menor preço global. Contudo, todos os itens se tratam de serviços interdependentes em sua totalidade, sendo 6 (seis) itens, não havendo, desta forma, como fazê-lo divisível sem desnaturá-lo.

2.12.3. Mesmo para os serviços que não constituem parte do lote, a divisão não se torna possível seja pelo fato de trata-se de item unitário, qual seja a contratação de serviço técnico profissional pelo período mínimo de 36 (trinta e seis) meses, seja pela indivisibilidade técnica do serviço de Centro Operacional de Segurança (SOC).

2.12.4. Para tanto, o Art 39 da Lei Nº 15.306 , de 08 de janeiro de 2013 do Estado do Ceará excepciona algumas hipóteses, quais sejam: *II - não houver um mínimo de 3 (três)*

fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados no Estado e capazes de cumprir as exigências estabelecidas no instrumento convocatório, exceto quando se tratar de incentivo à inovação tecnológica ou de serviços de informática; III - o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a Administração Pública Estadual ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado e à economia de escala;.

2.12.5. No caso aqui exposto, com toda a contextualização elaborada até então, fica evidente que o inciso III se amolda à situação ora posta, já vez que por se tratar de solução e serviços não divisíveis, não caberia particionar a entrega dos itens do lote entre fornecedores distintos.

2.12.6. Considera-se "não vantajosa a contratação" quando: *§ 1º Para fins do disposto no inciso III, considera-se não vantajoso para a Administração quando o tratamento diferenciado e simplificado não for capaz de alcançar os objetivos previstos no art. 30 desta Lei, justificadamente, ou resultar em preço superior ao valor estabelecido como referência*. (Lei Nº 15.306, de 08 de janeiro de 2013 do Estado do Ceará, Art. 39).

2.12.7. Diante do explanado, conclui-se que não há óbice quanto à aplicação da Lei Complementar 123/2006. Entretanto não é possível a divisão ou fragmentação dos itens em partes e nem aplicação do benefício da exclusividade para que ocorra a participação para ME/EPP, ante da impossibilidade da divisão técnica dos itens, conforme explanação apresentada neste Termo de Referência.

2.13. Da Subcontratação, Cisão ou Incorporação

2.13.1. Não será permitida a subcontratação total ou parcial do objeto.

2.13.2. Não será admissível a fusão, cisão ou incorporação da CONTRATADA.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Fornecimento de serviços para a implantação de um Security Operations Center (SOC), que é uma unidade imprescindível para a segurança da informação do TJCE, composta por diferentes equipes especializadas. Nesta contratação de serviços, as soluções requeridas são:

3.1.1. Serviço de gestão de incidentes de segurança (Blue Team): Serviço de desenvolvimento, planejamento, acompanhamento de implantação e manutenção das medidas de segurança da informação do TJCE, bem como detectar incidentes e elaborar estratégias, diagnosticar e acompanhar respostas a incidentes de segurança, com o objetivo de proteger ativos de informação e garantir a confidencialidade, integridade e confidencialidade dos dados do TJCE (Blue Team). Os detalhes técnicos

e operacionais são apresentados no documento TRF ANEXO I.

3.1.2. Serviço de gestão testes de invasão (Red Team): Serviço de execução de avaliações de segurança e testes de invasão, internos e externos, nos sistemas, aplicativos e infraestrutura do TJCE, com o objetivo de identificar vulnerabilidades, avaliar a eficácia das medidas de segurança implementadas e solicitar implementações das vulnerabilidades encontradas (Red Team). Os detalhes técnicos e operacionais são apresentados no documento TRF ANEXO I.

3.1.3. Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação: Serviços gerenciados de monitoramento e correlação de eventos, por meio de correlacionamento de logs, pacotes de redes e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, para detectar, analisar e responder a ameaças de segurança por meio do monitoramento e análise centralizado de logs de todos os ativos de rede atuais e considerados em demandas futuras do TJCE, usando a ferramenta SIEM com quantidade mínima de funcionamento de 3.000 EPS. Os detalhes técnicos e operacionais são apresentados no documento TRF ANEXO I.

4. ESPECIFICAÇÃO TÉCNICA

4.1. Conforme consta no documento TRF ANEXO I**.**

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Após a assinatura do contrato, será agendada uma reunião de alinhamento como primeira etapa do período de transição. O objetivo dessa reunião é facilitar a transferência de conhecimentos e a transição dos serviços para a CONTRATADA.

5.2. A execução do objeto seguirá a seguinte dinâmica:

5.2.1. A CONTRATADA deverá implantar os serviços, no prazo máximo de 30 dias corridos após assinatura de contrato e Ordem de Serviço das soluções contratadas com, pelo menos, os seguintes requisitos atendidos e documentados em um relatório de implantação:

5.2.1.1. Lotação de todos os profissionais alocados por perfil (com a devida documentação comprobatória conforme itens 2.4, 3.4 e 4.8 do documento TRF ANEXO I) para os horários de expediente regular e de plantão contínuo.

5.2.1.2. Comprovação da disponibilidade de uso dos recursos de TI descritos no item 1.3.6 do documento TRF ANEXO I para viabilização de imediata prestação

de serviços.

5.2.1.3. Relatório técnico produzido através da ferramenta SIEM, comprovando:

5.2.1.3.1. Coleta de logs efetuada pelo Coletor *on-premise*, conforme descrito nos itens (com subitens) de 4.2 e 4.3 do documento TRF ANEXO I.

5.2.1.3.2. Regras preestabelecidas, normalização e correlação de eventos conforme o item (com subitens) de 4.4. do documento TRF ANEXO I.

5.2.1.3.3. Capacidade de emitir alertas e notificações conforme item (com subitens) 4.2 do documento TRF ANEXO I.

5.2.1.3.4. Ter inicializado o armazenamento de logs conforme item 4.2.19 do documento TRF ANEXO I.

5.2.1.3.5. Apresentar o Dashboard em funcionamento conforme os itens (com subitens) 4.2.30, 4.2.31 e 4.2.32 do documento TRF ANEXO I.

5.2.1.3.6. Console de administração e operação do SIEM em funcionamento conforme item (com subitens) 4.5.3 do documento TRF ANEXO I.

5.2.2. Após a implantação, o TJCE emitirá um **Termo de Recebimento Provisório (TRP)** e em até 5 dias úteis validará a implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Caso a validação indique pendências de implantação, a CONTRATADA deverá executar as retificações em até 15 dias corridos.

5.2.3. Após a validação sem pendências da implantação, será assinado o **Termo de Recebimento Definitivo (TRD)** de implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Somente a partir da assinatura do TRD, a execução dos serviços será considerada inicializada para finalidade de pagamento, o qual será mensal e sujeito a glosas conforme o item 5.2.4 deste TR e a Tabela 5 do documento TRF ANEXO I.

5.2.4. Até 30 dias corridos após o TRD de implantação, a CONTRATADA deve apresentar um **plano de trabalho anual** com atividades mensais a serem executadas pelos membros do Blue/Red Team e a equipe de Serviços gerenciados de monitoramento e correlação de eventos. O plano de trabalho deverá ser validado pela equipe de segurança do TJCE e poderá ser modificado sob demanda da equipe de segurança do TJCE em qualquer momento.

5.2.5. O período inicial de 90 (noventa) dias corridos, após a assinatura do TRD de implantação, será considerado como período de estabilização da operação dos serviços,

durante o qual os indicadores de serviço não atingidos terão aplicadas as glosas de Tabela 4 e Tabela 5 do documento TRF ANEXO I para todos os serviços contratados, conforme os seguintes critérios em dias corridos:

5.2.5.1. Nos primeiros 30 (trinta) dias: não serão aplicadas as glosas previstas nas Tabelas 4 e 5 do documento TRF ANEXO I para cada ocorrência de indicador de serviço não atingido.

5.2.5.2. Do 31º ao 60º dia: aplicar-se-á efetivamente 25% (cinquenta por cento) dos pontos previstos em Tabela 4 e Tabela 5 do documento TRF ANEXO I para cada ocorrência de indicador de serviço não atingido. Nesta etapa todos os serviços descritos nos itens 2, 3 e 4 do documento TRF ANEXO I devem estar totalmente configurados corretamente.

5.2.5.3. Do 61º ao 90º dia: aplicar-se-á efetivamente 50% (setenta e cinco por cento) dos pontos previstos em Tabela 4 e Tabela 5 do documento TRF ANEXO I para cada ocorrência de indicador de serviço não atingido.

5.2.5.4. Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos em Tabela 4 e Tabela 5 do documento TRF ANEXO I para cada ocorrência de indicador de serviço não atingido.

5.2.5.5. Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização.

5.3. Reunião de Alinhamento e entrega do cronograma

5.3.1. O coordenador do SOC, em conjunto com o Blue/Red Team e a equipe de Serviços gerenciados de monitoramento e correlação de eventos (ver Tabela 2 do documento TRF ANEXO I**)**, deve apresentar mensalmente um relatório contendo as atividades executadas pelo SOC, as quais devem ser correlacionadas com as atividades do plano de trabalho anual (ver item 5.2.3 deste documento). Para o primeiro mês, o relatório deverá conter um diagnóstico do estado de maturidade da segurança da informação do TJCE e as ações a serem executadas no plano de trabalho proposto.

5.3.2. Um resumo das atividades rotineiras por equipe, unidade de prestação de serviços e frequência de serviços é mostrada na seguinte Tabela. Vale a pena ressaltar que a descrição detalhada dos serviços contratados está nos itens 2, 3 e 4 do documento TRF ANEXO I.

Serviço	Atividade Operacional	Unidade	Frequência
1	**Serviço de gestão de incidentes de segurança (Blue Team):**	Mensal	Rotineiro

	Análise, resolução, controle e documentação de eventos e incidentes de segurança da informação, seguindo os principais Frameworks de gestão de incidentes de segurança da informação e as melhores práticas de mercado.		ou por Requisição de Serviço
2	**Serviço de gestão testes de invasão (Red Team):** Identificar, mapear e documentar potenciais vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Para realizar esses testes, são utilizadas técnicas e ferramentas específicas com o intuito de simular a obtenção de acesso não autorizado e privilegiado aos ativos e informações. Além disso, o serviço também fornece recomendações para corrigir as vulnerabilidades identificadas, visando fortalecer a segurança dos sistemas e proteger os ativos e dados sensíveis.	Mensal	Requisições de Serviço
3	**Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação:** Realizar o monitoramento constante e ininterrupto dos ativos de segurança da informação, assim como de ataques cibernéticos direcionados ao TJCE. Serviço a ser realizado por meio do correlacionamento de logs, pacotes de rede e detecção de comportamentos anômalos em aplicações, serviços e infraestrutura com a ferramenta tecnológica SIEM. As atividades têm como objetivo identificar eventos de segurança da informação, que serão analisados e podem ser classificados como incidentes de segurança, conforme estabelecido no processo de gestão de incidentes.	Mensal	Rotineiro ou por Requisições de Serviço

5.3.3. Após a emissão do TRD de implantação, o coordenador do SOC, em conjunto com o Blue/Red Team e a equipe de serviços gerenciados de monitoramento e correlação de eventos (ver Tabela 2 do documento TRF ANEXO I), devem apresentar semanal e mensalmente, em reunião, um resumo do estado geral de segurança do TJCE, contendo: eventos, incidentes e vulnerabilidades relevantes da rede, trabalhos futuros de mitigação e estado do andamento das atividades rotineiras e sob demanda, as quais devem ser vinculadas com o plano de trabalho do SOC.

5.3.4. As requisições de serviço poderão ser abertas a qualquer momento,

independentemente do horário ou do dia, incluindo dias úteis, finais de semana, feriados e pontos facultativos, e deverão ser executados em conformidade com os níveis de serviços estabelecidos no documento TRF ANEXO I.

5.3.5. A CONTRATADA deverá disponibilizar todas as informações essenciais para a transição para uma possível e futura NOVA CONTRATADA, no prazo mínimo de 30 dias corridos antes do fim do contrato, desde que não seja efetivada a renovação do contrato. Além disso, será responsável por elaborar e atualizar toda a documentação necessária que possa não ter sido adequadamente gerada ou atualizada durante a vigência do contrato.

5.4. Local de Execução do Serviço

5.4.1. A execução dos serviços, assim como entrega e instalação dos equipamentos deverá ocorrer no seguinte endereço, após agendamento prévio com o fiscal técnico ou seu substituto: Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 - Edson Queiroz, Fortaleza - CE, 60811-690.

5.5. Forma de avaliação da qualidade dos bens e/ou serviços entregues.

5.5.1. Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, o TJCE, através do Fiscal Técnico, realizará, anualmente, a Avaliação de Desempenho, o que permitirá a adoção de eventuais ajustes no modelo de atendimento, conforme critérios abaixo, podendo ser criados outros que se fizerem necessários.

5.5.2. **Comunicação**: Avaliação qualitativa da comunicação do Contratado, como clareza na informação, formas de solicitações e questionamentos ao TJCE, educação e nível de formalidade no atendimento e tempo de resposta às solicitações.

5.5.3. **Confiabilidade**: Prestação correta (isenta de falhas e erros) do serviço/atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas.

5.5.4. **Organização**: Demonstração de planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

5.5.5. Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos seguintes conceitos: Péssimo (de 0 a 4,9) / Regular (de 5 a 7,4) / Bom (de 7,5 a 8,9) / Ótimo (de 9 a 10).

5.5.6. Anualmente, a empresa contratada será informada do conceito médio obtido no período e registrado nos autos do contrato, resultado este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

5.6. Todas as informações relevantes para o dimensionamento da proposta estão detalhadas no item 4.6 do documento TRF ANEXO I.

5.7. O horário e regime de execução do serviço é detalhado no item (com subitens) 1.3 do documento TRF ANEXO I.

5.8. Medição de resultados

5.8.1. Os serviços serão medidos, controlados e acompanhados pela Contratante durante o período de vigência do contrato de acordo com os Níveis Mínimos de Serviço (NMS) e suas respectivas notificações ou penalidades, as quais estão detalhadas no item 5 do documento TRF ANEXO I.

5.9. Mecanismos formais de comunicação

5.9.1. A metodologia adoptada para a requisição de serviços está detalhada no item 1.6 do documento TRF ANEXO I.

5.9.2. A CONTRATADA deverá emitir mensalmente, junto ao pedido de pagamento, o Relatório de Níveis Mínimos de Serviços, constando indicadores de requisições de serviços, NMS e chamados técnicos abertos, em andamento e encerrados no período, com no mínimo as seguintes informações:

5.9.2.1. Número do contrato.

5.9.2.2. Fiscal técnico responsável.

5.9.2.3. Número de chamado.

5.9.2.4. Descrição da ocorrência.

5.9.2.5. Severidade.

5.9.2.6. Nome de quem registrou o chamado ou solicitou abertura do chamado.

5.9.2.7. Data e hora de abertura do chamado.

5.9.2.8. Data e hora do início do atendimento.

5.9.2.9. Data e hora do atendimento local, se for o caso.

5.9.2.10. Data e hora de solução ou medida de contorno.

5.9.2.11. Descrição da resolução adotada.

5.9.3. Os relatórios deverão ser entregues mesmo quando não houver chamados/ocorrências no período.

5.9.4. Após a análise e aprovação do relatório descrito no item anterior, a Contratante deverá emitir o documento “Autorização para Faturamento”, descrito no próximo item deste TR.

5.9.5. Autorização para Faturamento: Autorização emitida pelo Fiscal Administrativo do Contrato ao Preposto da Contratada. Este documento contém a autorização para que a Contratada possa efetuar o faturamento.

5.10. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

5.10.1. A garantia contratual dos serviços, complementar à garantia legal, deve atender as

especificações técnicas do item 4 e os NMS descritos no item 5 do documento TRF ANEXO I, pelo prazo mínimo contratual de 36 (trina e seis) meses, contado a partir do primeiro dia útil subsequente à data do TRD.

6. MODELO DE GESTÃO DO CONTRATO

6.1. Deveres e Responsabilidades da Contratante.

6.1.1. Designar formalmente, na forma do art. 177, da Lei nº 14.133/21, representantes para gerenciar e exercer a fiscalização da execução do Contrato, independentemente do acompanhamento e controle exercido pela Contratada.

6.1.2. Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste TR, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE.

6.1.3. Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. Ele deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

6.1.4. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas.

6.1.5. Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com os termos do contrato assinado.

6.1.6. Proporcionar todas as condições e prestar as informações necessárias para que a Contratada possa cumprir com suas obrigações, dentro das normas e condições contratuais.

6.1.7. Prestar, por meio do Fiscal Técnico do Contrato, as informações e os esclarecimentos pertinentes aos serviços/bens avençados, que porventura venham a ser solicitados pela Contratada.

6.1.8. Informar à Contratada sobre atos que possam interferir direta ou indiretamente nos serviços prestados/entrega de bens.

6.1.9. Comunicar oficialmente à Contratada, quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

6.1.10. Registrar e oficializar a Contratada sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

6.1.11. Rejeitar, no todo ou em parte, os serviços executados que não atendam às especificações técnicas deste Termo de Referência.

6.1.12. Aprovar ou rejeitar, no todo ou em parte, os serviços executados ou entrega de equipamentos, que não estiverem em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

6.1.13. Efetuar o pagamento devido pela prestação dos serviços executados, desde que cumpridas todas as formalidades e exigências avençadas.

6.1.14. Aplicar as sanções previstas em contrato, assegurando à Contratada o contraditório e a ampla defesa.

6.1.15. Exigir, sempre que necessário, a apresentação da documentação pela CONTRATADA que comprove a manutenção das condições que ensejaram a sua contratação.

6.2. Deveres e Responsabilidades da Contratada

6.2.1. Manter atualizados seus dados cadastrais junto ao TJCE.

6.2.2. Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela Contratada, sem ônus adicional ao TJCE.

6.2.3. Cumprir fielmente os Níveis Mínimos de Serviço (NMS), conforme o item 5 do documento TRF ANEXO I, e demais especificações técnicas deste Termo de Referência.

6.2.4. Conceder acesso ao TJCE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do TJCE.

6.2.5. Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJCE, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.

6.2.6. Credenciar devidamente um Preposto para representá-lo em todas as questões relativas ao cumprimento dos serviços, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa com o TJCE e a equipe da CONTRATADA, sem custo adicional.

6.2.7. Assumir total responsabilidade pela execução dos serviços, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.

6.2.8. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.

6.2.9. Comunicar ao TJCE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos.

6.2.10. Submeter ao TJCE qualquer alteração que se tornar essencial à continuação da execução dos serviços.

6.2.11. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

6.2.12. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.

6.2.13. Selecionar e preparar rigorosamente o(s) empregado(s) que irá(ão) prestar os serviços.

6.2.14. Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência.

6.2.15. Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços.

6.2.16. Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, realizando-os de forma meticulosa e constante, mantendo sempre em perfeita ordem.

6.2.17. Orientar seus empregados de que não poderão se retirar dos prédios ou instalações da Contratante portando volumes ou objetos sem a devida autorização e liberação do Fiscal do contrato.

6.2.18. Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do CONTRATANTE, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

6.2.19. Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste

documento.

6.2.20. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço ou entrega de bens, ou em conexão com ele, ainda que acontecido em dependências do CONTRATANTE.

6.2.21. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.

6.2.22. Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços ou entrega de bens, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente.

6.2.23. Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.

6.2.24. Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua regularização.

6.2.25. Não transferir a outrem, no todo ou em parte, a execução do contrato.

6.2.26. Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

6.2.27. Responsabilizar-se pela conduta do empregado que for incompatível com as normas da Contratante, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação.

6.2.28. Receber as observações do Fiscal Técnico do contrato, relativamente ao desempenho das atividades/entrega de bens, e identificar as necessidades de melhoria.

6.2.29. Registrar e controlar, diariamente, as ocorrências e os serviços sob sua responsabilidade.

6.2.30. Permitir a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo Contratante, em conformidade com o artigo 117 da Lei nº 14.133/21.

6.2.31. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21.

6.2.32. Indenizar quaisquer danos ou prejuízos causados ao TJCE ou a terceiros, por ação ou

omissão do seu pessoal durante a execução dos serviços/entrega de bens.

6.2.33. Não colocar à disposição da Contratante, para o exercício de funções de chefia, pessoal que incidam na vedação dos artigos 1º e 2º da Resolução nº 156/2012 do Conselho Nacional de Justiça (Art. 4º - Resolução 156/2012 – CNJ).

6.2.34. Encaminhar para o atesto dos fiscais, as faturas emitidas dos serviços prestados.

6.2.35. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o CONTRATAN-TE for compelido a responder em decorrência desta avença.

6.2.36. Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços ou entrega de bens, da relação contratual mantida com o CONTRATANTE.

6.2.37. Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

6.2.38. Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.

6.2.39. Comprovar vínculo empregatício dos profissionais disponibilizados para prestação dos serviços objeto desta contratação através de Ficha de Registro de Empregado, ou Carteira de Trabalho, ou contrato de prestação de serviço (ou documento similar) ou ainda Contrato Social da empresa, em casos de vínculo societário.

6.2.40. Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo contratante.

6.2.41. Não subcontratar, ceder ou transferir, total ou parcial o objeto desta contratação.

6.2.42. Recrutar e selecionar os profissionais necessários à realização do serviço, de acordo com a qualificação técnica exigida, a ser previamente submetida ao Fiscal para verificação da conformidade.

6.2.43. Fornecer ao TJCE, ao início da prestação do serviço, a relação nominal dos técnicos que atuarão no cumprimento do objeto contratado, atualizando-a sempre que necessário.

6.2.44. Tal documentação deverá ser juntada nos autos dos contratos.

6.2.45. Manter atualizada a documentação comprobatória da qualificação dos profissionais alocados na execução do serviço e disponibilizar essa documentação ao Tribunal, sempre que solicitada.

6.2.46. Manter o TJCE formalmente avisado sobre demissões de profissionais que prestem serviço nas dependências do Tribunal, para fins de cancelamento da autorização de entrada e acessos a recursos, sistemas e aplicativos do TJCE.

6.2.47. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos, níveis, indicadores e condições não sejam cumpridos.

6.2.48. Conceder acesso ao TJCE, o controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do mesmo.

6.3. Forma de Acompanhamento do Contrato

ID	Evento	Forma de Acompanhamento
1	Da entrega da solução	O recebimento do objeto deverá ocorrer conforme definido no item 5 e seus subitens.
2	Durante a vigência do Contrato.	Será verificado o cumprimento do prazo de solução dos chamados, conforme descrito no item 5 do documento TRF ANEXO I.

6.4. Metodologia de Avaliação da Qualidade

6.4.1. Conforme item 5.5.

6.5. Níveis de Serviço

6.5.1. Conforme item 5.7.

6.6. Estimativa do Volume de Bens/Serviço

6.6.1. Conforme item 1.2.

6.7. Prazos e Condições

6.7.1. Os prazos são detalhados na seguinte Tabela:

N.º	Etapa	Quando	Responsável
1	Assinatura do contrato	Após a homologação do certame.	CONTRATANTE e CONTRATADA
2	Implantação dos serviços conforme os requisitos apresentados no item 5.2.1 por parte da CONTRATADA e entrega do TRP da CONTRATANTE para a CONTRATADA.	Em até 30 (trinta) dias corridos contados após a assinatura do contrato.	CONTRATANTE e CONTRATADA
3	Validação da implantação dos serviços (etapa anterior) mediante a emissão do TRD da CONTRATANTE para a CONTRATADA em caso de não possuir pendências ou solicitação de retificações para que a CONTRATADA	Em até 5 (cinco) dias úteis após a emissão do TRP.	CONTRATANTE

	efetue as correções e solicite um novo TRP (volta a Etapa 2).		
4	Início do período de validade/vigência dos serviços.	A partir da data de emissão do TRD.	CONTRATADA

6.7.2. Condições conforme o item 5.

6.8. Do Reajuste

6.8.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de apresentação da proposta.

6.8.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custo da Tecnologia da Informação (ICTI) - Ipea, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.8.2.1. O processo referente ao pedido de Reajuste supra deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.

6.9. Condições para Pagamento

6.9.1. Os pagamentos serão realizados através de depósito bancário, preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento mensal e definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade com as medições realizadas, validado previamente pela CONTRATANTE atestada pelo setor competente deste Tribunal de Justiça, via emissão do Termo de Recebimento Definitivo, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

6.9.2. O prazo para pagamento de faturas ou notas fiscais serão suspensos durante o período de indisponibilidade do sistema de pagamento do Estado do Ceará ao final de cada exercício financeiro, aproximadamente entre 20 de dezembro e 31 de janeiro do ano subsequente, cujos pagamentos serão realizados até o final da primeira quinzena do mês de fevereiro.

6.9.3. O Tribunal de Justiça reserva-se ao direito de recusar o pagamento, no ato do atesto, caso o objeto não esteja em conformidade com as condições deste instrumento.

6.9.4. Nenhum pagamento será efetuado à empresa antes regularizada as sanções que por ventura lhe tenham sido aplicadas.

6.9.5. Nas notas fiscais referentes aos serviços objeto do contrato, deverão estar descriminados os valores dos tributos: impostos sobre serviços – ISS, PIS/PASEP,

COFINS, FUST, FUNTTEL.

6.9.6. Os serviços de suporte e manutenção serão faturados mensalmente após a solicitação de pagamento por parte da CONTRATADA, sendo o pagamento condicionado ao aceite do Relatório de Instrumento de Medição de Resultados, conforme item 5.9.2, por parte da CONTRATANTE:

6.9.6.1. O valor do pagamento mensal estará diretamente vinculado ao índice alcançado para os indicadores estabelecidos, sendo pago conforme resultado obtido e decrementado (cumulativamente) quando não forem atingidas as metas exigidas.

6.9.6.2. Caso a CONTRATADA não cumpra com os seus compromissos, de qualidade e desempenho, terá a sua fatura reduzida conforme estabelecido nas Glosas apresentadas no item 5 do documento TRF ANEXO I.

6.9.6.3. Os redutores deverão ser levantados pela Contratada, anexados à solicitação de pagamento, sendo validados pelo TJCE. Os redutores serão aplicados sobre o faturamento mensal na ocorrência dos fatos geradores, independentemente da abertura de processo administrativo.

6.9.7. Constatada a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

6.9.8. Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

6.9.9. Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a CONTRA-TADA a ampla defesa.

6.9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação

6.9.11. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

6.9.12. Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) estar em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

6.9.13. O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual.

6.9.14. Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

6.9.15. Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

6.9.16. A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

6.10. Propriedade, Sigilo, Restrições

6.10.1. A CONTRATADA cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do Art. 93, da LEI Nº 14.133, DE 1º DE ABRIL DE 2021, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência do objeto contratado, entendendo-se por resultados quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros.

6.10.2. Toda a documentação produzida pela CONTRATADA referente à implantação dos equipamentos e documentos exigidos no termo de referência passam a ser propriedade de forma perpétua do TJCE, não precisando este Tribunal de autorização da CONTRATADA para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

6.10.3. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados (em outros contratos) pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso.

6.10.4. A obrigação assumida de Confidencialidade permanecerá válida durante o período de

vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente.

6.10.5. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados que, a qualquer título, venham a integrar a equipe executante do Objeto, a assinatura do **ANEXO III - TERMO DE CIÊNCIA**, bem como a assinatura do **ANEXO IV - TERMO DE COMPROMISSO**, onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

6.10.6. A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte, mediante assinatura do Termo de Confidencialidade constante no Termo de Referência.

6.11. Mecanismos Formais de Comunicação

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Emissão da Requisição de serviço/fornecimento	Contratante	Contratada	Requisição de serviço/fornecimento	Quando demandado pela SETIN.
Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, email, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato portável.	Quando necessário

7. ESTIMATIVA DE PREÇO

7.1. Os valores médios da Pesquisa de mercado e Memória de cálculo citados no item 2.6.2 são apresentados na seguinte Tabela.

7.2. As demandas previstas com IDs 4, 5 e 6 da próxima Tabela poderão ser contratadas opcionalmente, sob demanda de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual.

7.3. O custo fixo da contratação é o resultado da soma dos itens com Ids 1, 2 e 3 do VALOR MÉDIO (média aritmética simples) da Tabela mostrada abaixo. Ou seja R$ 8.427.276,68 para 36 meses, resultando em um valor aproximado de R$ 234.091,02 por mês ou R$ 2.809.092,23 por ano.

7.4. As demandas opcionais previstas com IDs 4, 5 e 6 da próxima Tabela contam com o seguinte VALOR MÉDIO (média aritmética simples) anual sob demanda: R$ 11.879,33 por pacote de 500EPS, R$ 23.051,66 por pacote de 1.000 EPS e R$ 42.300,00 por pacote de 2.000 EPS.

Id	Item	Qtd. Meses	Vlr. Unit Médio	Vlr. Total Médio
1	Serviço de gestão de incidentes de segurança (Blue Team).	**36**	**R$ 88.920,31**	**R$ 3.201.131,16**
2	Serviço de gestão testes de invasão (Red Team).	**36**	**R$ 47.177,13**	**R$ 1.698.376,68**
3	Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS.	**36**	**R$ 97.984,32**	**R$ 3.527.435,52**
Id	**Item**	**Qtd. Pacotes**	**Vlr. Unit Médio**	**Vlr. Total Médio**
4	Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.	**10**	**R$ 11.879,33**	**R$ 118.793,30**
5	Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.	**10**	**R$ 23.051,66**	**R$ 230.516,60**

6	Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.	10	**R$ 42.300,00**	**R$ 423.000,00**
Valor Total				**R$ 9.199.253,26**

8. ADEQUAÇÃO ORÇAMENTÁRIA

Fonte	**TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - PROMOJUD**
Programa	**512 - EXCELÊNCIA NO DESEMPENHO DA PRESTAÇÃO JURISDICIONAL**
Ações	**15504 - MODERNIZAÇÃO DA INFRAESTRUTURA DE TI - 1º GRAU (PROMOJUD - COMP. I)**

Período	ID	Item	QTD. Meses	Valor Unitário	Valor (1° Grau) Investimento
2023	1	Serviço de gestão de incidentes de segurança (Blue Team).	36	R$ 88.920,31	**R$ 3.201.131,16**
	2	Serviço de gestão testes de invasão (Red Team).	36	R$ 47.177,13	**R$ 1.698.376,68**
	3	Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS.	36	R$ 97.984,32	**R$ 3.527.435,52**

Período	ID	Item	Qtd. Pacotes	Valor Unitário	Valor (1° Grau) Investimento
2023	4	Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.	10	R$ 11.879,33	**R$ 118.793,30**
	5	Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.	10	R$ 23.051,66	**R$ 230.516,60**
	6	Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.	10	R$ 42.300,00	**R$ 423.000,00**
Valor total					**R$ 9.199.253,26**

9. SANÇÕES APLICÁVEIS

9.1. Comete infração administrativa, nos termos da lei, a licitante que:

9.1.1. I - deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pela Administração, em sede de diligência.

9.1.2. II - salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

9.1.2.1. a) não enviar a proposta ajustada após a negociação;

9.1.2.2. b) recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. c) pedir para ser desclassificado quando encerrada a etapa competitiva;

9.1.2.4. d) deixar de apresentar amostra, quando exigível.

9.1.3. III - não celebrar o contrato ou não entregar a garantia ou documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.

9.1.4. IV - recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

9.1.5. V - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

9.1.6. VI - fraudar a licitação.

9.1.7. VII - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.7.1. a) agir em conluio ou em desconformidade com a lei;

9.1.7.2. b) induzir deliberadamente a erro no julgamento;

9.1.7.3. c) apresentar amostra falsificada ou deteriorada;

9.1.7.4. d) praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

9.1.7.5. e) praticar ato lesivo previsto no art. 5° da Lei 12.846/2013.

9.2. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido no instrumento convocatório, descrita no item 9.1.3 (inciso IV), caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação. A exigência da garantia obedecerá ao disposto no art. 58 da Lei nº 14.133/2021.

9.3. Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar a contratada as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.3.1. I – advertência;

9.3.2. II – multa;

9.3.3. III - impedimento de licitar e contratar; e

9.3.4. IV - declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.4. Na aplicação das sanções serão considerados:

9.4.1. I - a natureza e a gravidade da infração cometida;

9.4.2. II - as peculiaridades do caso concreto;

9.4.3. III - as circunstâncias agravantes ou atenuantes;

9.4.4. IV - os danos que dela provierem para a Administração Pública;

9.4.5. V - a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.5. A sanção de multa calculada na forma do edital ou do contrato, não será inferior a 0,5% (cinco décimos por cento), nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.

9.5.1. A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o complementem, às sanções e penalidades administrativas, inclusive multas.

9.5.1.1. Caso a Contratada se torne inadimplente na execução dos serviços, a Contratante poderá, sem prejuízo de outras medidas, a título de multa, o equivalente a 0,5% (cinco décimos por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, para a conclusão da demanda, nos termos e condições dispostas no Termo de Referência, sem prejuízo das sanções legais e responsabilidades civil e criminal.

9.5.2. A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

9.5.3. Os percentuais de multas aplicadas incidirão sempre sobre do valor global do termo de contrato licitado ou celebrado ou instrumento equivalente.

9.6. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.7. Na aplicação da sanção será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.8. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no item 9.1 (incisos I, II e III), quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.9. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas no item 9.1 (incisos IV, V, VI e VII), bem como pelas infrações administrativas previstas no item 9.1 (incisos I, II e III) que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

9.15. Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

9.16. As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.

9.17. Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

9.18. Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 156 da Lei n. 14.133/21:

9.18.1. Aplicação de multa administrativa, além das Glosas previstas no item 5.7.

9.18.1.1.Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas

hipóteses de inexecução total ou violação do sigilo.

9.18.1.2. Na ordem de 0,5% do valor total da contratação, ao dia de suspenção ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços contratados ao total de 10%, moratório.

9.18.1.3. Caso os limites do subitem anterior sejam excedidos, configura-se então casos de inexecução contratual.

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Proposta de Preço

10.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:

10.1.1.1. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

10.1.1.2. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

10.1.1.3. Deve fazer menção ao número do pregão e do processo licitatório;

10.1.1.4. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

10.1.1.5. Deve conter na última folha o número do CNPJ da empresa;

10.1.1.6. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

10.1.1.7. Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a licitante julgar necessário;

10.1.1.8. Indicação do nome do banco, número da agência, número da conta corrente, para fins de recebimento dos pagamentos.

10.1.1.9. Objetivando facilitar e agilizar o processo de validação das especificações técnicas da Solução e como forma de comprovação, a licitante deverá anexar todas as documentações técnicas comprobatórias das características e especificações para cada item do Serviços a serem adquiridos.

10.1.1.10. Deverá ser anexado junto a sua proposta, documento contendo o item do Edital e sua referência comprobatória, informando/indicando/referenciando as referidas documentações técnicas comprobatórias.

10.2. Modalidade e Tipo de Licitação

10.2.1. A modalidade da licitação sugerida é o Pregão Eletrônico, em conformidade com a Lei

14.133/21, tendo em vista o objeto se tratar de bem e serviço comum, cujos padrões de qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

10.2.2. A licitação será do tipo menor preço. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item 7.

10.2.3. O objeto desta contratação será realizado por execução indireta, sob o regime de empreitada por Preço Unitário, nos termos dos art. 46°, I, da Lei n. 14.133/21.

10.3. Justificativa de Adoção da Modalidade da Licitação

10.3.1. Modalidade de Licitação

10.3.1.1. A contratação da solução ora pretendida é oferecida por diversos fornecedores no mercado de TIC, vez que apresenta características padronizadas e usuais. Assim, trata-se de serviço comum pois é fácil encontrar empresas no mercado que ofereçam serviços de tecnologia da informação, manutenção, suporte e garantia da Solução pretendida. Devido à alta demanda por esses serviços, no setor privado e público, há uma ampla oferta de fornecedores com diferentes níveis de expertise e qualidade e, portanto, licitação via Pregão, em sua forma eletrônica, pelo tipo menor preço individual, previamente ao menor preço individual de cada item, e modo de disputa aberto e fechado.

10.3.1.2. Nos critérios de habilitação técnica, não serão solicitados prazos de validades dos atestados de capacidade técnica, abrangendo maior competitividade no certame, sem deferir os ditames legais, vez que o objeto que será licitado é usual de mercado e não possui uma existência muito longeva, para limitar períodos. Serão solicitados documentos/atestados emitidos por fabricantes de alguns componentes, em detrimento dos vários itens tecnológicos e do alto montante orçamentário.

10.4. Qualificação Econômico-Financeira

10.4.1. A Qualificação Econômico-Financeira tem como objetivo avaliar a capacidade financeira e econômica das empresas interessadas em participar da concorrência, garantindo assim a segurança do contrato e a viabilidade do projeto. No Tribunal de Justiça do Ceará, a Qualificação Econômico-Financeira é um critério importante para a escolha da empresa vencedora, pois garante a solvência financeira e a capacidade de cumprimento do contrato firmado.

10.4.2. Certidão negativa de falência, concordata, recuperação judicial ou extrajudicial, expedida por quem de competência na sede da pessoa jurídica ou certidão negativa de execução patrimonial expedida no domicílio da pessoa física.

10.4.3. No caso de cooperativa, a mesma está dispensada da apresentação da Certidão exigida no subitem acima.

10.4.4. **BALANÇO PATRIMONIAL** e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira do licitante, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 meses da data de apresentação da proposta.

10.4.5. **COMPROVAÇÃO DA BOA SITUAÇÃO FINANCEIRA** atestada por documento, assinado por profissional legalmente habilitado junto ao Conselho Regional de Contabilidade da sede ou filial do licitante, demonstrando que a empresa apresenta índice de Liquidez Geral (LG) maior ou igual a 1,0 (um vírgula zero), calculada conforme a fórmula abaixo:

LG = (AC + ARLP)/(PC + PELP) ≥ 1,0

Onde:

LG – Liquidez Geral.

AC – Ativo Circulante.

ARLP – Ativo Realizável a Longo Prazo.

PC – Passivo Circulante.

PELP – Passivo Exigível a Longo Prazo.

10.4.6. No caso de sociedade por ações, o balanço deverá ser acompanhado da publicação em jornal oficial, em jornal de grande circulação e do registro na Junta Comercial.

10.4.7. No caso das demais sociedades empresárias, o balanço deverá ser acompanhado dos termos de abertura e de encerramento do Livro Diário - estes termos devidamente registrados na Junta Comercial - constando ainda, no balanço, o número do Livro Diário e das folhas nos quais se acha transcrito ou autenticada na junta comercial, devendo tanto o balanço quanto os termos ser assinados por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

10.4.8. No caso de empresa recém-constituída (há menos de 01 ano), deverá ser apresentado o balanço de abertura acompanhado dos termos de abertura e de encerramento devidamente registrados na Junta Comercial, constando no balanço o número do Livro e das folhas nos quais se acha transcrito ou autenticado na junta comercial, devendo ser assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

10.4.9. No caso de sociedade simples e cooperativa - o balanço patrimonial deverá ser inscrito no Cartório de Registro Civil de Pessoas Jurídicas assinado por contador registrado no

Conselho Regional de Contabilidade e pelo titular ou representante legal da instituição, atendendo aos índices estabelecidos neste instrumento convocatório.

10.4.10. **PATRIMÔNIO LÍQUIDO MÍNIMO** não inferior a 10% da estimativa de custos, que deverá ser comprovado através da apresentação do balanço patrimonial.

10.4.11. A comprovação solicitada visa garantir que a CONTRATADA possua capacidade e porte suficiente para atender ao objeto desta contratação, bem como a capacidade financeira de sustentar suas atividades diante das oscilações de demandas que ocorrem durante a vigência do contrato.

10.5. Qualificação Técnica

10.5.1. Com o intuito de minimizar os riscos da contratação e alcançar os resultados esperados, é imprescindível que o LICITANTE possua capacidade técnica e de fornecimento para executar o objeto da licitação.

10.5.2. A exigência de comprovação de capacidade técnica relacionada ao objeto licitado se dá com fulcro no Art. 67 inciso I da Lei nº 14.133/21 e visa garantir que a LICITANTE já forneceu os serviços a serem contratados e, portanto, possui capacidade técnico-operacional para fornecê-lo adequadamente.

10.5.3. Conforme o Art. 67, inciso VI e § 2º da Lei nº 14.133/21: *§ 2º Observado o disposto no caput e no § 1º deste artigo, será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados.*; a licitante classificada deverá apresentar, para fins de habilitação, 1 (um) ou mais atestados de capacidade técnica que comprove a capacidade de fornecimento de serviços em até o mínimo 50% das demandas tecnológicas citadas nos itens 2, 3, 4 e na Tabela 3 do documento TRF ANEXO I. Os atestados de capacidade técnica devem atender os requisitos mostrados nos subitens 10.5.3.1 a 10.5.3.3, exclusivamente em seu nome, expedidos por pessoa jurídica de direito público ou privado, composto pela prestação de serviços SOC (Blue e Red Team) com coleta e análise de correlacionamento de informações de segurança e gestão de eventos (*Security Information and Event Management* - SIEM) em ambientes com as seguintes características:

10.5.3.1. A execução de serviços por no mínimo de 12 (doze) meses ininterruptos de serviços compostos por *Blue Team*, *Red Team* e Monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM.

10.5.3.2. No mínimo 500 (quinhentos) eventos por segundo (EPS) na ferramenta

SIEM.

10.5.3.3. Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 100 (cem) ativos e 1.000 (mil) usuários.

10.5.4. A LICITANTE disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados.

10.5.5. Caso a LICITANTE não comprove as exigências previstas neste Termo de Referência por meio das documentações requeridas, será desclassificada.

10.5.6. O atestado deverá conter:

10.5.6.1. Razão Social, CNPJ e Endereço Completo da Empresa ou Órgão Emitente.

10.5.6.2. Razão Social da Contratada.

10.5.6.3. Número e vigência do contrato.

10.5.6.4. Objeto do contrato.

10.5.6.5. Local e Data de Emissão.

10.5.6.6. Assinatura do responsável pela emissão do atestado.

10.5.7. Tratando-se de empresa ou sociedade estrangeira em funcionamento no país, deve possuir Decreto de Autorização e Ato de Registro, ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

10.5.8. A não comprovação de alguma característica exigida, quando solicitada pelo Contratante, levará à desclassificação da proposta.

10.5.9. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da LICITANTE. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

10.5.10. O TJCE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas no Termo de Referência, podendo buscar por meios próprios ou exigir a apresentação de documentação complementar, tais como Notas Fiscais, Contratos, Atas do Pregão Original, entre outros, referente à prestação de serviços relativos aos atestados apresentados

10.5.11. É permitido o agrupamento de atestados de capacidade técnico-operacional, a fim de comprovar a experiência na prestação de serviços com características técnicas semelhantes ao objeto desta contratação.

10.5.12. É possível aceitar a apresentação de atestados de serviços executados simultaneamente como comprovação do quantitativo mínimo do serviço, uma vez que essa situação é equivalente, em termos de comprovação da capacidade técnico-operacional, a uma única contratação.

10.5.13. Os atestados devem estar relacionados a serviços realizados no contexto de sua atividade econômica principal ou secundária, conforme descrito no contrato social atualizado.

10.5.14. A comprovação de capacidade técnica estará sujeita à confirmação da veracidade de suas informações através de possíveis diligências, conforme prescreve o art. 59, § 2º, da Lei 14.133/21.

10.5.15. Por fim, caso a empresa esteja sob falência, concurso de credores, dissolução ou liquidação, deve apresentar Plano de Recuperação Judicial, devidamente homologado. Se nessas condições e, ainda, sendo formada em consórcio de empresas, esta não deverá ser controladora, coligada ou subsidiária entre si, devendo, da mesma forma, apresentar Plano de Recuperação Judicial, devidamente homologado.

11. GARANTIA CONTRATUAL

11.1. A CONTRATADA deverá entregar ao Gerente de Contratação do objeto, que submeterá à Coordenadoria Central de Contratos e Convênios do TJCE, no prazo prescrito no art. 96 da Lei n.º 14.133/2021, a título de garantia, a quantia equivalente a 5% (cinco por cento) do valor global da contratação, cabendo-lhe optar dentre as modalidades previstas no art. 96, Lei n.º 14.133/2021.

11.1.1. A garantia será devolvida à CONTRATADA somente depois do cumprimento integral das obrigações assumidas, inclusive recolhimento de multas e satisfação de prejuízos causados ao CONTRATANTE.

11.1.2. Será exigida do licitante vencedor a indicação na sua proposta a modalidade da garantia escolhida, a fim de possibilitar a contagem do prazo de acordo com cada modalidade.

11.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

11.2.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas.

11.2.2. As multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA.

11.2.3. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

11.3. A contratada terá o prazo mínimo de 1 (um) mês, contando do recebimento do termo de

intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pela modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

11.3.1. A apólice deverá seguir as regras estatuídas na Circular Susep nº 662, de 11 de abril de 2022, quando da escolha por parte do licitante vencedor da modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

11.3.2. O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas, conforme inciso II do artigo 97 da Lei Nº 14.133/21.

11.3.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados neste documento, observada a legislação que rege a matéria.

11.4. A contratada terá o prazo mínimo de 10 (dez) dias corridos, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pelas demais modalidades previstas no § 1º do art. 96, da Lei Nº 14.133/21.

11.4.1. A garantia em dinheiro deverá ser efetuada em instituição bancária indicada pelo CONTRATANTE, com correção monetária, em favor do CONTRATANTE.

11.4.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

11.4.3. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.5. A garantia deverá ter validade durante a execução do contrato de 90 (noventa) dias após término da vigência contratual, devendo acompanhar as modificações referentes ao valor e à vigência desta mediante a complementação da caução ou emissão do respectivo endosso pela seguradora ou instituição bancária fiadora.

11.5.1. O prazo para complementação da caução ou emissão do endosso da garantia referente aos aditivos contratuais deverá seguir os mesmos prazos estabelecidos nos subitens 11.3 e 11.4.

11.6. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento de multas, ela deve ser complementada no prazo de até 10 (dez) dias úteis, contados da solicitação do CONTRATANTE, a partir do qual se observará o disposto abaixo:

11.6.1. A não complementação ou renovação, tempestiva, da garantia do contrato ensejará a suspensão de pagamentos até a regularização do respectivo documento, independentemente da aplicação das sanções contratuais.

11.6.2. A inobservância do prazo fixado para apresentação, complementação ou renovação da garantia acarretará a aplicação das sanções previstas neste Termo de Referência.

11.7. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

11.8. A garantia será considerada extinta:

11.8.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro ou títulos da dívida pública, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

11.8.2. No prazo de 90 (noventa) após o término da vigência, caso o CONTRATANTE não comunique a ocorrência de sinistros.

11.9. A ausência de prestação da garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa e rescisão unilateral do contrato administrativo.

12. VIGÊNCIA CONTRATUAL

12.1. A vigência do contrato inicia na data de sua assinatura vigorará por até 36 (trinta e seis) meses, podendo ser prorrogado até limite permitido pela Lei 14.133/21.

12.2. A escolha do prazo de 36 (trinta e seis) meses de vigência baseia-se não somente no investimento, mas também na continuidade e no desempenho de funções de segurança da informação do TJCE, agregado à possibilidade de renovação dos itens de serviço, até o limite permitido pela atual legislação, desde que se comprove vantajoso ao TJCE.

12.3. Além disso, no custo administrativo de um processo licitatório, já que quanto maior o número de procedimentos, maior o gasto da administração, considerando contratações de serviços continuados, como o que aqui se trata.

12.4. O prazo dilatado permitirá obtenção de ganho de escala, reduzindo o grau de incerteza da contratação e consequentemente melhores preços para a Administração.

12.5. Ademais, é maior a atratividade do certame pelo mercado, por meio de uma maior diluição dos custos dos serviços oferecidos pela contratada durante o lapso temporal do contrato, favorecendo a Administração em termos de economicidade e ampliação da competitividade.

12.6. Como também está alinhada ao padrão praticado no mercado, como pode ser verificado nas contratações públicas similares (disponível no item 2.6.2).

12.7. Por se tratar de um objeto de execução crítica e de tamanha importância para o judiciário cearense, como também foi definida acima, a importância da solução a ser adquirida, vemos também, a importância e quão crítica é a perfeita execução do objeto e a relevância de uma

manutenção e suporte contínuo. Garantindo qualidade e eficiência no funcionamento da Solução, bem como a facilidade e eficiência na gestão do contrato para a Administração.

12.8. A contratação em tela envolve serviços de natureza continuada, necessários à conservação do futuro patrimônio público, objeto desta contratação acima descrito, e ao bom andamento das atividades judiciárias e administrativas desenvolvidas pelo Poder Judiciário Cearense e, consequentemente, para toda a sociedade de modo geral.

12.9. Os serviços relacionados à manutenção integral de todos os componentes da solução e seu funcionamento é que vinculam-se à indispensável continuidade da sua prestação, pois os referidos serviços objetivam à manutenção profissional, eficiente, competente, capacitada e confiante da infraestrutura de processamento de dados, logrando evitar transtornos relacionados à solução de continuidade na prestação do objeto contratual. Além dessa essencialidade do serviço em pleno funcionamento, a ideia de manter a solução sob constante cuidado operacional e funcionando ininterruptamente (habitualidade), relaciona-se com a necessidade monitorar e responder a incidentes cibernéticos, possibilitando, assim, condições adequadas ao exercício das atividades-fim da Corte de Justiça do Estado do Ceará, de seus servidores, dos colaboradores e demais jurisdicionados.

12.10. A caracterização de um serviço como contínuo requer a demonstração de sua essencialidade e habitualidade para o contratante, conforme explicação supra. Sabe-se que a essencialidade se atrela à necessidade de existência e manutenção do contrato, pelo fato de eventual paralisação da atividade contratada implicar em prejuízo ao exercício das atividades da Administração contratante, condição integramente esclarecida no item anterior. Já a habitualidade ficou configurada pela necessidade desta atividade ser prestada mediante contratação de terceiros de modo permanente, ou seja, estendendo-se por mais de um exercício financeiro de forma contínua.

12.11. Atenta-se, nesse sentido, ao entendimento da Corte de Contas da União, quando em seu Acórdão n° 132/2008, da Segunda Câmara, sob relatoria do Ministro Aroldo Cedraz, prescreve que contratos dessa natureza intentam “manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional”.

12.12. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, suporte e garantia inerentes a solução a ser adquirida, sobretudo os utilizados pelo TJCE, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos.

12.13. Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, de suporte e de garantia, inerentes à solução a ser adquirida, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual, em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos, e a imperiosidade da sua prestação ininterrupta em face do desenvolvimento habitual das atividades administrativas, sob pena de prejuízo ao interesse público, denota-se necessária a contratação pelo tempo indicado, conforme descrito neste documento.

12.14. Diante do exposto, considera-se de extrema relevância para a Administração a contratação do objeto em tela, entendendo imprescindível a vigência do termo de contrato por até 36 (trinta e seis) meses, contados da data de emissão do Termo de Recebimento Definitivo.

Equipe de Planejamento da Contratação

Max Eduardo Vizcarra Melgar - 48994 Integrante Técnico	**Fábio de Carvalho Leite – 9594** Integrante Administrativo	**Heldir Sampaio Silva - 9630** Integrante Demandante

Cristiano Henrique Lima de Carvalho – 5198
Área Demandante

13. APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Licitação para iniciação de procedimento licitatório, segundo o art. 38 da Lei nº 8.666 de 21 de junho de 1993.

Autoridade Competente

Denise Maria Norões Olsen – 24667
Área de Tecnologia da Informação

Fortaleza, 26 de setembro de 2023.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

TRF ANEXO I

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

Os serviços gerenciados de segurança da informação serão compostos pelos serviços mostrados na seguinte Tabela.

Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação

LOTE	SERVIÇO	DESCRIÇÃO DO SERVIÇO	QTD
1	1	**Serviço de gestão de incidentes de segurança (Blue Team), por 36 meses.**	1
	2	**Serviço de gestão testes de invasão (Red Team), por 36 meses.**	1
	3	**Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS por 36 meses.**	1
	4	**Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses.**	10
	5	**Serviço de contratação de pacotes de 1.000 EPS da ferramenta SIEM por 12 meses.**	10
	6	**Serviço de contratação de pacotes de 2.000 EPS da ferramenta SIEM por 12 meses.**	10

1. REQUISITOS OPERACIONAIS MÍNIMOS DO SOC

1.1. O Security Operations Center (SOC) é uma unidade essencial para a segurança da informação, composta por diferentes equipes especializadas. O Blue Team é responsável pela defesa e monitoramento contínuo dos sistemas e redes, detectando e respondendo a incidentes de segurança. O Red Team realiza testes de penetração e simula ataques para identificar vulnerabilidades e pontos fracos, fortalecendo as defesas. O serviço de monitoramento e correlação de eventos, com o uso de uma ferramenta SIEM, coleta e analisa dados de segurança em tempo real, detectando padrões suspeitos e atividades maliciosas. Essa combinação de Blue Team, Red Team e serviço de monitoramento e

correlação de eventos permite uma abordagem abrangente de segurança, fortalecendo a postura de defesa, antecipando e respondendo a ameaças, e garantindo a proteção dos ativos de um órgão ou organização.

1.2. O Blue Team comandará as operações no SOC. O SOC deve ser composto por profissionais de segurança da informação altamente qualificados para desempenhar várias funções cruciais e garantir a proteção e integridade dos recursos computacionais do TJCE.

1.3. A prestação de todos os serviços descritos neste Anexo deve ser realizada conforme:

1.3.1. Horário de expediente regular: Durante os dias úteis e de segunda a sexta-feira, com carga horária diária de 8h, entre 7h e 19h de acordo a definição do TJCE e de forma remota, com exceção da presencialidade do Red Team para atividades de testes de intrusão envolvendo acesso físico à rede ou segurança física (sob demanda do TJCE e com antecedência mínima de 30 dias corridos). Neste horário, a CONTRATADA deverá prestar serviços com no mínimo 1 (um) profissional por perfil (ver Tabela 2. Força de Trabalho Orientativa). Não haverá expediente forense nos feriados nacionais, estaduais e municipais, bem como nas datas determinadas pela Presidência do Tribunal de Justiça, formalizadas através de portaria publicada no Diário da Justiça Eletrônico. O recesso natalino compreendido entre os dias 20 de dezembro e 06 de janeiro deverá ser considerado como dia útil para prestação dos serviços, mesmo não ocorrendo o expediente forense.

1.3.2. Horário de plantão contínuo: Deverá estar disponível em regime de plantão contínuo e fora do horário de expediente regular, 24 horas por dia, 7 dias por semana e durante todos os 365 dias do ano de forma remota, no mínimo 1 (um) profissional da equipe do Blue Team e 1 (um) profissional da equipe Serviço de monitoramento e correlação de eventos (ver Tabela 2. Força de Trabalho Orientativa) para lidar com solicitações de serviços relacionados a incidentes ou desastres de sistemas críticos e tratamento de incidentes no ambiente computacional do TJCE.

1.3.3. Todos os profissionais devem obrigatoriamente compor o quadro de colaboradores

da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

1.3.4. Será adotado um método de trabalho fundamentado no princípio de delegação de responsabilidade para a execução dos serviços. Esse princípio estabelece que o TJCE será responsável pela gestão do contrato e pela verificação do cumprimento dos padrões de qualidade exigidos para os serviços entregues, enquanto a CONTRATADA será responsável pela execução dos serviços e pela gestão dos profissionais sob sua responsabilidade.

1.3.5. A CONTRATADA terá a responsabilidade de executar os serviços e realizar um acompanhamento diário para garantir a qualidade e o cumprimento dos níveis de serviço estabelecidos. Caso surjam problemas que possam prejudicar a eficiência dos serviços ou a alcançar os níveis de serviço acordados, essas questões devem ser prontamente comunicadas por escrito ao TJCE, a fim de tomar as medidas necessárias para ajustes e correções.

1.3.6. A CONTRATADA deve ser responsável por fornecer ao(s) integrante(s) do Blue/Red Team e do Serviço de monitoramento e correlação de eventos, as devidas ferramentas computacionais de trabalho no ambiente remoto ou presencial pré-agendado (Red Team): computador/laptop, servidores, telas de monitoramento, periféricos computacionais, hardware e software licenciado, assim como demais ativos computacionais necessários.

1.3.7. Para garantir a segregação adequada de funções e promover a efetividade das equipes envolvidas, fica estabelecido que os integrantes de cada equipe, ou seja, do Blue Team, Red Team e Serviços de monitoramento e correlação de eventos, não poderão exercer atividades simultaneamente em mais de um perfil (ver Tabela 2. Força de Trabalho Orientativa). Cada profissional deve ser alocado exclusivamente em um perfil, com responsabilidades específicas e atribuições relacionadas à sua respectiva função. É de responsabilidade da contratada garantir o cumprimento desta exigência, assegurando que nenhum integrante atue em mais de um perfil ou

equipe. Este requisito tem como objetivo principal fortalecer a especialização de cada perfil por equipe, garantindo o adequado desempenho das atividades e a maximização dos resultados alcançados no âmbito do SOC.

1.3.8. Com o objetivo de aprimorar a precisão das informações de suporte para a elaboração das propostas, foi disponibilizado um quadro que apresenta a Força de Trabalho Orientativa para os perfis profissionais que serão alocados no TJCE, com suas respectivas quantidades. Vale ressaltar que o dimensionamento da força de trabalho por perfil é de total responsabilidade da empresa contratada:

Tabela 2. Força de Trabalho Orientativa

Perfil	Quantidade Mínima de Profissionais por Equipe	Equipe
Especialista em Segurança	1	Blue Team
Analista de Segurança Pleno	1	Blue Team
Analista de Segurança Sênior	1	Red Team
Analista de Segurança Pleno	1	Serviço de monitoramento e correlação de eventos

1.3.9. Considerando que a prestação do serviço é baseada em níveis mínimos de serviço, a Tabela 2. Força de Trabalho Orientativa é informativa. O quantitativo apresentado foi baseado na força de trabalho prevista que tem como escopo os serviços de gestão dos ativos de rede que fazem parte do parque tecnológico de segurança da informação do TJCE, conforme mostrado na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE.

1.4. A CONTRATADA é responsável por manter as licenças de software proprietário, que serão usados nos serviços mostrados nos itens 2, 3 e 4, ativas e válidas, devendo apresentar ao TJCE uma cópia autenticada dessas licenças anualmente.

1.5. A CONTRATADA é responsável pelo correto funcionamento dos equipamentos usados por ela para a prestação dos serviços mostrados nos itens 2, 3 e 4, sem custos adicionais para o TJCE.

1.6. A CONTRATADA deverá realizar todas suas atividades com o suporte de ferramenta de

Gerenciamento de Serviços de TI (ITSM) do TJCE, a fim de permitir o acompanhamento do histórico do ciclo de vida dos chamados (registro, análise, intervenções e encerramento) abertos pela CONTRATADA e a equipe de segurança da informação do TJCE. A CONTRATADA contará com o devido treinamento da ferramenta de ITSM imediatamente após o início da execução dos serviços e antes dos 30 dias iniciais após assinatura do TRD de implantação.

1.7. Frameworks referenciais: a execução dos serviços prestados, principalmente o processo de resposta a incidentes e testes de invasão ou penetração, devem seguir as boas práticas dos seguintes frameworks: MITRE ATT&CK, NIST, SANS, OSSTMM 3, ISSAF/PTF, ISO 27000 e OWASP.

2. SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA (BLUE TEAM)

2.1. O Blue Team desempenhará um papel fundamental na identificação, investigação e mitigação de incidentes, visando garantir a integridade e disponibilidade dos sistemas de informação. As atividades do Blue Team serão medidas por Níveis Mínimos de Serviço (NMS) e são apresentadas nos itens 2.1 e 2.3.

2.2. Monitoramento de segurança: Os membros do Blue Team devem monitorar continuamente os eventos e incidentes produzidos pelos ativos de redes, sistemas e aplicativos do TJCE (mostrados na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE) em busca de atividades suspeitas. Isso envolve o tratamento de dados gerados pelos Serviços gerenciados de monitoramento e correlação de eventos (SIEM), na sua interação com as ferramentas de segurança já implementadas ou que serão implementadas no TJCE, com o objetivo de identificar eventos ou incidentes de segurança da informação. No entanto, as atividades ou responsabilidades do Blue Team não incluem a administração ou configuração das ferramentas de segurança da informação:

2.2.1. Serviço de Next Generation Firewall (hardware, software e licenças fornecidos pelo TJCE).

2.2.2. Serviço de Web Application Firewall (hardware, software e licenças fornecidos pelo TJCE).

2.2.3. Serviço de VPN – Redes Privadas Virtuais (hardware, software e licenças fornecidos pelo TJCE).

2.2.4. Serviço de Antivírus Corporativo – EDR (software e licenças fornecidos pelo TJCE).

2.2.5. Gestor de Vulnerabilidades (software e licenças fornecidos pelo TJCE).

2.2.6. Ferramenta de Multifactor Authentication - MFA (software e licenças fornecidos pelo TJCE).

2.2.7. Ferramentas, exclusivamente de segurança da informação, a serem implantadas no TJCE.

2.3. Detecção e resposta a incidentes: ao identificar atividades maliciosas ou intrusões, os membros do Blue Team tomam medidas imediatas para responder a esses incidentes. Eles

devem analisar e investigar as ameaças, identificar a origem, determinar o escopo do incidente, diagnosticar remediações e acompanhar a aplicação de contramedidas para mitigar os riscos e minimizar o impacto dos ataques.

2.3.1. Análise de segurança: os membros do Blue Team devem analisar regularmente as informações de segurança coletadas de várias fontes, como logs de eventos, alertas de segurança e inteligência de ameaças. Eles devem correlacionar dados e realizar análises para identificar padrões, tendências e indicadores de comprometimento, ajudando a antecipar e prevenir futuros ataques.

2.3.2. Análise de ameaças: uma vez que uma atividade suspeita é identificada, os membros do Blue Team devem conduzir uma análise de ameaças para determinar a natureza e a gravidade da ameaça. Isso envolve a análise de indicadores de comprometimento (IOCs), como endereços IP, nomes de domínio, logs de eventos, registros de rede e arquivos maliciosos. A CONTRATADA deverá centralizar as ações de correção de segurança na ferramenta SIEM para classificação de prioridade de incidentes e gerenciamento de vulnerabilidades e riscos, usando integração nativa e centralizada com a ferramenta Tenable.

2.3.3. Gerenciamento de vulnerabilidades: será responsabilidade do Blue Team realizar avaliações regulares de vulnerabilidades nos sistemas do TJCE e recomendar as medidas necessárias para mitigar essas vulnerabilidades. Eles também devem acompanhar as atualizações de segurança, patches e correções fornecidas pelos fornecedores de software e hardware, assim como demandar e supervisionar que essas atualizações sejam implementadas.

2.3.4. Coleta de inteligência de ameaças: Os membros do Blue Team devem monitorar ativamente as informações e inteligência de ameaças provenientes de várias fontes, como comunidades de segurança, fornecedores de segurança e agências de inteligência. Esses dados ajudam a identificar novas tendências de ameaças, táticas e técnicas utilizadas pelos atacantes, permitindo que o SOC esteja preparado e atualizado para enfrentar essas ameaças.

2.3.5. Desenvolvimento de políticas de segurança: os membros do Blue Team devem ser

responsáveis por avaliar, modificar e desenvolver políticas, normas e procedimentos de segurança (existentes ou novos) que ajudem a proteger os sistemas e a infraestrutura do TJCE. Isso deve incluir a definição de requisitos de segurança para novos projetos, a aplicação de controles de acesso e a criação de políticas de senhas.

2.3.6. Monitoramento de conformidade: o Blue Team é responsável por demandar que as políticas, padrões e regulamentações de segurança sejam seguidos dentro do TJCE. O Blue Team deve monitorar e relatar violações de conformidade, demandar a aplicação de medidas corretivas e conferir que os sistemas e processos estejam alinhados com as diretrizes de segurança do TJCE.

2.3.7. Auditorias de Segurança Internas: avaliação sistemática das políticas, normas, procedimentos e controles de segurança existentes, por meio de revisões de controles, verificação da conformidade, identificação de lacunas e elaboração de relatórios detalhados com recomendações para melhoria e planos de ação corretiva.

2.3.8. Auditorias de segurança externas: avaliar a postura de segurança do TJCE, definindo escopo, gerenciando o processo de auditoria, revisando relatórios, implementando recomendações e acompanhando o progresso das ações corretivas, visando garantir a conformidade, identificar vulnerabilidades e fortalecer as medidas de segurança.

2.3.9. Avaliação de riscos: avaliar os riscos associados às vulnerabilidades identificadas durante os testes de penetração (ver item 3). Classificar as vulnerabilidades com base em sua gravidade, impacto potencial e probabilidade de exploração, fornecendo informações importantes para a priorização de ações corretivas.

2.3.10. Recomendações de segurança: com base nos resultados das avaliações de segurança, devem ser fornecidas recomendações detalhadas para fortalecer as defesas do TJCE com indicações de atualizações de software, configurações de segurança, políticas e práticas recomendadas para mitigar as vulnerabilidades identificadas. A CONTRATADA abrirá as Requisições de Serviço contendo as recomendações de correções, acompanhará e validará a execução das

recomendações, as quais serão executadas pela equipe do TJCE.

2.3.11. Colaborar com a equipe de Red Team e outras equipes de segurança para identificar pontos fracos, testar a eficácia das medidas de segurança e recomendar melhorias.

2.3.12. Treinamento: a contratada deverá, a cada 2 meses, realizar apresentação remota via Microsoft Teams do próprio TJCE, para os servidores do TJCE sobre conscientização em Segurança da Informação com duração mínima de 1 hora. Previamente deverá apresentar o plano da apresentação (roteiro do treinamento e material didático utilizado) para aprovação pela equipe de segurança do TJCE. A divulgação, agendamento e emissão dos certificados de participação ficará a cargo do TJCE/SETIN/Assessoria de Comunicação. O TJCE realizará a gravação do treinamento e a CONTRATADA deverá concordar na cessão de direitos de uso de material didático, assim como da voz, imagem e vídeo do instrutor e do material didático apresentado.

2.3.13. Resposta a incidentes: em caso de incidentes de segurança de níveis médios ou grave, ou emergências cibernéticas, os membros do Blue Team devem atuar como parte principal integrante da equipe de resposta a incidentes. Isso envolve o diagnóstico do incidente e a demanda de contramedidas imediatas para conter a propagação de ataques, isolamento de sistemas afetados, remoção de malware, restauração de backups e outras ações para mitigar os danos causados pelo incidente. O Blue Team deve coordenar e colaborar com outras equipes envolvidas na resposta, como a equipe de TI, a equipe de comunicações e outras partes interessadas, para restaurar a segurança e a normalidade das operações governamentais. Os seguintes processos de resposta a incidentes, ou variações em função de Frameworks de segurança da informação, devem ser seguidos:

2.3.13.1 O processo de resposta a incidentes de segurança será iniciado sempre que um evento adverso for relatado pelo Serviço Gerenciado de Monitoramento e Correlação de Eventos (conforme descrito neste Anexo), mas não se limitando exclusivamente a ele.

2.3.13.2 Após a abertura do incidente de segurança, cabe ao Blue Team, com o apoio de outros profissionais de TI do TJCE, analisar os logs e artefatos enviados, visando identificar inicialmente as fontes responsáveis pela geração desses logs.

2.3.13.3 Após a realização das análises iniciais do incidente, o Blue Team deverá empenhar-se na identificação dos principais vetores de ataque que comprometeram o ambiente do TJCE.

2.3.13.4 Como próximo passo, o Blue Team deverá informar ao time de segurança da informação do TJCE, seguindo os Níveis Mínimos de Serviços descritos neste documento, as informações preliminares sobre o incidente de segurança ocorrido, juntamente com as estratégias e abordagens planejadas para resolver o incidente. O Blue Team deve fornecer dados e informações mínimas esperadas, conforme especificado a seguir:

2.3.13.4.1 Prioridade: o incidente será representado por um número que indicará sua prioridade ou severidade, em uma escala de 1 a 4, sendo 1 a prioridade mais alta.

2.3.13.4.2 Classificação: deverá ser atribuída uma única palavra que classifique o tipo do incidente, como malware, phishing, misconfiguration, entre outros.

2.3.13.4.3 Fonte do incidente: devem ser fornecidos os detalhes dos nomes dos dispositivos, endereços de e-mail, endereços IP, detalhes da vulnerabilidade ou outros elementos de identificação que indiquem a origem do incidente.

2.3.13.4.4 Destino do incidente: Deve ser fornecidos os detalhes dos nomes dos dispositivos, endereços de e-mail, endereços IP ou outros elementos de identificação que indicam os ativos afetados.

2.3.13.4.5 Ações recomendadas: devem ser fornecidas instruções

inteligentes e de fácil compreensão, que detalhem as ações de remediação já realizadas pelo Blue Team, assim como as ações que o TJCE deve tomar.

2.3.13.4.6 Fontes da Detecção: devem ser fornecidos os detalhes das fontes dos logs ou dos dispositivos de segurança que identificaram (ou colaboraram na identificação) do incidente. Essa informação será útil para análise da causa raiz ou para a implementação de medidas de remediação direcionadas.

2.3.13.5 Em conjunto com o TJCE, o Blue Team será responsável por determinar a severidade do incidente de segurança. A severidade do incidente de segurança da informação será estabelecida levando em consideração a combinação de urgência e impacto, sendo que o impacto representa a crítica do incidente em relação aos aspectos do negócio, e a urgência refere-se à velocidade necessária para sua resolução.

2.3.13.6 Após as análises iniciais do incidente, será responsabilidade do Blue Team realizar uma análise mais aprofundada, levando em consideração o comportamento do ataque e/ou artefato (por exemplo: malware).

2.3.13.7 Após a identificação do comportamento e dos principais vetores de ataque, o Blue Team deverá elaborar uma estratégia para a mitigação e contenção do ataque em questão. No caso de ser necessário realizar alterações no ambiente computacional do TJCE para conter e mitigar o incidente, tais alterações devem ser autorizadas previamente e implementadas pelo corpo técnico de segurança do TJCE. Após a obtenção da autorização, a equipe de segurança do TJCE poderá implementar as alterações necessárias.

2.3.13.8 Após a mitigação do incidente de segurança, o próximo passo exigido é que o Blue Team inicie o processo de coleta de todas as evidências

relevantes e identifique os serviços afetados. Essas evidências serão utilizadas ao longo do processo, visando a realização da análise forense do caso.

2.3.13.9 O processo de restauração dos serviços e soluções afetadas será acompanhado pelo Blue Team e será realizado pela equipe de segurança da informação e de tecnologia da informação do TJCE.

2.3.13.10 O Blue Team deve consolidar os dados coletados durante o processo de tratamento do incidente, a fim de iniciar a análise forense correspondente. Essa análise tem como objetivo identificar pessoas, locais e/ou eventos relevantes, correlacionando todas as informações coletadas e gerando um laudo final sobre o incidente de segurança em questão.

2.3.13.11 O Blue Team é responsável por conduzir a reconstrução dos ataques em todos os incidentes que resultaram em invasão ou vazamento, ou quando considerado necessário, em um ambiente controlado, como sandbox em servidores físicos, máquinas virtuais, ferramentas em nuvem ou outros ambientes computacionais. Esse ambiente deve ser implementado, controlado e de propriedade da CONTRATADA.

2.3.13.12 É incumbência do Blue Team documentar as lições aprendidas do incidente de segurança em questão, ao longo de todo o período de vigência do contrato, com o intuito de construir uma extensa base de conhecimento sobre ataques adversos.

2.3.13.13 O processo descrito é o mínimo esperado a ser seguido e executado pelo Blue Team, no entanto, devido ao caráter contínuo do serviço estabelecido neste Anexo, espera-se que o Blue Team busque constantemente melhorias, as quais podem ser implementadas mediante aprovação do TJCE.

2.4. Perfil do BlueTeam.

2.4.1. Todos os profissionais do Blue Team devem possuir graduação em cursos de

tecnologia da informação e contar com experiência comprovada (CTPS ou contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 18 meses.

2.4.2. Perfil do Especialista em Segurança - Coordenador do SOC.

2.4.2.1 Será o responsável por gerenciar os profissionais do Blue Team, Red Team e do Serviço de monitoramento e correlação de eventos.

2.4.2.2 Será líder e parte da equipe Blue Team (ver Tabela 2. Força de Trabalho Orientativa).

2.4.2.3 Deve contar com a certificação Certified Information Systems Security Professional (CISSP).

2.4.2.4 Deve contar, ou obter em no máximo 6 meses após a contratação, com pelo menos, uma das seguintes certificações: Certified Information Systems Auditor (CISA); Certified Information Security Manager (CISM); GIAC Security Essentials Certification (GSEC); Certified Incident Handler (GCIH); CompTIA CySA+.

2.4.3. Perfil do Analista de Segurança Pleno - Blue Team.

2.4.3.1 Deve contar com, pelo menos, uma das seguintes certificações: Certified Information Systems Auditor (CISA); Certified Incident Handler (GCIH); CompTIA CySA+.

3. SERVIÇO DE GESTÃO TESTES DE INVASÃO (RED TEAM)

3.1. O Red Team será responsável por conduzir avaliações de segurança e testes de penetração, internos e externos, nos sistemas, aplicativos e infraestrutura do TJCE, com o objetivo de identificar vulnerabilidades e avaliar a eficácia das medidas de segurança implementadas.

3.2. O Red Team trabalhará em estreita colaboração com a equipe de segurança da informação, fornecendo *insights* e recomendações para melhorar a postura de segurança do órgão.

3.3. Responsabilidades ou atividades do Red Team.

3.3.1. Testes de invasão: realizar testes de penetração simulando ataques cibernéticos para identificar vulnerabilidades nos sistemas, redes e aplicativos do TJCE. Explorar técnicas avançadas de hacking ético para encontrar pontos fracos na segurança e avaliar a eficácia das defesas existentes.

3.3.2. Os alvos dos testes de invasão, assim como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados pela equipe de segurança da informação do TJCE, mediante Requisição de Serviço disponibilizado através da ferramenta de ITSM do TJCE, antes de cada campanha a ser executada.

3.3.3. Qualquer atividade que possa comprometer ou prejudicar um ambiente ou ativo do TJCE deve ser comunicada imediatamente, antes de sua execução, devido à importância de manter a disponibilidade dos ambientes e serviços em funcionamento.

3.3.4. As seguintes ferramentas tecnológicas devem contar com licenciamento e ser disponibilizadas pela CONTRATADA para o uso do Red Team nos testes de invasão, sob demanda das atividades do TJCE para o Red Team (qualquer dúvida ou questionamento de dimensionamento deve ser realizado na Vistoria Técnica):

3.3.4.1 Metasploit Pro.

3.3.4.2 Shodan.

3.3.4.3 Burp Suite Professional.

3.3.4.4 DeHashed.

.

3.3.5. O teste de invasão deverá obedecer às seguintes fases, podendo ser adaptadas conforme os Frameworks existentes na literatura:

3.3.5.1 Planejamento.

3.3.5.1.1 Na fase de planejamento, todas as premissas, processos, atividades e cronogramas descritos e aprovados na Requisição de Serviço serão detalhados e apresentados.

3.3.5.1.2 Serão fornecidas informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser aplicadas ambas, de acordo com a definição do escopo):

3.3.5.1.2.1. Técnica da caixa-preta: envolve ter pouco ou nenhum conhecimento prévio sobre o ambiente a ser avaliado. O especialista em segurança deverá descobrir e explorar o ambiente durante o processo de avaliação.

3.3.5.1.2.2. Técnica da caixa branca: permite que o avaliador tenha acesso irrestrito a todas as informações relevantes para o teste de segurança.

3.3.5.1.2.3. Técnica da caixa cinza ou híbrida: o avaliador tem conhecimento limitado sobre o alvo, ou seja, uma média de informações e recursos disponíveis entre as técnicas de caixa preta e branca.

3.3.5.2 Descoberta

3.3.5.2.1 Deverá ser utilizada, no mínimo, ferramentas de análise de vulnerabilidades, bem como a gestão de vulnerabilidades, além de empregar técnicas manuais de análise de vulnerabilidade. As ferramentas devem ser apresentadas para conhecimento e aprovação prévia antes de sua utilização,

assim como a metodologia empregada na análise manual de vulnerabilidades.

3.3.5.2.2 Durante a fase de Descoberta, os seguintes requisitos devem ser cumpridos e incluídos no "Relatório de Teste de Invasão", quando aplicável:

3.3.5.2.2.1. Coleta passiva, com a utilização de, no mínimo, as seguintes técnicas: Whois e nslookup (consultas DNS) ; Sites de busca; Listas de discussão; Blogs de colaboradores; Dumpster diving ou trashing; Informações livres; Packet sniffing “passive eavesdropping”; Captura de banner.

3.3.5.2.2.2. Coleta ativa, com a utilização de, no mínimo, as seguintes técnicas: Port scanning (Mapeamento de rede); Varredura de vulnerabilidade.

3.3.5.2.2.3. Varredura de vulnerabilidade para identificar: Hosts ativos na rede; Portas e serviços em execução; Serviços ativos e vulneráveis nos hosts; Sistemas operacionais; Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas; Configurações feitas nos hosts sem observância de boas práticas em segurança computacional; Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas; Identificação de vetores de ataque e cenários para exploração; Vulnerabilidades Detectadas (CVE); Vulnerabilidades de Alto Risco;

Vulnerabilidades de Médio Risco; Vulnerabilidades de Baixo Risco; Informações a serem aplicadas na fase de ataques.

3.3.5.2.2.4. Análise de serviços e aplicações web: Uso indevido de sistema de arquivos e arquivos temporários; Evasão de informação por configurações default de tratamento de erros; Tratamento indevido de entrada; Problemas relacionados à má configuração dos serviços; Gerenciamento inseguro de sessões web.

3.3.5.3 Ataque

3.3.5.3.1 Todas as atividades suspeitas de comprometer um ambiente ou ativo devem ser relatadas imediatamente antes de sua execução, levando em consideração a importância de manter a disponibilidade dos ambientes e serviços em funcionamento.

3.3.5.3.2 Deverá ser conduzido um teste de vulnerabilidades e invasão em endereços IPs, URLs, aplicações ou outros ativos especificados do ambiente computacional, incluindo servidores, bancos de dados, ativos de rede, equipamentos de segurança e outros dispositivos relevantes para o teste de invasão.

3.3.5.3.3 Deverão ser aplicados, no mínimo, os seguintes tipos de ataques: Violações do protocolo HTTP; SQL Injection; LDAP Injection; Cookie Tampering; CrossSite; Scripting (XSS); Directory Transversal; Buffer Overflow; OS Command Execution; Command Injection;nRemote Code Inclusion; Server Side Includes (SSI) Injection; File disclosure; Information Leak; Zero day attacks; DDos

(Distribuited Denial of Service); Dos (Denial of Service); Contra protocolo TCP; Ataques contra a aplicação e OWASP Top 10.

3.3.5.3.4 Os ataques de negação de serviço, tanto no protocolo TCP quanto no nível de aplicação, devem utilizar/demonstrar/explorar, no mínimo, as seguintes técnicas específicas: Bugs em serviços, aplicativos e sistemas operacionais; SYN flooding; Fragmentação de pacotes de IP (Smurf e fraggle, Teardrop, nuke e land); Ataques contra o protocolo TCP (Sequestro de conexões; Prognóstico de número de sequência do protocolo TCP; Ataque de Mitnick; Source routing).

3.3.5.3.5 Ataques em nível da aplicação: Buffer Overflow; Problemas com o SNMP; Vírus, worms e cavalos de Tróia.

3.3.5.3.6 Ataques de injeção de Código: Ataques XSS (Crosssite Script); Comprometimento do acesso remoto; Manutenção de acesso; Encobrimento de rastros da invasão.

3.3.5.3.7 Para os testes de invasão direcionados aos serviços web, abrangendo tanto a Intranet quanto a Internet, serão considerados e aplicados os seguintes testes com base no OWASP TESTING GUIDE 4.2:

3.3.5.3.7.1. Padrões para testes de gerenciamento de configuração: OWASPCM001, OWASPCM002, OWASPCM003, OWASPCM004, OWASPCM005, OWASPCM006, OWASPCM007, OWASPCM008.

3.3.5.3.7.2. Padrões para testes de autenticação: OWASPAT001, OWASPAT002,

OWASPAT003, OWASPAT004, OWASPAT005, OWASPAT006, OWASPAT007, OWASPAT008, OWASPAT009 e OWASPAT010.

3.3.5.3.7.3. Padrões para testes de gerenciamento de sessão: OWASPSM001, OWASPSM001, OWASPSM002, OWASPSM003, OWASPSM004, OWASPSM005.

3.3.5.3.7.4. Padrões para testes de autorização: OWASPAZ001, OWASPAZ002 e OWASPAZ003.

3.3.5.3.7.5. Padrão para testes de negócio lógico: OWASPBL001.

3.3.5.3.7.6. Padrões para testes de validação de dados: OWASPDV001; OWASPDV002, OWASPDV003, OWASPDV004, OWASPDV005, OWASPDV006, OWASPDV007, OWASPDV008, OWASPDV009, OWASPDV010, OWASPDV011, OWASPDV012, OWASPDV013, OWASPDV014, OWASPDV015 e OWASPDV016.

3.3.5.3.7.7. Padrões para testes de negação de serviços: OWASPDS001, OWASPDS002, OWASPDS003, OWASPDS004, OWASPDS005, OWASPDS006, OWASPDS007 e OWASPDS008.

3.3.5.3.7.8. Padrões para testes de serviços web: OWASPWS001, OWASPWS002,

OWASPWS003, OWASPWS004, OWASPWS005, OWASPWS006 e OWASPWS007.

3.3.5.3.8 Cada teste realizado deve ser acompanhado por relatórios que incluam os seguintes resultados: Referência-base (Whitepaper); Ameaças encontradas; Riscos levantados ao ambiente computacional; Contramedidas para mitigar as ameaças encontradas.

3.3.5.4 Relatório de Teste de Invasão

3.3.5.4.1 Após a conclusão da fase de ataque, será elaborado e entregue à equipe de segurança do TJCE um relatório de Teste de Invasão, abrangendo cada teste realizado e contendo, no mínimo, as seguintes informações: objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão.

3.3.5.4.2 Ao final da fase de ataque, no Relatório de Teste de Invasão, devem ser abordadas e detalhadas, no mínimo, as seguintes informações: Detalhes da infraestrutura descoberta, alvo dos testes de invasão; Equipamentos e recursos demandados para este teste; Tipos de ataque; Prazos (janelas de tempo para execução dos testes); Pontos de contato da CONTRATADA (responsáveis para tratamento de questões

abordadas nos testes); Tipos de testes realizados pelos especialistas em segurança da informação; Confirmação ou refutação de a existência de vulnerabilidades; Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade; Obtenção de acesso e possível escalada de privilégios; Detalhamento da metodologia do ataque; Recomendações para sanar riscos e vulnerabilidades.

3.3.5.4.3 Uma reunião será realizada entre o Red Team e a equipe de segurança do TJCE, na qual o conteúdo completo do Relatório Teste de Invasão será apresentado detalhadamente. Durante a reunião, todas as dúvidas do corpo técnico do TJCE serão esclarecidas.

3.3.5.4.4 Após a entrega do Relatório Teste de Invasão, o Blue Team, em colaboração com a equipe de segurança do TJCE, procederá à análise do documento com o intuito de implementar as recomendações, mitigar os riscos identificados ou, quando necessário, aceitá-los.

3.3.5.4.5 Após a análise e implementação das medidas de remediação, a equipe de segurança do TJCE tem a opção de solicitar ao Red Team a realização de um novo teste de invasão para avaliar os resultados, resultando na emissão de um relatório atualizado.

3.3.5.4.6 O prazo para conclusão de cada Requisição de Serviço, que inclui diagnósticos, análises, avaliações e testes, acompanhado da entrega de todos os relatórios específicos de avaliação de vulnerabilidades dos ambientes mencionados neste Anexo, será determinado individualmente para cada atividade, dividindo-se em:

Atividades do Pentest; Entrega do relatório "Teste de Invasão"; Ações corretivas das vulnerabilidades apontadas pelo Red Team e aplicadas pelo Blue Team; Reavaliação Pentest, caso necessário; Entrega do Relatório Final do Teste de Invasão. Todas as fases dos testes de invasão devem ser detalhadamente documentadas com evidências na ferramenta de ITSM do TJCE.

3.4. Perfil do Analista de Segurança Sênior - Red Team

3.4.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS ou contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 18 meses.

3.4.2. Deve contar com a certificação Certified Ethical Hacker (CEH).

3.4.3. Deve contar, ou obter em no máximo 6 meses após a contratação, com pelo menos, uma das seguintes certificações: GIAC Exploit Researcher and Advanced Penetration Tester (GXPN); Offensive Security Certified Professional (OSCP); EC-Concil Licensed Penetration Tester (LPT); IACRB Certified Expert Penetration Tester (CEPT); CompTIA Pentest+.

4. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

4.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TJCE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em Frameworks de gestão de incidentes (NIST SP 800-61, ISO/IEC 27035 e SANS Incident Handling) e fornecendo como serviço a solução tecnológica *Security Information and Event Management* (SIEM)

4.2. Características gerais da solução SIEM

4.2.1. A CONTRATADA deve fornecer o serviço de coleta, análise e correlação de logs, por meio de uma solução de Gerenciamento de Informações e Eventos de Segurança (SIEM).

4.2.2. A tecnologia de SIEM a ser implantada deve ter sido homologada e utilizada em outras instituições públicas ou privadas, conforme os documentos de qualificação técnica a serem apresentados pela licitante.

4.2.3. Todo hardware e software deve ser fornecido pela CONTRATADA como serviço na vigência do contrato.

4.2.4. A CONTRATADA deverá implantar coletores (virtualizados ou em hardware) no ambiente do TJCE, a fim de realizar a coleta de logs localmente no ambiente do TJCE, absorvendo toda a responsabilidade de implantação dos coletores (Servidores, Máquinas Virtuais, Processamento, Sistema Operacional, etc). O TJCE somente fornecerá energia e link de conexão para o funcionamento da implantação dos coletores.

4.2.5. Para a implantação dos coletores, poderá ser aceito o uso de *Virtual Appliance* da CONTRATADA a ser instalado no ambiente computacional do TJCE, mediante a verificação e aprovação prévias dos requisitos técnicos pela equipe de segurança da informação do TJCE e o atendimento das demais exigências e requisitos

apresentados neste Anexo.

4.2.6. O TJCE fornecerá conectividade, espaço físico em Rack e energia elétrica para o funcionamento do hardware e software da solução SaaS (Software as a Service).

4.2.7. A solução deverá consolidar eventos de log de dispositivos, terminais e aplicativos distribuídos.

4.2.8. A solução deverá correlacionar as informações de diferentes fontes de logs e agregar eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes.

4.2.9. A solução do processamento de dados transmitidos pelos coletores e executada pela ferramenta SIEM deve ser implementada no modelo totalmente SaaS.

4.2.10. A solução deverá ter disponibilidade mensal mínima de 99,7%, conforme Nível Mínimo de Serviço apresentado na Tabela 4. Indicadores de Nível de Serviço.

4.2.11. A solução deve ser flexível a períodos de sazonalidade, permitindo aumento da licença quando necessário e retorno ao volume inicial contratado quando o período de sazonalidade finalizar.

4.2.11.1 A solução deve possibilitar a recepção de eventos que temporariamente ultrapassem os limites contratados. O volume excedente será processado assim que o volume for normalizado, funcionando com picos temporários sem perder eventos ou incorrer em cobranças adicionais por excesso.

4.2.11.2 A cobrança sobre o volume sazonal será realizada conforme o volume de Eventos por Segundo (EPS) tratado.

4.2.12. A solução deverá possibilitar a coleta dos logs *on-premise*, por meio do uso de agentes.

4.2.12.1 Os agentes devem ser capazes de realizar o monitoramento da integridade de arquivos, alertando sobre inclusão, alteração, remoção e leitura de arquivos presentes em equipamentos Windows/Linux monitorados.

4.2.12.2 Os agentes de coleta devem oferecer suporte para a coleta de logs via

Syslog de outras plataformas.

4.2.12.3 Os agentes de coleta devem ser capazes de identificar e separar "relay logs" (servidores Syslog que recebem e repassam logs de várias outras fontes) de forma independente, garantindo uma correlação adequada.

4.2.12.4 A solução deve permitir o monitoramento e envio de alertas relativos a agentes que não estejam funcionando corretamente ou estejam inoperantes.

4.2.12.5 A solução deve operar usando agentes, com exceção dos dispositivos que geram logs usando o protocolo padrão Syslog.

4.2.13. A solução deve disponibilizar o uso da ferramenta *User Behavior Analytics* (UBA) em computadores de usuários determinados pelo TJCE, sem custo adicional e com regras pré-definidas e modificáveis.

4.2.14. Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM.

4.2.15. Quando coletando logs que estão hospedados na nuvem, a coleta deve ocorrer diretamente da nuvem da aplicação para a nuvem do SIEM, sem permitir que os logs passem pela infraestrutura do TJCE. Isso é válido desde que a solução em nuvem permita a coleta por meio de integrações via API. Qualquer questionamento de serviços em nuvem usados pelo TJCE poderão ser esclarecidos na Vistoria Técnica.

4.2.16. A solução deverá segregar logicamente os logs do TJCE dos demais logs de outras contratantes que utilizem a solução de SIEM SaaS na infraestrutura da CONTRATADA.

4.2.17. A solução deve ser monitorada para garantir disponibilidade e infraestrutura em tempo integral, 24 horas por dia, 7 dias por semana, durante todo o ano.

4.2.18. Se a solução consistir em módulos, eles devem ser fornecidos por um único fabricante para garantir suporte completo em relação a funcionalidades, integrações e compatibilidade de 100% com a solução. Como um dos requisitos da ferramenta SIEM para a assinatura do TRD de implantação, a CONTRATADA

deverá apresentar documentação fornecida pelo fabricante para comprovar a cobertura de garantia do fabricante relacionada com a funcionalidade da ferramenta SIEM.

4.2.19. A solução deve armazenar os logs por pelo menos 6 meses online, conforme diretrizes da PORTARIA No 162, DE 10 DE JUNHO DE 2021 do CNJ.

4.2.20. O armazenamento dos logs deve ser efetuado no território brasileiro pela CONTRATADA. Os logs não poderão trafegar por território fora do Brasil.

4.2.21. A coleta, normalização e correlacionamento dos eventos dos dispositivos monitorados devem ocorrer em tempo próximo ao real.

4.2.22. A fim de aprimorar a operação e a compreensão dos eventos, é obrigatório normalizá-los e categorizá-los em um único padrão que será utilizado pela solução.

4.2.23. A solução deve possibilitar a criação de metadados personalizados, permitindo a extração de dados existentes na linha de log (raw). Isso pode ser realizado por meio de recursos como expressões regulares ou interfaces gráficas dedicadas para essa finalidade.

4.2.24. Propriedades customizadas poderão ser utilizadas em regras de correlação online e histórica.

4.2.25. A solução deve possibilitar a agregação de eventos similares.

4.2.26. A solução deve atribuir uma métrica de prioridade tanto para os eventos quanto para os alertas/incidentes.

4.2.27. A solução deve ser capaz de gerar alertas/incidentes com base em regras predefinidas anteriormente.

4.2.28. A solução deve ter a capacidade de armazenar os eventos, incluindo aqueles normalizados, de forma compactada.

4.2.29. A solução deve possibilitar a análise de eventos com base em contexto, como usuários, localização geográfica e qualquer outro metadado presente nos eventos.

4.2.30. A solução deve fornecer painéis gráficos ou integração com painéis gráficos existentes no TJCE (dashboards), que apresentam indicadores de segurança, aplicações e monitoramento do SIEM.

4.2.31. Os painéis gráficos (dashboards) devem ser personalizáveis por usuário, permitindo a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução na interface web.

4.2.32. O Dashboard integrado deve:

4.2.32.1 Fornecer um painel que apresente uma visão consolidada das métricas de segurança dos ativos monitorados.

4.2.32.2 Permitir a personalização do painel, incluindo a adição de relatórios e métricas.

4.2.32.3 Realizar a análise dos eventos de segurança da informação em quase tempo real.

4.2.32.4 Assegurar a funcionalidade de análise por meio do drill-down, possibilitando a exploração detalhada a partir de um gráfico de visão geral, com a capacidade de descer aos diferentes níveis de análise conforme necessário.

4.2.32.5 Permitir o acesso da equipe do TJCE em qualquer momento.

4.2.33. Ter a capacidade de enviar e-mails ou mensagens via SMS contendo notificações sobre incidentes ou alertas.

4.2.34. A solução deve oferecer, no mínimo, os seguintes métodos de coleta de eventos: Syslog (UDP, TCP), Syslog com criptografia TLS, JDBC, SNMP (v1, v2 e v3), Registro de Eventos do Microsoft, Cliente MQ Series, Arquivos de Log em formato de texto, Kafka, Checkpoint OPSEC/LEA, CISCO NSEL e Protocolo Juniper NSM.

4.2.35. A solução deve ser capaz de encaminhar os logs e fluxos, em seu formato nativo, para outros sistemas de segurança da informação ou servidores Linux/Windows em tempo real.

4.2.36. A solução deve ser capaz de encaminhar eventos já normalizados para outros sistemas de correlação em tempo real.

4.2.37. A solução deve oferecer a capacidade de configurar a ofuscação de qualquer parte dos dados recebidos após a normalização. A configuração da ofuscação de dados

deve ser realizada por meio de chaves de criptografia.

4.2.38. A solução deve ser capaz de automatizar a resposta a incidentes, executando scripts como ação personalizada dentro das regras de correlação.

4.2.39. A solução deve permitir a personalização e customização de diversos modelos de e-mail que serão enviados como resposta aos incidentes identificados.

4.2.40. A solução deve ser capaz de processar logs no formato JSON, identificando e criando automaticamente os campos comuns do log como metadados para aquele tipo de log.

4.2.41. A solução deve permitir a criação de metadados com nomes personalizados, à escolha do administrador, e possibilitar a referência desses metadados em pesquisas e regras de correlação.

4.2.42. A solução deve permitir a personalização/definição de metadados para extrair dados de uma linha de log (raw), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, possibilitando o uso desses dados em pesquisas de eventos.

4.3. Características do coletor de logs do SIEM

4.3.1. A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de preferência (network appliance ou virtualização), desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos do TJCE.

4.3.2. Os coletores deverão comunicar-se com o SIEM da CONTRATADA através de VPN com tráfego criptografado.

4.3.3. Deverá possibilitar a compressão/compactação e criptografia dos dados para o envio dos logs à nuvem.

4.3.4. Deverá realizar a filtragem e seleção dos eventos a serem inseridos na solução ou mantidos na base de dados da solução, conforme períodos definidos previamente.

4.3.5. Deverá possibilitar a criação e modificação de políticas de retenção.

4.3.6. Deverá realizar a normalização e categorização dos eventos em um padrão único, que será utilizado pela solução.

4.3.7. Deverá oferecer suporte nativo para o reconhecimento e coleta de pelo menos 250 tipos distintos de fontes de dados.

4.3.8. Deverá processar eventos em formato comprimido (zip, gz, tar.gz) sem exigir descompressão manual.

4.3.9. Deverá realizar a agregação de eventos, exibindo a contagem de ocorrências quando o mesmo evento acontecer dentro de um período curto.

4.3.10. A possibilidade de efetuar a agregação de eventos deve ser configurável, permitindo escolher entre realizar ou não essa operação.

4.3.11. Deverá preservar o evento bruto (raw), juntamente com seus metadados para fins de armazenamento e consultas futuras.

4.3.12. Deverá ter a capacidade de agregar informações de localização geográfica dos endereços IP envolvidos no evento, a fim de utilizá-las na correlação.

4.3.13. Um único componente da solução deve ter a capacidade de coletar, processar e normalizar tanto os eventos de segurança quanto os eventos de negócio (não relacionados à segurança).

4.3.14. Os eventos de segurança e de negócios devem ser normalizados para um único padrão de eventos.

4.3.15. A solução deve oferecer suporte à integração de dispositivos ou logs que não são nativamente suportados.

4.3.16. A integração de logs ou dispositivos deve ser feita através da interface web, utilizando expressões regulares, JSON e recursos similares, sem definir de maneira obrigatória a utilização de linguagens de programação ou scripts, como Java, C, TCL/TK, PowerShell, Shell Scripts, entre outros.

4.3.17. A integração mencionada deve ser compatível com as seguintes formas de coleta de eventos:

4.3.17.1 Check Point OPSEC/LEA.

4.3.17.2 Kafka.

4.3.17.3 Arquivos de Log em Formato de texto.

4.3.17.4 Syslog (UDP, TCP).

4.3.17.5 Microsoft Event Log.

4.3.17.6 Juniper NSM Protocol.

4.3.17.7 SNMP (v1, v2 e v3).

4.3.17.8 CISCO NSEL.

4.3.17.9 Syslog criptografado com TLS.

4.3.17.10 PAN-OS XML

4.3.17.11 Common Event Format (CEF)

4.3.17.12 Outros formatos de logs presente nos ativos de rede do TJCE (switches, access point, etc).

4.3.18. A solução precisa ter suporte incorporado para, no mínimo, as seguintes fontes de logs:

4.3.18.1 Windows.

4.3.18.2 Linux.

4.3.18.3 IBM/AIX.

4.3.18.4 HP-UX, Solaris.

4.3.18.5 Oracle Database.

4.3.18.6 IBM/DB2.

4.3.18.7 PostgreSQL.

4.3.18.8 MS SQL Server.

4.3.18.9 Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet, Hillstone, Huawei, Palo Alto e SonicWall).

4.3.18.10 Network IPS/IDS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee).

4.3.18.11 Outras fontes de logs de tecnologias presentes na infraestrutura do TJCE.

4.3.19. A solução deve oferecer a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, a partir das opções nativamente suportadas e enviadas via Syslog.

4.3.20. A solução deve ter a capacidade de criar automaticamente data sources com base

na detecção do tipo de fonte de log, incluindo tipos de logs personalizados na solução, quando enviados via Syslog.

4.3.21. A solução deve ter suporte para IP overlap, ou seja, categorizar os eventos de forma que seja possível gerenciar eventos provenientes de fontes de log que estão em redes distintas, mas possuem o mesmo endereço IP.

4.4. Recursos de correlação de logs do SIEM.

4.4.1. Considera-se tempo de processamento "quase real" no receptor, ao processamento instantâneo da informação mais o atraso de tráfego de dados entre o emissor e o receptor.

4.4.2. A solução deve realizar a correlação de eventos provenientes das fontes de logs e flows, resultando na geração de incidentes de segurança.

4.4.3. A solução deve efetuar a correlação dos eventos em tempo quase real.

4.4.4. A solução deve efetuar a correlação dos flows em tempo quase real.

4.4.5. A solução deve oferecer a capacidade de criar regras inexistentes e editar as existentes.

4.4.6. A solução deve permitir a correlação de qualquer informação presente no evento, inclusive dados financeiros ou outras informações que não estejam relacionadas a endereçamento IP, portas, etc.

4.4.7. Oferecer um mínimo de 150 regras incorporadas, permitindo a criação ilimitada de novas regras ou personalização das regras incorporadas:

4.4.7.1 Ataques de força bruta com e sem sucesso.

4.4.7.2 Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis).

4.4.7.3 Infecção de equipamentos por vírus.

4.4.7.4 Comprometimento ou invasão de ativos da rede.

4.4.7.5 Anomalias de Logon: excessivas falhas de logon, logons fora do expediente, logons a partir de endereços IP não usuais.

4.4.7.6 Realização de ações suspeitas por parte de usuários privilegiados.

4.4.7.7 Detecção de padrões em logs observados e não observados.

4.4.7.8 Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade).

4.4.7.9 Bloqueio de contas e password scans.

4.4.7.10 Ataques comuns em aplicações WEB, como XSS e SQL injection.

4.4.7.11 Ataques de negação de serviço (DoS e DDoS).

4.4.7.12 Identificação em tempo real e de maneira automatizada da origem dos eventos de segurança, identificando cidades, estados e países e não somente os endereços IP de origem.

4.4.7.13 Botnets, worms, DDoS e outros zero-day malwares, através do cruzamento dos logs de DNS, DHCP, web proxy e tráfego de rede.

4.4.8. As regras podem variar desde a detecção simples de thresholds até o uso de operadores lógicos comuns para correlacionar eventos distintos, possibilitando:

4.4.8.1 Permitir a utilização de thresholds estáticos ou dinâmicos.

4.4.8.2 Facilitar a execução de scripts automáticos em casos de incidentes.

4.4.8.3 Permitir a configuração de políticas de notificação com base na severidade do incidente, hora do dia e serviço.

4.4.8.4 Integrar a solução com a monitoração de capacidade e desempenho dos ativos gerenciados via SNMP.

4.4.9. A capacidade de autodetecção deve incluir:

4.4.9.1 Oferecer recursos mínimos de busca de eventos, incluindo: busca em tempo real utilizando palavras-chave semelhantes ao Google e consultas estruturadas semelhantes ao SQL, assim como ter a capacidade de converter os resultados da busca em relatórios ou widgets de painel.

4.4.10. A solução deve incluir regras de correlação específicas para regulamentações e conformidades aplicáveis ao TJCE, com suporte mínimo para PCI, ISO 27001 e GDPR ou LGPD.

4.4.11. A solução deve possuir um repositório que ofereça novas regras de correlação especializadas em segurança para atualização e expansão da capacidade de detecção de incidentes, sem custos adicionais.

4.4.12. A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surtos ou ausência de eventos/tráfego, quando comparados a períodos semelhantes (por exemplo, mesmo período do dia, mesmo dia da semana).

4.4.13. A solução deve permitir a criação de regras que identifiquem desvios em qualquer metadado, em relação aos limites preestabelecidos.

4.4.14. A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que ocorrem ao longo do tempo e não foram previstos ou observados anteriormente.

4.4.15. A solução deve integrar-se com ferramentas externas como Nslookup, Whois e Nmap.

4.4.16. A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (watchlist), permitindo também a criação e edição automatizada e manual de listas.

4.4.17. A solução deve ser capaz de correlacionar eventos e fluxos de rede, como NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução.

4.4.18. A solução deve ser capaz de correlacionar eventos provenientes de múltiplas fontes, tipos ou localizações.

4.4.19. A solução deve ter a capacidade de priorizar os eventos e incidentes com base em critérios que incluem, pelo menos, severidade e criticidade/relevância do evento ou incidente. Deve ser possível utilizar uma combinação desses critérios para determinar a prioridade.

4.4.20. Os incidentes devem ser agrupados, no mínimo, de acordo com:

4.4.20.1 Endereço de origem.

4.4.20.2 Endereço de destino.

4.4.20.3 Categoria.

4.4.21. A solução deve ter, no mínimo, os seguintes tipos de correlação:

4.4.21.1 Extrapolação de um limite (threshold).

4.4.21.2 Correlação por anomalia e padrão de comportamento.

4.4.21.3 Correlação por regras.

4.4.22. Como resultado das regras, a solução deve ter a capacidade de realizar ações automáticas, no mínimo:

4.4.22.1 Enviar e-mail.

4.4.22.2 Enviar mensagem para o usuário conectado no console.

4.4.22.3 Criar um incidente no sistema de workflow interno.

4.4.22.4 Enviar traps SNMP e popular listas (watchlist).

4.4.23. A solução deve possuir a capacidade de se integrar com os principais sistemas de inteligência de ameaças de riscos globais e das soluções de segurança da informação presente no TJCE, tais como: PAN-DB, Tenable.io Threat Intelligenc, Kaspersky Threat Intelligence, HP ThreatLink (DVLabs), Symantec DeepSight, Verisign iDefense, IBM X-Force, etc.

4.4.24. A solução deve oferecer a flexibilidade de utilizar qualquer metadado dos eventos em regras de correlação.

4.4.25. A solução deve permitir testar as regras de correlação em eventos passados, com um período de tempo e escopo claramente definidos.

4.4.26. A correlação histórica deve fornecer a opção de escolher o período a ser analisado, com suporte mínimo para correlação de 1 dia, 7 dias e 30 dias.

4.4.27. As regras de correlação histórica devem processar logs e flows, gerando alertas quando os eventos/flows analisados corresponderem às especificações definidas na regra.

4.4.28. Uma regra de correlação deve ter a capacidade de correlacionar eventos de tipos e origens distintos, verificando situações como a sequência de eventos diferentes, a contagem de eventos e a ausência de um evento após a ocorrência de outro.

4.5. Recursos da console de administração e operação do SIEM.

4.5.1. A console de administração e operação deve ser configurada e operada pela CONTRATADA.

4.5.2. A console de consulta deve incluir a capacidade de classificar os eventos em geral

em três grupos distintos:

4.5.2.1 Eventos de auditoria (logins, logouts, erros de autenticação, etc.).

4.5.2.2 Eventos de Segurança (ataques, comprometimento, roubo de dados, fraudes, etc.).

4.5.2.3 Eventos de Operação (erros, eventos críticos de ativos e rede, etc.).

4.5.3. A console deve contar com as seguintes especificações:

4.5.3.1 Ter uma interface web única, via HTTPS, para administração, gerenciamento e operação do sistema como um todo, garantindo a confidencialidade dos dados.

4.5.3.2 Ter acesso controlado e autenticado por usuário.

4.5.3.3 Ter capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários.

4.5.3.4 Permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0.

4.5.3.5 Garantir acesso aos dados e funcionalidades específicas por perfis de usuário.

4.5.3.6 O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução de acordo com os perfis de usuários definidos pelo administrador.

4.5.3.7 O controle de acesso deve ser configurado para permitir o acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, atividades de Redes e Logs.

4.5.3.8 Permitir a visualização de eventos, flows de rede e incidentes de segurança em tempo quase real.

4.5.3.9 Permitir a pesquisa nos eventos históricos com base em metadados, oferecendo a capacidade de drill-down, ou seja, refinamento da pesquisa a partir da seleção de elementos no resultado para realizar uma nova pesquisa.

4.5.3.10 Disponibilizar a visualização dos eventos relacionados a um alerta e/ou

incidente de segurança identificado pelas regras de correlação da solução.

4.5.3.11 A solução deve permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

4.5.3.12 Ter a capacidade de criar novos painéis gráficos (dashboards) e modificar os existentes.

4.5.3.13 Ter a capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (exemplo: Firewall, Proxy e antivírus na mesma visualização).

4.5.3.14 Ter a capacidade de criar listas (watchlist) e alterar as existentes, permitindo a inserção dos dados de forma manual, por linha de comando e automática por meio das regras de correlação.

4.5.3.15 Permitir a remoção de dados das listas (watchlist) de forma manual, automática por meio das regras de correlação e por expiração do tempo de vida da informação.

4.5.3.16 Possuir a capacidade de gerenciar e configurar centralmente todas as partes distribuídas da solução.

4.5.3.17 Possuir a capacidade de atualizar os componentes da solução por meio da console central de administração.

4.5.3.18 Ter a capacidade de restaurar informações de cópia de segurança do banco de dados, configurações e dados que foram arquivados previamente pela solução.

4.5.3.19 Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente.

4.5.3.20 Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes ou definidos pelo usuário.

4.5.3.21 Para análise dos eventos e flows de rede, é necessário ter suporte a

filtros de eventos, incluindo filtros simples, pesquisa de expressões e buscas avançadas diretamente na base de dados.

4.5.3.22 Deve oferecer APIs do tipo webservices, seguindo o padrão "RESTful API", para permitir o acesso externo à solução, possibilitando a busca de informações de eventos e flows, assim como a manipulação de incidentes.

4.5.3.23 Deve suportar o controle de acesso à solução com base em informações externas, validando atributos do usuário ou grupo a que ele pertence. Essa validação de autorização deve ser suportada em diretórios LDAP ou Windows Active Directory.

4.5.3.24 Deve fornecer uma API para a criação de fontes de logs (data sources) por meio de uma interface ReST, com o objetivo de automatização.

4.5.4. Os relatórios devem contar com as seguintes especificações:

4.5.4.1 Deve permitir a geração de relatórios, em quase tempo real, que englobem diversas informações em um único documento, como dados de segurança e rede.

4.5.4.2 Fornecer a funcionalidade de geração de relatórios de conformidade, abrangendo, pelo menos, SOX, PCI e ISO.

4.5.4.3 Deve ser permitido agendar a execução de relatórios em qualquer horário ou período, com a opção de enviar os resultados por e-mail.

4.5.4.4 Deve permitir a criação de relatórios relacionados a incidentes, logs, flows de rede e vulnerabilidades.

4.5.4.5 Deve organizar os relatórios em grupos temáticos, permitindo a criação de novos agrupamentos de relatórios pelos usuários.

4.5.4.6 Deve possibilitar a personalização de novos relatórios com base em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes.

4.5.4.7 Deve gerar relatórios de eventos, alertas/incidentes em níveis técnico e gerencial, que podem ser exportados nos formatos PDF, HTML, XLS, CSV, XML e RTF/DOC.

4.5.4.8 Os usuários devem ter acesso apenas aos seus próprios relatórios ou aos relatórios disponibilizados por outros usuários. Os administradores devem ter acesso a todos os relatórios.

4.5.4.9 Deve ser possível definir perfis de usuários com permissões/restrições para editar os modelos de relatórios.

4.5.4.10 Deve ser possível gerar relatórios com base em dados que contenham endereços IPv6.

4.5.4.11 A funcionalidade de backup deve preservar os dados dos relatórios.

4.5.4.12 Deve permitir a geração de relatórios que incluam os eventos associados a um incidente detectado por regras de correlação.

4.5.4.13 Permitir classificar eventos de segurança: ataques, reconhecimento, malware, atividades suspeitas de rede ou usuários, etc.

4.5.4.14 Contar com a opção de incluir os TOP endereços lógicos de origem das ameaças, TOP países e cidades de origem das ameaças e dos alertas de segurança.

4.5.5. A CONTRATADA deverá garantir que terá acesso ao suporte do fabricante da tecnologia SIEM durante a vigência do contrato. Para isso, a CONTRATADA deverá apresentar um acordo de suporte direto com o fabricante, assegurando que terá acesso a especialistas qualificados para resolver dúvidas, consultas ou problemas de configuração relacionados à ferramenta SIEM.

4.6. Dimensionamento do SIEM.

4.6.1. Considerando os elementos listados na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE as seguintes ferramentas consultadas:

4.6.1.1 Planilha de cálculo de EPS da IBM baseada no preenchimento na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE, com estimativa final de demanda na faixa de 10.100 a 11.300 EPS.

Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE

Item	Tipo de equipamento	Qde.
1	Sistemas Núcleo de Alto Volume	2
2	Sistemas Núcleo de Médio Volume	3
3	Infraestrutura de Segurança Típica	2
4	Soluções de Autenticação	7
5	Soluções de Serviços de Rede	39
6	Soluções IaaS/PaaS	0
7	Soluções Núcleo SaaS	1
8	Soluções Anti-Malware	1
9	Soluções de Criptografia	1
10	Registros de Servidores Web/Email	264
11	Soluções de Gerenciamento de Inventário	1
12	Soluções de HIPS e Decepção	1
13	Soluções de Borda SaaS	0
14	Registros de Servidores	42
15	Registros de Estações de Trabalho/Hosts	9050
16	Sistemas de Rede	1275

4.6.1.2 Calculadora de EPS: https://teskalabs.com/products/logman.io/eps-calculator/ com demanda de 5.873 EPS, conforme mostrado abaixo:

TeskaLabs SIEM and Log Management EPS Calculator

Sizing your Log Management and SIEM solution right is important and not an easy task. The solution is to make an analysis of your infrastructure as it directly impacts your Log Management / SIEM and the storage required to operate it efficiently. The two key numbers are Events per Second (EPS) and Gigabytes per Day (GB/day) indicating the volume of data processed in your IT infrastructure.

The calculation is based on the number of types of devices (nodes) in your IT infrastructure, which includes servers, routers, switches, firewalls and other network devices and applications.

Events Per Second (EPS) define the number of events or processes that take place in a given time on any IT appliance in your IT infrastructure.

Log Sources	Count	EPS	Daily volume
Windows desktops	905(	45.25	18.1 GB
Windows Servers	7	28	1.7 GB
Linux Servers	10	30	716.8 MB
Application Firewalls	1	30	716.8 MB
Network Firewalls	2	320	6.0 GB
Network Routers	2	2	41.0 MB

Network Switches	625	1250	12.5 GB
Network Flows	0	0	0.0 GB
Network Wireless LAN	650	3250	39.0 GB
Network Load Balancers	1	5	61.4 MB
Network IPS/IDS	1	100	2.4 GB
Network VPN	2	4	102.4 MB
Network Web Proxy	1	20	1.0 GB
Other Network Devices	0	0	0.0 GB
Hypervisor (Microsoft Hyper-V, VMware ESXi etc)	31	465	37.5 GB
WebServers	251	251	555.2 MB
Database	42	42	74.4 MB
Mail Servers	13	26	57.5 MB
Antivirus, DLP, EDR, etc.	1	5	11.1 MB
Other applications	0	0	0.0 GB
Custom		0	0 GB
	Total	5873	120.5 GB

4.6.1.3 Calculadora de EPS: https://siemsizingcalculator.logpoint.com/ com demanda de 6.226,53 EPS, conforme mostrado abaixo:

LOGPOINT Contact About Us

Infrastructure

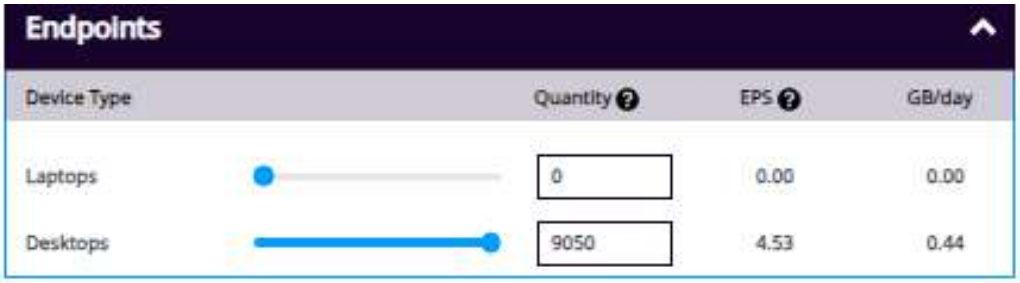
Device Type	Quantity	EPS	GB/day
Windows Servers - HIGH EPS (Event Log)	7	49.00	4.73
Windows Servers - MED EPS (Event Log)	1	3.00	0.29
Windows Servers - LOW EPS (Event Log)	0	0.00	0.00
Linux Servers	10	30.00	0.72
Unix Servers	0	0.00	0.00
Network Wireless LAN	650	3250.00	39.23
Hypervisor (ESXi, Hyper-V etc)	31	465.00	37.42
Web Servers	251	251.00	5.05
Email Servers	0	0.00	0.00

Security

Device Type	Quantity	EPS	GB/day
Network Firewalls (Layer 7 Internal)	1	240.00	9.66
Network Firewalls (Layer 7 - DMZ)	0	0.00	0.00
Network Firewalls (Internal)	2	480.00	9.66
Network Firewalls (DMZ)	2	100.00	2.01
Network IPS/IDS	1	100.00	2.41
Antivirus	0	0.00	0.00
Data Loss Protection (DLP)	0	0.00	0.00
Others	0	0.00	0.00

Network

Device Type	Quantity	EPS	GB/day
VPN Server	1	2.00	0.05
Network Routers	2	2.00	0.04
Switches	625	1250.00	10.06



Endpoints

Device Type	Quantity	EPS	GB/day
Laptops	0	0.00	0.00
Desktops	9050	4.53	0.44

4.6.1.4 Calculadora de EPS: https://positka.in/siem-sizing-calculator com demanda de 8.304 EPS, conforme mostrado abaixo:

SIEM Sizing Calculator – Calculate your infrastructure EPS

Design an efficient plan for sizing SIEM as per your infrastructure with our ha calculator. The calculation is based on the volume of data ingested to the SIE devices in your IT infrastructure.

Data Source	Number of Devices (endpoints)	In monitoring scope? (Yes / No)	Estimated EPS per day
Network and security			
User Authentication / SSO / PAM / IAM	1	Yes	10
Active Directories, Domain Controlers	7	Yes	70
Switches (syslog)	625	Yes	1250
Routers (syslog)	2	Yes	2
Wireless Access Points	650	Yes	3250
Firewalls	2	Yes	400
DDoS Protection	0	Yes	0
VPNs	1	Yes	5
Proxy Systems	1	Yes	20
Vulnerability Scanners	1	Yes	5

IDS / IPS	1	Yes	15
Threat Intelligence Feeds	0	Yes	0
Data Loss/Leakage Prevention (DLP)	0	Yes	0
EDR (Endpoint Detection & Response)	0	Yes	0
WAF (Web Application Firewall)	1	Yes	30
Network Load Balancers	1	Yes	5

Infrastructure and applications			
Windows Servers (physical and virtual)	7	Yes	105
Unix Servers (physical and virtual)	10	Yes	30
Virtual Infrastructure Servers (Hypervisor)	31	Yes	465
Web Servers	251	Yes	2510
Application Servers	13	Yes	65
Database Instances	42	Yes	42
Storage Arrays	0	Yes	0

Cloud			
Cloud Services - Azure	0	Yes	0
Cloud Services - AWS	0	Yes	0
Cloud Services - Google	0	Yes	0
SaaS	1	Yes	25
Totals	1648		8304

4.6.2. A variação de EPS de ferramentas SIEM de múltiplos fabricantes, em uma mesma infraestrutura de redes, pode ser influenciada por vários fatores, incluindo o desempenho e eficiência da ferramenta, a capacidade de processamento do hardware subjacente e a otimização das configurações da ferramenta para o ambiente específico. Cada fabricante de SIEM pode ter implementações e abordagens diferentes para a coleta, processamento e análise de eventos de segurança. Essas diferenças podem impactar diretamente a capacidade do SIEM de lidar com um grande volume de eventos por segundo.

4.6.3. Os cálculos mostrados no item 4.6.1 são dados sobredimensionados porque na implantação podem haver ferramentas que diminuam a demanda de EPS (exemplo: EDR ou XDR) e nem todos os ativos podem ser considerados necessários para monitoramento. Sendo assim, a quantidade demandada de EPS é incerta (relatada pelos próprios fabricantes) até ser evidenciado na implantação da solução SIEM. Para não existir risco de contratar uma quantidade maior de EPS do que a mínima possível implantada, e conforme orientação de fornecedores, serão demandados inicial e aproximadamente 30% da maior estimativa de EPS levantada (item 4.6.1.1). Ou seja, a CONTRATADA deve fornecer o serviço de solução SIEM com funcionamento de 3.000 EPS por 36 meses a partir do TRD de implantação.

4.6.4. Como estratégia de complementação de EPS, a CONTRATADA deve oferecer a possibilidade de fornecer até 10 pacotes adicionais, usados sob demanda, de 500 EPS, 1.000 EPS ou 2.000 EPS cada um (ver serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação). Os pacotes adicionais podem ser demandados de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual. Portanto, os quantitativos de pacotes de EPS contratados representam meramente uma estimativa de utilização de serviço. Não haverá obrigação do TJCE na utilização do quantitativo parcial ou total dos pacotes de extra que são apresentados nos serviços 4, 5 e 6 da Tabela 1. Serviços gerenciados e inter-relacionados necessários de segurança da informação. Somente serão

devidos e pagos os pacotes adicionais efetivamente prestados e demandados através das respectivas Ordens de Serviço. A quantidade de pacotes adicionais demandados pode ser redimensionado em qualquer momento para quantidades maiores ou anualmente em quantidade menor (dentro da duração do contrato) e em função da mudança de monitoramento demandado pelo TJCE.

4.7. Serviço de monitoramento e correlação de eventos de segurança da informação

4.7.1. As atividades do Serviço de monitoramento e correlação de eventos de segurança da informação serão medidas por Níveis Mínimos de Serviço.

4.7.2. Os profissionais alocados no serviço de monitoramento e correlação de eventos (Analista SIEM) serão integrantes das operações no SOC conforme perfil descrito no item 4.8.

4.7.3. A CONTRATADA deverá disponibilizar, nas instalações do TJCE (Fortaleza/CE), o acesso de leitura a console das tecnologias que suportam os serviços de Gestão de Vulnerabilidades e de Coleta, Análise e Correlação de Logs (SIEM).

4.7.4. Monitoramento 24x7x365 da infraestrutura de TI, utilizando a ferramenta SIEM como sua tecnologia base, conforme apresentado na Tabela 3. Dimensionamento de EPS por tipo de equipamento na rede do TJCE e futuras expansões ou modificações.

4.7.5. A CONTRATADA deverá adotar uma abordagem preventiva e reativa, identificando eventos suspeitos, classificando os incidentes de cibersegurança e fornecendo ao TJCE um relatório para cada evento identificado.

4.7.6. A CONTRATADA terá a responsabilidade de identificar e classificar os eventos de segurança utilizando a ferramenta de SIEM. O Blue Team, com apoio do serviço de monitoramento e o Red Team, será responsável por tratar o evento no serviço/host indicado no relatório fornecido pela CONTRATADA.

4.7.7. O serviço de SIEM deverá oferecer ao TJCE as seguintes facilidades:

4.7.7.1 Monitoração de correlação de eventos.

4.7.7.2 Gestão de incidentes.

4.7.7.3 Criação de novas regras de correlação e casos de uso e detecção.

4.7.7.4 Inteligência de ameaças e conformidade.

4.7.8. Triagem de incidentes identificados pelo serviço de monitoramento.

4.7.8.1 É necessário realizar uma triagem inicial nos chamados abertos pela monitoração de segurança, identificando e agrupando os potenciais incidentes que possuam características semelhantes, como ataques direcionados ao mesmo servidor, ataques originados do mesmo IP ou múltiplas falhas de login, por exemplo.

4.7.8.2 Após a etapa de triagem inicial, os chamados devem ser avaliados para determinar se são resultantes de falsos positivos/negativos, além disso, serão realizados testes para verificar a veracidade do incidente detectado.

4.7.9. Problemas identificados pelo serviço de monitoramento.

4.7.9.1 A equipe da CONTRATADA deve abrir chamados de problema em seu próprio sistema e no sistema do TJCE, relacionados ao serviço de monitoração, a fim de identificar a causa raiz. O Blue Team, com o suporte do serviço de monitoramento e o Red Team, deve solucionar o(s) problema(s) identificado(s) ao atender as demandas de incidentes.

4.7.9.2 Os chamados devem ser atendidos pelo Blue Team, com o apoio do serviço de monitoramento.

4.7.10. Incidentes de segurança identificados pelo serviço de monitoramento.

4.7.10.1 O Blue Team, com o suporte do serviço de monitoramento e o Red Team, será responsável por lidar com todo tipo de incidente e executar os procedimentos de resposta (item 2.3.13) para que seja implementada a respectiva solução.

4.7.10.2 O TJCE deve ser notificado sobre os incidentes por meio do sistema de chamados, e-mail e/ou telefone, conforme acordado previamente com o TJCE, de acordo com as necessidades de comunicação interna e/ou externa.

4.7.10.3 A CONTRATADA deve fornecer informações sobre os incidentes ao TJCE, por meio da abertura de chamados na ferramenta de ITSM do

TJCE.

4.7.11. Ocorrência de Incidentes no serviço de monitoramento.

4.7.11.1 Em caso de detecção de algum incidente de segurança, a CONTRATADA deve contatar imediatamente o TJCE por telefone, e-mail e abertura de chamado na ferramenta de ITSM do TJCE. Isso é necessário para que sejam tomadas as medidas corretivas e legais adequadas, tanto pela equipe da CONTRATADA quanto, se necessário, com a colaboração da equipe do TJCE, seguindo o procedimento estabelecido para resposta a incidentes (item 2.3.13).

4.7.11.2 O serviço de monitoramento deve comunicar imediatamente ao TJCE sobre acessos indevidos, instalação de códigos maliciosos ou qualquer outra ação que represente um risco para a segurança do ambiente do TJCE. Isso deve ser feito mesmo se essas tentativas não forem bem-sucedidas, mas houver persistência por parte do agente mal-intencionado.

4.7.11.3 O serviço de monitoramento deve fornecer todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que os incidentes de segurança relatados possam ser investigados pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12. Resposta a incidentes no serviço de monitoramento.

4.7.12.1 A CONTRATADA deve incluir as informações necessárias, como origem do ataque, tipo de ataque, data e hora, logs, causa do incidente de segurança e o procedimento de resposta ao incidente na ferramenta de ITSM do TJCE, a fim de possibilitar a implementação das medidas corretivas necessárias pelo Blue Team, com o suporte do serviço de monitoramento e do Red Team.

4.7.12.2 Os incidentes de segurança devem estar relacionados a eventos de segurança das soluções monitoradas e podem incluir, mas não se limitar

a, acessos indevidos, instalações de códigos maliciosos, indisponibilidade de serviços devido a ataques de negação de serviço (DoS e DDoS), ataques por força bruta ou qualquer outra ação que possa comprometer a confidencialidade, disponibilidade ou integridade das informações do TJCE.

4.7.13. Software e Hardware necessários para a solução SIEM no serviço de monitoramento.

4.7.13.1 A CONTRATADA é responsável por fornecer os softwares e hardwares necessários para implantar os serviços gerenciados de monitoramento e correlação de eventos de segurança da informação, durante o prazo do contrato e sem custos adicionais para o TJCE.

4.7.14. Configuração do *Security Information and Event Management* (SIEM).

4.7.14.1 A CONTRATADA deverá ativar o serviço que será utilizado como ferramenta, durante a vigência do contrato e antes do TRD de implantação, para prestação do Serviço de Coleta, Análise e Correlação de Logs, através de uma solução SIEM.

4.7.14.2 A CONTRATADA deve realizar a implementação das configurações, regras e políticas apropriadas para o ambiente do TJCE, levando em consideração as necessidades específicas do ambiente.

4.7.14.3 O TJCE, com o suporte da CONTRATADA, será responsável por realizar as configurações nos equipamentos de rede (switches, roteadores, servidores, etc.), servidores Linux/Windows e equipamentos de segurança da informação do TJCE para enviar os logs para a solução de SIEM. Adicionalmente, as configurações na solução de SIEM são de responsabilidade da CONTRATADA.

4.7.14.4 As configurações, regras de correlação, alertas e outras configurações do SIEM serão implementadas pela CONTRATADA e de propriedade intelectual e responsabilidade exclusiva do TJCE. Portanto, essas configurações não devem ser extraídas, copiadas, manipuladas ou

removidas sem o consentimento expresso do TJCE.

4.7.14.5 A Solução de SIEM deve abrir automaticamente chamados na ferramenta de ITSM do TJCE sempre que detectar um possível incidente de disponibilidade ou segurança.

4.7.14.6 Toda a mão de obra especializada necessária para a instalação e configuração da solução de SIEM deve ser fornecida pela CONTRATADA.

4.7.14.7 A CONTRATADA é responsável por executar todas as operações de monitoramento, gerenciamento e administração da solução de SIEM, conforme determinação do TJCE, abrangendo, mas não se limitando a:

4.7.14.7.1. Coleta de logs.

4.7.14.7.2. Criação de regras de correlação, não havendo limite mínimo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados.

4.7.14.7.3. Realização de configurações do SIEM (agentes, regras de incidentes, regras de correlação, etc).

4.7.14.7.4. Interação com o fabricante da solução.

4.7.14.7.5. Backup e restore.

4.7.14.7.6. Resolução de problemas.

4.7.14.7.7. Suporte.

4.7.14.7.8. Instalação de serviços relativos ao escopo contratado.

4.7.14.7.9. Atualização, de acordo com as recomendações do fabricante.

4.7.14.7.10. Outras operações citadas nos itens 4.3, 4.4 e 4.5.

4.7.14.8 Durante a fase de implantação, a CONTRATADA deve apresentar um conjunto de regras pré-definidas para ativação. Essas regras só serão implementadas após a aprovação do TJCE.

4.7.14.9 CONTRATADA será responsável por documentar as regras aprovadas pelo TJCE. A documentação de regras aprovadas (novas ou atualizadas)

deve seguir os processos de gerenciamento de mudanças do TJCE.

4.7.14.10 O TJCE tem permissão para solicitar alterações nas regras de correlação de eventos, de forma a ajustá-las às suas necessidades.

4.7.14.11 A CONTRATADA deverá prestar todos os serviços relativos ao SIEM (implantação, configuração, manutenção, análise de logs, detecção/resposta a incidentes, backup e restore, etc), conforme requisitos de funcionamento do SIEM apresentados nos itens 4.1 até 4.6.

4.7.14.12 A operação da console de administração e operação deverá ser de responsabilidade exclusiva da CONTRATADA, conforme especificações técnicas dos itens 4.1 até 4.6.

4.7.14.13 É de responsabilidade da CONTRATADA realizar a integração do SIEM de forma a possibilitar o recebimento de alertas e a abertura automática de incidentes na ferramenta de ITSM do TJCE.

4.8. Perfil dos profissionais do Analista de Segurança Sênior - SIEM.

4.8.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS, contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 12 meses.

4.8.2. Deve contar com a certificação relacionada e emitida pelo fabricante da ferramenta SIEM usada no serviço de monitoramento e correlação de eventos.

4.8.3. Deve contar com proficiência de inglês intermediário para poder estabelecer comunicação com a comunidade técnica do fabricante da ferramenta SIEM, com o objetivo de obter informações que ajudem na implantação, execução, configuração e manutenção da ferramenta SIEM.

4.8.4. Deve contar com especialização em segurança da informação, comprovada através de certificado de conclusão oudiploma emitido por instituição de ensino superior reconhecida pelo Ministério da Educação ou com, pelo menos, uma das seguintes certificações: CompTIA Security+; EXIN Information Security Foundation; EXIN Ethical Hacking Foundation; GIAC Security Essentials (GSEC).

5. NÍVEIS MÍNIMOS DE SERVIÇO

5.1. Os Níveis Mínimos de Serviço (NMS) são parâmetros claros e mensuráveis que têm como objetivo avaliar e verificar vários aspectos dos serviços contratados, incluindo qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança. Esses critérios são estabelecidos de forma objetiva para garantir a excelência na prestação dos serviços.

5.2. Os serviços serão avaliados por meio de indicadores e NMS estabelecidos em fórmulas de cálculo específicas.

5.3. A responsabilidade de cumprir os NMSs é da CONTRATADA. A avaliação será realizada pela equipe de fiscalização do TJCE mensalmente, levando em consideração as metas exigidas dos serviços, conforme descrito na Tabela 4. Indicadores de Nível de Serviço. Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento (pontos) serão cumulativas.

5.4. A empresa contratada é responsável por manter os padrões de qualidade estabelecidos para a prestação dos serviços, conforme Tabela 4. Indicadores de Nível de Serviço e Tabela 5. Glosas por descrição de referências para todos os serviços contratados.

5.5. A CONTRATADA terá uma redução de 2% (dois por cento) sobre o valor da fatura referente ao mês de ocorrência, a cada 15 pontos, ou um valor proporcional de redução de 2% a cada 15 pontos de glosa. Exemplo: para uma glosa de 10 pontos, a redução será de 1,33% como resultado da conta proporcional (10/15)*2%.

5.6. A meta exigida estabelece o valor exato (=), o limite máximo (<=) ou o limite mínimo (>=) que a CONTRATADA deve alcançar para cada um dos indicadores.

5.7. A meta exigida do cálculo com base no mês calendário será aplicado ao menor valor instantâneo entre os indicadores relativos aos horários de expediente regular ou horários de plantão contínuo. Por exemplo, um incidente que tenha sido inicializado no horário de plantão contínuo faltando 5 minutos para que comece o horário de expediente regular, passará a ter a menor meta entre ambos horários (após os 5 minutos) até a sua solução. Da mesma forma, um incidente que tenha sido inicializado no horário de expediente regular faltando 5 minutos para que comece o horário de plantão contínuo, passará a ter a menor meta (após os 5 minutos) entre ambos horários até a sua solução.

5.8. A CONTRATADA será responsável apenas pelos índices relacionados às solicitações de serviços e incidentes atribuídos a ela. Ela não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outras equipes do TJCE, nem por situações dependentes de terceiros, que, portanto, não serão consideradas para fins de cálculo.

5.9. Requisições de serviço e incidentes reabertos referem-se a solicitações de serviço ou incidentes que foram considerados resolvidos, mas ainda estão pendentes de solução.

Tabela 4. Indicadores de Nível de Serviço

Serviço da Tabela 1	Nº	Indicadores de Nível de Serviço	Cálculo com base no mês calendário	Meta Exigida	Glosa
1, 2 e 3	1	Atividades rotineiras mensais definidas nos itens 2, 3 e 4, e programadas de acordo com o Plano de Trabalho ou por Requisição de Serviço.	Tempo = (Horas investidas nas atividades programadas) – ([Horas acordadas na OS]*1,25)	<=0 minutos	60 pontos
1 e 3	2	Índice de disponibilidade dos serviços de monitoramento e correlação de eventos (SIEM).	100 * [(Total de tempo com disponibilidade no mês – com exceção de indisponibilidade de energia ou link de conexão) / (Total de tempo no mês)] %	>= 99,7%	5 pontos (+2 pontos a cada hora excedente)
	3	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de expediente regular.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
	4	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de indisponibilidade e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) – (Hora do início da indisponibilidade)	<= 180 minutos	30 pontos (+5 pontos a cada 20 minutos excedentes)
	5	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de expediente regular.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 120 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	6	Tempo máximo para diagnóstico de incidente nos serviços de segurança do TJCE, em caso de degradação de desempenho e em horário de plantão contínuo.	Tempo = (Hora do diagnóstico) - (Hora do início da degradação de desempenho)	<= 240 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
	7	Tempo máximo de não acompanhamento	Tempo = (Hora da solicitação de	<= 15	10 pontos

		a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de expediente regular.	acompanhamento) – (Hora de resposta da solicitação)	minutos	(+5 pontos a cada 10 minutos excedentes)
	8	Tempo máximo de não acompanhamento a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de plantão contínuo.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 45 minutos	10 pontos (+5 pontos a cada 10 minutos excedentes)
	9	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados por outras equipes e em horário de expediente regular.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
	10	Tempo máximo de não acompanhamento a incidentes de degradação de desempenho que estão sendo solucionados por outras equipes e em horário de plantão contínuo.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 90 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
	11	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente.	Tempo = (Hora de conclusão do planejamento da requisição de mudança) – (Hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente)	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)
	12	Tempo máximo para abertura de chamados de suporte com terceiros. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de abertura do chamado) – (Hora da triagem)	<= 30 minutos	5 pontos (+2 pontos a cada 5 minutos excedente)
1	13	Tempo máximo para resolução de requisições de serviços relacionados aos Produtos de UTM, NGFW, EDR, WAF, Gestor de vulnerabilidades. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 180 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
	14	Tempo máximo para resolução de requisições de serviços relacionados a outros ativos de segurança da informação.	Tempo = (Hora de resolução da solicitação) – (Hora da solicitação)	<= 30 horas	10 pontos (+3 pontos a cada hora excedente)
	15	Tempo máximo para triagem de incidentes de segurança e em horário de expediente regular.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 15 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	16	Tempo máximo para triagem de incidentes de segurança e em horário de plantão contínuo.	Tempo = (Hora da triagem) – (Hora de entrada do evento de segurança)	<= 120 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
	17	Tempo máximo para resposta de	Tempo = (Hora do início da resposta) –	<= 60	10 pontos

		incidentes de segurança de gravidade alta e em horário de expediente regular.	(Hora da triagem)	minutos	(+3 pontos a cada 5 minutos excedentes)
	18	Tempo máximo para resposta de incidentes de segurança de gravidade alta e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 480 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	19	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 150 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	20	Tempo máximo para resposta de incidentes de segurança de gravidade média e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	21	Tempo máximo para resposta de incidentes de segurança de gravidade baixa e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 210 minutos	5 pontos (+2 pontos a cada hora excedente)
	22	Tempo máximo para resposta de incidentes de segurança de gravidade baixa e em horário de plantão contínuo.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 420 minutos	5 pontos (+2 pontos a cada hora excedente)
	23	Tempo máximo para comunicação de incidentes a central de serviços da CONTRATADA e à equipe de segurança do TJCE. Somente aplicável a partir do horário de expediente regular.	Tempo = (Hora da comunicação) – (Hora da triagem)	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes)
2	24	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço.	Tempo = (Horas investidas na Requisição de Serviço) – ([Horas acordadas na OS]*1,25)	<=0 minutos	15 pontos

Tabela 5. Glosas por descrição de referências para todos os serviços contratados

Nº	Descrição	Referência	Glosa
1	Não implementar a coleta de logs (via coletores), sua integração com a ferramenta SIEM e a retenção de logs após o período de carência de glossa.	Por ocorrência e por dia	15 pontos
2	Deixar de disponibilizar presencialmente no TJCE o Red Team, conforme descrito no item 1.3.1.	Por ocorrência e por dia	15 pontos
3	Deixar de fornecer os documentos comprobatórios de qualificação de qualquer profissional.	Por ocorrência e por dia	15 pontos
4	Deixar de documentar atividades rotineiras ou de requisição de serviço na ferramenta de ITSM.	Por ocorrência	5 pontos

5	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, mesmo em situações de substituição temporária.	Por profissional e por dia	15 pontos
6	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	50 pontos
7	Suspender, colocar como pendente, pausar ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	5 pontos
8	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável.	Por regra incluída, alterada ou excluída	10 pontos
9	Fraudar, manipular ou descaracterizar indicadores, metas de níveis de serviço e de desempenho por quaisquer subterfúgios.	Por ocorrência	100 pontos
10	Deixar de cumprir qualquer outra obrigação estabelecida no contrato e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10 pontos
11	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	180 pontos
12	Causar qualquer dano aos equipamentos do TJCE por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50 pontos
13	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10 pontos
14	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 TJCE.	Por ocorrência	10 pontos
15	Incluir, excluir ou alterar regras nos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	20 pontos
16	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada ou Rotineira.	Por ocorrência	10 pontos
17	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique, sem prejuízo de outras sanções legais e das cabíveis penais previstas no art. 156, da Lei n. 14.133/2021.	Por ocorrência	60 pontos
18	Deixar de apresentar relatórios, levantamentos ou inventários no prazo determinado em comum acordo.	Por ocorrência	15 pontos
19	Deixar de comunicar o contratante da substituição de profissionais responsáveis pela execução das atividades.	Por ocorrência	30 pontos
20	Deixar de atuar tempestivamente no caso de incidentes graves.	Por ocorrência	60 pontos
21	Deixar de cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
22	Deixar de cumprir ou implementar as rotinas em conformidade com os processos de trabalho do TJCE e da Diretoria de Tecnologia da Informação	Por ocorrência	10 pontos
23	Deixar de apresentar mensalmente propostas de melhorias no ambiente	Por ocorrência	5 pontos
24	Deixar de notificar sobre ocorrências recorrentes.	Por ocorrência	5 pontos