ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ESTUDOS TÉCNICOS PRELIMINARES - ETP

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

1. INTRODUÇÃO

1.1 Este documento tem como finalidade de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1 Identificação das necessidades de negócio

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, como por exemplo:

2.1.1.1 Dados processuais: informações relacionadas a processos judiciais.

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

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

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

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.

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

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:

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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.

2.1.3. 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:

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

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

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.

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

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.

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

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.

2.1.4. 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:

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

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.

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

2.1.5. Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes de segurança da informação.

2.2 Identificação das necessidades tecnológicas

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:

2.2.1.1. 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.

2.2.1.2. 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. Contar com serviços especializados em solução tecnológica *Security Information and Event Management* (SIEM) para agregação, consolidação e padronização de tratamento dos registros ou logs, criados pelos equipamentos de rede e de segurança

da informação do TJCE, conforme os seguintes tópicos do Manual de referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital (ANEXO V DA PORTARIA No 162, DE 10 DE JUNHO DE 2021 do CNJ):

2.2.2.1. Inciso 34-d: os dados de eventos sejam coletados e correlacionados a partir de várias fontes e sensores. Sugere-se utilizar solução de *Security Information and Event Management* (SIEM) para auxiliar no correlacionamento de eventos.

2.2.2.2. Inciso 34-e: existam thresholds e regras para geração de incidentes a partir dos eventos coletados.

2.2.2.3. Inciso 34-f: exista monitoramento específico de segurança cibernética para o ambiente físico, a rede e as atividades pessoais a fim de se detectar eventos.

2.2.3. 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):

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

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

2.2.3.3. Inciso 6.7: Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais.

2.2.3.4. 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.

2.2.4. 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.

2.2.5. 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 **ETP - ANEXO I**.

2.2.6. 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.

2.3 Demais requisitos necessários e suficientes à escolha da solução de TIC

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

2.3.2. Apresentar, sempre que solicitado, durante a execução do contrato, documentos que comprovem o cumprimento da legislação em vigor quanto às obrigações assumidas.

2.3.3. Todas as informações obtidas ou coletadas pela empresa provedora da Solução de Tecnologia da Informação, durante a prestação dos serviços, devem ser tratadas como confidenciais. É proibida qualquer divulgação a terceiros, e a empresa deve garantir que seus sócios, funcionários e subcontratados (em outros clientes) mantenham absoluto sigilo sobre os dados, informações, documentos, especificações técnicas e comerciais aos quais possam ter acesso no decorrer dos serviços executados.

2.3.4. A obrigação assumida de Confidencialidade permanecerá válida durante e após o período de vigência contratual.

2.3.5. Acatar as recomendações da fiscalização do TJCE, facilitando a ampla ação desta, com pronto atendimento aos pedidos de esclarecimento porventura solicitados.

2.3.6. As obrigações e conhecimentos sobre os requisitos de segurança serão ratificados pelo TJCE e a empresa fornecedora da solução de TI em documentos posteriores.

2.3.7. Ter implementados os serviços especializados citados nos itens 3.1, 3.1 e 3.2 por um período mínimo de 36 meses. Período adequado para a implementação e consolidação dos serviços contratados, objetivando garantir uma maior eficiência e eficácia na prestação dos serviços. Além disso, um contrato com duração de no mínimo 36 meses, proporcionará maior estabilidade e previsibilidade tanto para a CONTRATANTE quanto para a CONTRATA-DA, 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 6).

2.3.8. 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).

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

3.1. **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 operacionais e técnicos deste serviço encontram-se no documento **ETP - ANEXO I**.

3.2. **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 operacionais e técnicos deste serviço encontram-se no documento **ETP - ANEXO I**.

3.3. **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. Os detalhes operacionais e técnicos deste serviço encontram-se no documento **ETP - ANEXO I**.

4. ANÁLISE DE SOLUÇÕES POSSÍVEIS

4.1. Identificação das Soluções

Id	Descrição da solução (ou cenário) para a Demanda
1	Serviços Gerenciados de Segurança da Informação 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 fortalecer sua postura de segurança, reduzir riscos e proteger seus ativos críticos, permitindo que elas se concentrem em suas principais atividades comerciais.

	Nessa 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. 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	Solução de ampliação da maturidade de ambiente A proposta consiste na oferta de serviços de segurança de rede e inclui a disponibilização de softwares e suas licenças, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico. A solução compreende a aquisição de equipamentos (hardware), software e prestação de serviços. A solução propõe a avaliação do pagamento por meio de uma combinação de "unidades", “meses” e “horas de serviço”, que são comumente utilizados para projetos ou serviços.
3	Solução integrada de serviços gerenciados de rede Nesta solução, busca-se promover a prestação de serviços com o objetivo de fornecer recursos e sistemas de informação estáveis e eficientes, que englobam: a maturidade e disponibilidade do ambiente; a independência tecnológica; o fortalecimento da governança de TI; a segurança de dados e informações; a prevenção de riscos de interrupção dos serviços; a transferência de conhecimento no momento adequado; o aumento da satisfação dos usuários com os produtos e serviços de TI fornecidos; e a gestão sustentável da administração, operação e suporte da rede. À empresa contratada é atribuída a responsabilidade de definir e gerenciar os profissionais envolvidos na prestação dos serviços, bem como suas respectivas entregas. Essa responsabilidade inclui o ajuste da equipe de colaboradores de acordo com as necessidades da entidade/órgão, visando o cumprimento das demandas solicitadas. A remuneração está diretamente relacionada à quantidade de ativos de Infraestrutura que serão gerenciados.

4.2. Análise Comparativa de Soluções

Requisito	Id da Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	**X**		
	2	**X**		
	3	**X**		
A Solução está disponível no Portal do Software Público Brasileiro?	1		**X**	
	2		**X**	
	3			**X**

A Solução é um software livre ou software público?	1		**X**	
	2		**X**	
	3			**X**
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	1			**X**
	2			**X**
	3			**X**
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1		**X**	
	2		**X**	
	3			**X**
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	1			**X**
	2			**X**
	3			**X**

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. Solução 2 - Solução de ampliação da maturidade de ambiente.

5.1.1. A solução 2 é normalmente relacionada a projetos ou serviços que requerem um aumento significativo no volume de serviços prestados. Esse pagamento está vinculado ao cumprimento dos ANS definidos, e podem ser aplicados redutores no faturamento por meio de glosas, caso haja descumprimento.

5.1.2. Esta solução é descrita em outros certames como adequada para entidades com ativos de menor criticidade e ambientes tecnológicos não altamente críticos, não sendo aplicável aos serviços específicos de gestão de incidentes de segurança (Blue Team), gestão de testes de invasão (Red Team) e serviços gerenciados de monitoramento e correlação de eventos de segurança da informação. Isso ocorre porque esses serviços requerem um nível mais avançado de segurança e expertise técnica, não se limitando apenas a controles mínimos.

5.1.3. O gerenciamento de incidentes de segurança, por exemplo, envolve a detecção, resposta e mitigação de eventos de segurança, exigindo conhecimentos especializados, investigação forense e coordenação eficaz com diferentes partes envolvidas.

5.1.4. Da mesma forma, os testes de invasão (Red Team) envolvem simulações de ataques para identificar vulnerabilidades e pontos fracos nos sistemas, e exigem habilidades avançadas de hacking ético e análise de segurança. Esses serviços não podem ser realizados de forma eficaz com uma abordagem de controles mínimos, pois

requerem uma análise profunda e abrangente dos sistemas e uma resposta proativa a potenciais riscos de segurança.

5.1.5. Já os serviços gerenciados de monitoramento e correlação de eventos de segurança da informação (SIEM), demandam a coleta, análise e correlação de dados de várias fontes, como logs de segurança, eventos de rede e sistemas, a fim de identificar atividades maliciosas ou suspeitas. Esses serviços exigem uma infraestrutura tecnológica robusta, capacidades avançadas de análise de segurança e profissionais especializados para interpretar os eventos e tomar as medidas apropriadas.

5.1.6. Portanto, esses serviços específicos de segurança da informação exigem abordagens mais avançadas e especializadas do que uma Solução de ampliação da maturidade de ambiente que se destina a ambientes menos críticos. É necessário considerar a natureza e complexidade dos serviços de segurança para garantir uma abordagem adequada e eficaz na proteção dos ativos e na gestão de incidentes de segurança.

5.1.7. Diante do exposto, a solução 2 se configura uma solução tecnicamente inviável para o atendimento a necessidade do TJCE.

5.2. Solução 3 - Solução integrada de serviços gerenciados de rede

5.2.1. Neste modelo, as demandas são encaminhadas por meio de Ordens de Serviço periódicas, com base na quantidade estimada de USI's para o período. As atividades de TI são pré-definidas em um Catálogo de Serviços, seguindo os padrões de qualidade, procedimentos e qualificações estabelecidos para a execução. A empresa contratada tem a responsabilidade de cumprir as atividades solicitadas conforme são demandadas, em conformidade com o modelo de execução.

5.2.2. A solução 3 contará com fiscalização técnica é mais complexa, maior necessidade de maturidade do órgão na definição das atividades a serem consumidas e risco de pagamento por atividades irreais, complexidade na mensuração do custo de cada atividade.

5.2.3. A adoção do modelo de serviços da solução 3, com remuneração baseada na quantidade de ativos de infraestrutura a serem geridos e catálogos de serviços, apresenta desafios de execução devido à falta de experiência prévia no âmbito do TJCE para um projeto de SOC. Isso resulta na ausência de um histórico preciso e confiável de consumo anterior. Além disso, a demanda do TJCE inclui serviços de gerenciamento de segurança que são essenciais para operar a segurança do TJCE.

5.2.4. Diante do exposto, a solução 3 se configura uma solução tecnicamente inviável para o atendimento a necessidade do TJCE.

6. PESQUISA DE PREÇOS DE MERCADO DAS SOLUÇÕES VIÁVEIS

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

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1 A implementação de um SOC é essencial para fortalecer a postura de segurança da organização. Ao longo de 36 meses, o SOC proporcionará um Blue Team altamente especializado para a gestão de incidentes de segurança, permitindo a identificação e resposta eficaz a ameaças em tempo real. Adicionalmente, a inclusão do Red Team para condução de testes de invasão possibilitará a avaliação proativa da infraestrutura e das defesas, identificando potenciais vulnerabilidades antes que possam ser exploradas por atacantes maliciosos. A integração de serviços gerenciados de monitoramento e correlação de eventos através da ferramenta SIEM aprimorará a capacidade da organização de detectar padrões suspeitos e comportamentos anômalos, permitindo uma resposta mais ágil e precisa a incidentes de segurança. Embora o investimento inicial possa ser significativo, os benefícios em termos de detecção precoce, resposta eficiente a ameaças e redução do risco de violações de segurança certamente justificam os custos associados a essa iniciativa. Portanto, os custos associados a essa estratégia de segurança são plenamente justificáveis, dada a proteção substancial que ela proporciona aos ativos e à integridade operacional da organização.

Solução 1 - Serviços Gerenciados de Segurança da Informação	
Descrição	Serviços de Security Operations Center (SOC) composto por Serviço de gestão de incidentes de segurança (Blue Team), Serviço de gestão testes de invasão (Red Team), por 36 meses e Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM.
Análise	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. Sendo assim, o custo fixo da contratação é o resultado da soma dos itens com Ids 1, 2 e 3 do VALOR MÉDIO 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. Vale a pena ressaltar que o valor anual estimado de **R$ 2.809.092,23** é baseado em propostas comerciais antes de um pregão. Em outras palavras, esse valor muito pro-

	vavelmente será reduzido como resultado da competitividade dos licitantes. Ainda considerando o valor anual estimado de **R$ 2.809.092,23**, ele é muito próximo ao valor da estimativa preliminar de R$ 2.604.763,00, presente no Plano Anual de Contratações (PAC) de 2023. As demandas previstas com IDs 4, 5 e 6 da próxima Tabela contam com o seguinte VALOR MÉDIO 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.

8. IDENTIFICAÇÃO DA SOLUÇÃO ESCOLHIDA

8.1. Solução Escolhida: a solução 1 é a solução escolhida pelos seguintes motivos.

8.1.1. 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 documento **ETP - ANEXO I**.

8.1.2. 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 3.

8.1.3. 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.

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

8.1.4.1. 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.

8.1.4.2. 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:

8.1.4.2.1. 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.

8.1.4.2.2. 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.

8.1.4.2.3. 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.

8.1.4.2.4. 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.

8.1.4.2.5. 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.

8.1.4.2.6. 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.

8.1.4.2.7. 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.

8.1.4.2.8. 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.

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

8.1.5.1. 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.

8.1.5.2. 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:

8.1.5.2.1. 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.

8.1.5.2.2. 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.

8.1.5.2.3. 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.

8.1.5.2.4. 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.

8.1.5.2.5. 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.

8.1.5.2.6. 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.

8.1.5.2.7. 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 TJCE e em suas práticas de segurança.

8.1.6. Benefícios do Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação por 36 meses:

8.1.6.1. 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:

8.1.6.1.1. 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.

8.1.6.1.2. 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.

8.1.6.1.3. 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.

8.1.6.1.4. 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.

8.1.6.1.5. 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.

8.1.6.1.6. 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.

8.1.6.1.7. 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.

8.1.7. Viabilidade financeira:

8.1.7.1. 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.

8.1.7.2. 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:

8.1.7.2.1. 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.

8.1.7.2.2. 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.

8.1.7.2.3. 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.

9. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

9.1. Os detalhes técnicos e operacionais dos itens 3.1, 3.2 e 3.3 estão listados no documento **ETP - ANEXO I**.

10. JUSTIFICATIVA PARA O PARCELAMENTO DO OBJETO

10.1. 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 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

10.2. 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:

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

10.4.2. Permitir que grupos especializados concentrem sua atuação em atividades que

proporcionem maior fluxo de valor à instituição.

10.3. 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).

10.4. 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:

10.4.1. 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.

10.4.2. 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.

10.4.3. 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.

10.4.4. 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.

10.4.5. 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.

10.5. 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.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

11.1. Inexistentes.

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.1. Os valores médios da Pesquisa de mercado e Memória de cálculo citados no item 6 são apresentados na seguinte Tabela.

12.2. 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.

12.3. O custo fixo da contratação é o resultado da soma dos itens com Ids 1, 2 e 3 do VALOR MÉDIO 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.

12.4. As demandas opcionais previstas com IDs 4, 5 e 6 da próxima Tabela contam com o seguinte VALOR MÉDIO 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.

VALORES MÉDIOS			
Item	**Qtd.**	**Valor Unit. Médio**	**Valor Total Médio**
Serviço de gestão de incidentes de segurança (Blue Team).	36	**R$ 88.920,31**	**R$ 3.201.131,07**
Serviço de gestão testes de invasão (Red Team).	36	**R$ 47.177,13**	**R$ 1.698.376,77**
Serviços gerenciados de monitoramento e correlação de eventos usando a ferramenta tecnológica SIEM com 3.000 EPS.	36	**R$ 97.993,58**	**R$ 3.527.768,84**
Objeto	**Qtd Pacotes**	**Valor Unit. Médio**	**Valor Total**
Serviço de contratação de pacotes de 500 EPS da ferramenta SIEM por 12 meses	10	**R$ 11.879,33**	**R$ 118.793,33**

Serviço de contratação de pacotes de 1000 EPS da ferramenta SIEM por 12 meses	10	**R$ 23.051,66**	**R$ 230.516,66**
Serviço de contratação de pacotes de 2000 EPS da ferramenta SIEM por 12 meses	10	**R$ 42.300,00**	**R$ 423.000,00**
Valor Total			**R$ 9.199.586,67**

13. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

13.1. Os estudos preliminares demonstram que a solução descrita é necessária e que a contratação pretendida é viável, pois existem fornecedores no mercado que oferecem regularmente a solução e os serviços necessários para atender às demandas da Administração, seguindo os princípios da economicidade e eficiência da administração pública.

13.2. Além disso, destaca-se que a contratação atende adequadamente às demandas de negócio formuladas, com benefícios adequados, custos compatíveis e economicidade, e com riscos administráveis. Diante dessas informações, conclui-se que a contratação é tecnicamente viável.

14. APROVAÇÃO e ASSINATURA

14.1. Declaramos a viabilidade da contratação, conforme justificativa e os benefícios esperados apresentados neste Estudo Técnico Preliminar, considerando os resultados pretendidos e as metas a serem alcançadas especificadas no Documento de Oficialização da Demanda.

Max Eduardo Vizcarra Melgar – 48994
Integrante Técnico

Heldir Sampaio Silva – 9630
Integrante Requisitante

Denise Maria Norões Olsen – 24667
Autoridade da Área de TIC

Fortaleza, 02 de agosto de 2023.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ETP – 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 4. Dimensionamento de EPS por tipo de equipamento na rede do TJCE.

1.4. A implantação dos serviços contratados.

1.4.1. 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.

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

1.4.2.1 Lotação de todos os profissionais alocados por perfil (com a devida

documentação comprobatória conforme itens 1.3.3, 2.4, 3.4 e 4.8) para os horários de expediente regular e de plantão contínuo.

1.4.2.2 Comprovação da disponibilidade de uso dos recursos te TI descritos no item 1.3.6 para viabilização de imediata prestação de serviços.

1.4.2.3 Relatório técnico produzido através da ferramenta SIEM, comprovando:

1.4.2.3.1 Coleta de logs efetuada pelo Coletor *on-premise*, conforme descrito nos itens 4.1 e 4.3.

1.4.2.3.2 Regras preestabelecidas, normalização e correlação de eventos conforme o item 4.4.

1.4.2.3.3 Capacidade de emitir alertas e notificações conforme item 4.1.

1.4.2.3.4 Ter inicializado o armazenamento de logs conforme item 4.2.19.

1.4.2.3.5 Apresentar o Dashboard em funcionamento conforme os itens 4.2.30, 4.2.31 e 4.2.32.

1.4.2.3.6 Console de administração e operação do SIEM em funcionamento conforme item 4.5.

1.4.3. Após a implantação, o TJCE emitirá um Termo de Recebimento Provisório (TRP) e em até 5 dias úteis validará a implantação. Caso a validação indique pendências de implantação, a CONTRATADA deverá executar as retificações em até 15 dias corridos.

1.4.4. Após a validação sem pendências da implantação, será assinado o Termo de Recebimento Definitivo (TRD) de implantação e, somente a partir desta data, a execução dos serviços será considerada inicializada para finalidade de pagamento, o qual será mensal e sujeito a glosas conforme os itens 1.4.6, Tabela 5. Indicadores de Nível de Serviço e Tabela 6. Glosas por descrição de referências para todos os serviços contratados.

1.4.5. 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.

1.4.6. 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 5. Indicadores de Nível de Serviço e Tabela 6. Glosas por descrição de referências para todos os serviços contratados, conforme os seguintes critérios:

1.4.6.1 Nos primeiros 30 (trinta) dias: não serão aplicadas as glosas previstas em e para cada ocorrência de indicador de serviço não atingido.

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

1.4.6.3 Do 61º ao 90º dia: aplicar-se-á efetivamente 50% (setenta e cinco por cento) dos pontos previstos em e , para cada ocorrência de indicador de serviço não atingido.

1.4.6.4 Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos em e , para cada ocorrência de indicador de serviço não atingido.

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

1.4.7. 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.

1.4.8. O coordenador do SOC, em conjunto com o Blue/Red Team e a equipe de Serviços

gerenciados de monitoramento e correlação de eventos, deve apresentar mensalmente um relatório contendo as atividades executadas pelo SOC, as quais devem ser correlacionadas com as atividades do plano de trabalho. 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.

1.4.9. Um resumo das atividades rotineiras por equipe, unidade de prestação de serviços e frequência de serviços é mostrado na seguinte Tabela. Vale a pena ressaltar que a descrição detalhada dos serviços contratados está nos itens 2, 3 e 4.

Tabela 3. Resumo das atividades rotineiras por equipe

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

	incidentes.		

1.4.10. 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, 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.

1.4.11. 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 neste anexo.

1.5. 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.

1.6. 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.

1.7. 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.

1.8. 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 2.2 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 (a maioria mostrados na Tabela 4. 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 e prestadores de serviço do TJCE sobre conscientização em Segurança da Informação com duração mínima de 1 hora. Previamente deverá apresentar o plano da aula ou 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 realizada em uma possível 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 (Cross-site 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 5. 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.

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

4.2.33. 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.

4.2.34. 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.

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

4.2.36. 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.

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

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

4.2.39. 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.

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

4.2.41. 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 200 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, 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. 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 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 4. 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 da Tabela 4. 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 4. 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.

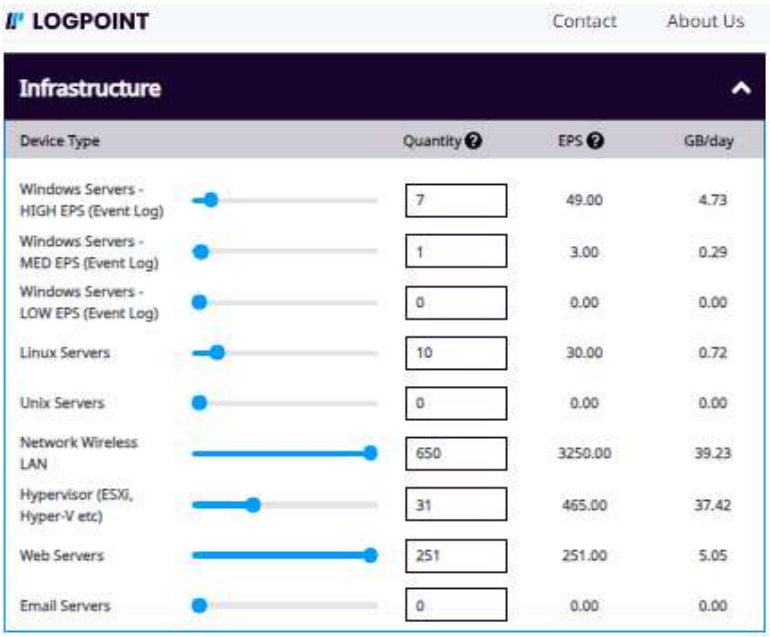
The calculation is based on the number of types of devices (nodes) in your IT infrastructure, which includes servers, routers, switches, firewalls and other network devices and applications.

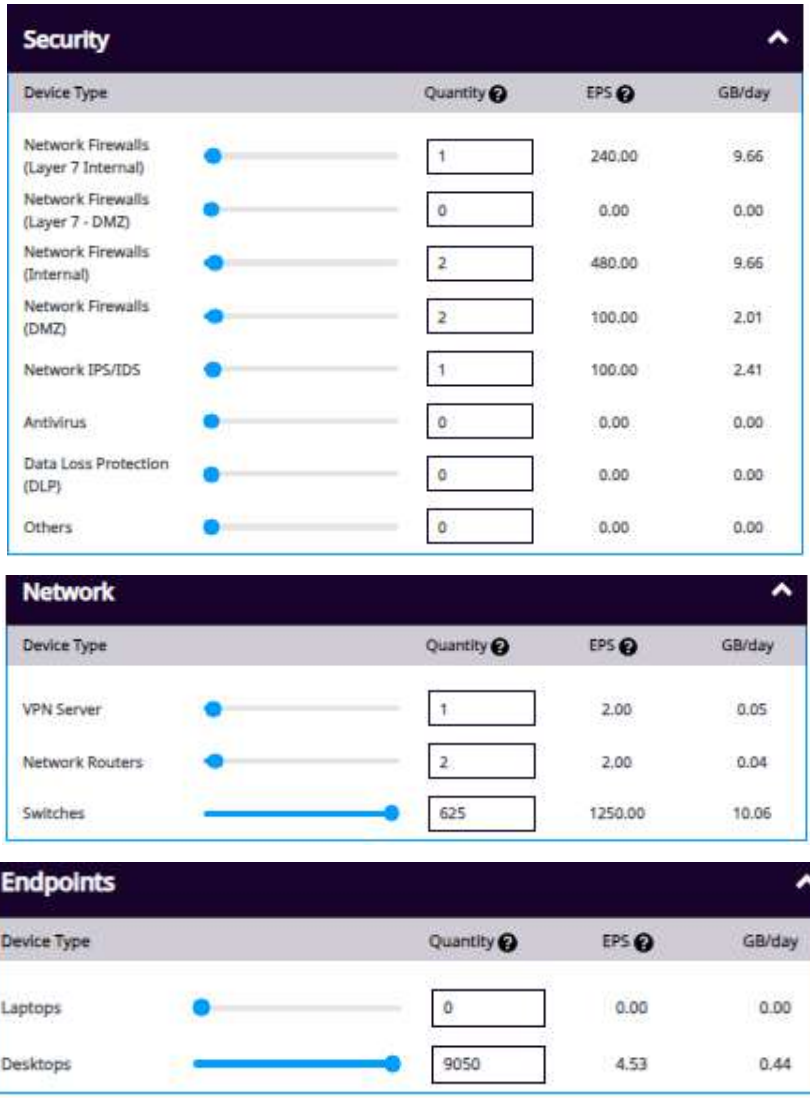
Events Per Second (EPS) define the number of events or processes that take place in a given time on any IT appliance in your IT infrastructure.

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:





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 pode haver ferramentas que diminuam a demanda de EPS (exemplo: EDR ou XDR) e nem todos os ativos de rede 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 4. 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 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.

4.7.11. 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.

4.7.11.1 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.

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

TJCE.

4.7.12. Ocorrência de Incidentes no serviço de monitoramento.

4.7.12.1 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).

4.7.12.2 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.

4.7.12.3 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.

4.7.13. Resposta a incidentes no serviço de monitoramento.

4.7.13.1 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.

4.7.13.2 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.

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

4.7.14.1 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.

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

4.7.15.1 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.

4.7.15.2 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.

4.7.15.3 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.

4.7.15.4 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.

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

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

4.7.15.7 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:

4.7.15.7.1. Coleta de logs.

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

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

4.7.15.7.4. Interação com o fabricante da solução.

4.7.15.7.5. Backup e restore.

4.7.15.7.6. Resolução de problemas.

4.7.15.7.7. Suporte.

4.7.15.7.8. Instalação de serviços relativos ao escopo contratado.

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

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

4.7.15.8 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.

4.7.15.9 A 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.

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

4.7.15.11 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.

4.7.15.12 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.

4.7.15.13 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 ou contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 12 meses.

4.8.2. Deve contar com a certificação oficial 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 ou diploma 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 5. Indicadores de Nível de Serviço. Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento (pontos) serão cumulativas.

5.4. A CONTRATADA deverá emitir mensalmente, junto ao pedido de pagamento, os relatórios constando indicadores de requisições de serviços, NMS e chamados técnicos abertos, em andamento e encerrados no período, com no mínimo as seguintes informações:

5.4.1. Número do contrato.

5.4.2. Número de acionamento

5.4.3. Descrição da ocorrência.

5.4.4. Severidade.

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

5.4.6. Data e hora de abertura do chamado.

5.4.7. Data e hora do início do atendimento.

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

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

5.4.10. Descrição da resolução adotada.

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

5.6. A empresa contratada é responsável por manter os padrões de qualidade estabelecidos para a prestação dos serviços, conforme Tabela 5. Indicadores de Nível de Serviço e

Tabela 6. Glosas por descrição de referências para todos os serviços contratados.

5.7. 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%.

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

5.9. 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 os 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 os horários até a sua solução.

5.10. 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.

5.11. 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 5. 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 a incidentes críticos de disponibilidade que estão sendo solucionados por outras equipes e em horário de expediente regular.	Tempo = (Hora da solicitação de acompanhamento) – (Hora de resposta da solicitação)	<= 15 minutos	10 pontos (+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	Tempo = (Hora de conclusão do planejamento da requisição de mudança) – (Hora de disponibilização dos patches e hotfixes ou divulgação de	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)

		grave vulnerabilidade ou ameaça emergente.	grave vulnerabilidade ou ameaça emergente)		
	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 incidentes de segurança de gravidade alta e em horário de expediente regular.	Tempo = (Hora do início da resposta) – (Hora da triagem)	<= 60 minutos	10 pontos (+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 6. 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	Por ocorrência	10 pontos

	particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo TJCE.		
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

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

MAPA DE GERENCIAMENTO DE RISCOS

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

1. INTRODUCÃO

O Tribunal de Justiça do Estado do Ceará reconhece a importância fundamental da segurança da informação na proteção de seus ativos e no cumprimento de suas obrigações legais e institucionais. Com o objetivo de fortalecer suas defesas e promover a mitigação de riscos cibernéticos, o Tribunal está em busca de um fornecedor de Serviço de Operação e Gerenciamento de Segurança (SOC - Security Operations Center).

Este documento faz parte do processo de elaboração do edital para a contratação dos serviços de SOC, que englobam a gestão de incidentes de segurança (Blue Team), os testes de invasão (Red Team) e o monitoramento e correlação de eventos de segurança da informação com uma ferramenta SIEM.

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual. O mapa de gerenciamento de riscos permitirá uma análise sistemática dos perigos potenciais, considerando ameaças internas e externas, vulnerabilidades existentes e o impacto que cada risco pode ter nas operações do Tribunal. Com base nessa análise, serão propostas medidas de segurança adequadas e eficazes para minimizar os riscos e aumentar a resiliência do ambiente de TI.

É essencial destacar que este mapa de gerenciamento de riscos será uma ferramenta contínua e dinâmica, sujeita a revisões e atualizações periódicas para refletir as mudanças no cenário de ameaças e as evoluções tecnológicas. A tabela mostrada abaixo apresenta as métricas de classificação que serão utilizadas para o diagnóstico do grau ou nível de risco para cada risco identificado:

Classificação	*Valor*
Muito Baixo	*1*
Baixo	*2*
Médio	*3*
Alto	*4*
Muito Alto	*5*

A tabela acima apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Matriz de exposição aos riscos						
		Impacto				
		1	2	3	4	5
Probabilidade	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

Id	Risco	Relacionado ao(à): [1]	P [2]	I [3]	Nível de Risco (P x I) [4]
R01	Problemas no processo de licitação para contratação de serviço de TI	Planejamento da Contratação	5	4	20
R02	Falha na caracterização do objeto	Gestão Contratual e Solução Tecnológica	1	5	5
R03	Falha na justificativa para escolha da solução	Planejamento da Contratação	1	5	5
R04	Restrição à competitividade	Seleção do Fornecedor	1	4	4
R05	Falha na pesquisa de preços	Planejamento da	1	4	4

		Contratação			
R06	Impugnações ou interposição de recurso	Seleção do Fornecedor	4	2	8
R07	Interrupção da execução ou rescisão do contrato	Gestão Contratual e Solução Tecnológica	2	5	10
R08	Falta de pessoal técnico competente para fiscalização do contrato	Gestão Contratual	1	5	5
R09	Prestação de serviço por profissionais inexperientes ou sem conhecimento técnico adequado	Gestão Contratual	3	4	12
R10	Não atendimento dos Níveis Mínimos de Serviços	Gestão Contratual e Solução Tecnológica	2	4	8
R11	Falha na estimativa de volume de serviços	Gestão Contratual	4	4	16
R12	Contingenciamento orçamentário	Gestão Contratual	1	4	4
R13	Descumprimento de cláusulas contratuais pela Contratada	Gestão Contratual e Solução Tecnológica	2	4	8
R14	Irregularidade no cumprimento de questões trabalhistas	Gestão Contratual	2	3	6
R15	Risco de dependência excessiva do fornecedor (*vendor lock-in*).	Gestão Contratual e Execução dos serviços	2	3	6
R16	Problemas de integração e compatibilidade de sistemas entre o serviço contratado e o parque tecnológico do TJCE.	Execução dos serviços	3	5	15

3. AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Risco 01	**Risco:**	Problemas no processo de licitação para contratação de serviço de TI.	
	Probabilidade:	Muito alto	
	Impacto:	Alto	
	Dano 1:	Atraso na contratação e consequente indisponibilidade de serviço por falta de manutenção em funcionalidades, comprometendo a capacidade detecção e resposta a incidentes.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**

	1	Acompanhamento do cronograma, revisão e gestão das mudanças nos documentos de planejamento da contratação, visando garantir o cumprimento dos prazos.	Equipe de Planejamento da Contratação
	2	Produzir os documentos de planejamento da contratação em conformidade rigorosa com a legislação e os normativos complementares.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Dedicação prioritária da equipe de planejamento para minimizar os impactos.	Equipe de Planejamento da Contratação
	2	Solicitar novos prazos ao demandante com a devida justificativa.	Equipe de Planejamento da Contratação

Risco 02	**Risco:**	Falha na caracterização do objeto a ser contratado.	
	Probabilidade:	Muito baixo	
	Impacto:	Muito alto	
	Dano 1:	Não atendimento das necessidades da contratação.	
	Dano 2:	Rescisão contratual.	
	Dano 3:	Descontinuidade dos Serviços.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Alinhar os requisitos técnicos às necessidades do negócio e aos objetivos da contratação.	Equipe de Planejamento da Contratação
	2	Verificar se os artefatos de planejamento da contratação atendem às necessidades e objetivos propostos.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Ajustar os artefatos de planejamento da contratação a fim de solucionar as falhas identificadas.	Equipe de Planejamento da Contratação
	2	Detalhar minuciosamente as características do objeto da contratação para aperfeiçoar a elaboração dos documentos de planejamento.	Equipe de Planejamento da Contratação

Risco 03	**Risco:**	Falha na justificativa para escolha da solução
	Probabilidade:	Muito baixo
	Impacto:	Muito alto

	Dano 1:	Não atendimento ao princípio da motivação dos atos administrativos.	
	Dano 2:	Impossibilidade de contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Alinhar as necessidades da contratação ao justificar a exigência dos requisitos técnicos, especialmente quando resultarem em redução da competitividade no processo de seleção do fornecedor.	Equipe de Planejamento da Contratação
	2	Verificar se os requisitos exigidos são estritamente necessários e justificáveis para atender às expectativas da proposta de contratação.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Apresentar justificativa da necessidade perante órgãos de controle.	Equipe de Planejamento da Contratação
	2	Melhorar a elaboração dos documentos de planejamento da contratação, solicitando somente os requisitos estritamente necessários e justificáveis para atender às expectativas da contratação proposta.	Equipe de Planejamento da Contratação

Risco 04	**Risco:**	Restrição à competitividade	
	Probabilidade:	Muito baixo	
	Impacto:	Alto	
	Dano 1:	Valores de contratação não realistas.	
	Dano 2:	Suspensão da contratação.	
	Dano 3:	Direcionamento indevido do objeto.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Garantir que sejam evitados a inclusão de requisitos excessivos e restritivos à competitividade, focando apenas nos requisitos estritamente necessários para atender ao objetivo da contratação.	Equipe de Planejamento da Contratação
	2	Verificar se os requisitos exigidos são estritamente necessários e justificáveis para atender às expectativas da contratação proposta.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Supressão dos critérios restritivos.	Equipe de Planejamento da Contratação
	2	Melhorar a elaboração dos documentos de	Equipe de

		planejamento da contratação ao exigir somente os requisitos estritamente necessários e justificáveis para atender às expectativas da proposta de contratação.	Planejamento da Contratação

Risco 05	**Risco:**	Falha na pesquisa de preços	
	Probabilidade:	Muito baixo	
	Impacto:	Alto	
	Dano 1:	Elevação dos preços ou inexequibilidade das propostas.	
	Dano 2:	Impossibilidade de contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Executar os procedimentos para a realização de pesquisa de preços seguindo as orientações da lei 14.133 e Resolução de contratações do CNJ.	Equipe de Planejamento da Contratação
	2	Expandir a pesquisa de preços, não limitando-se a apenas três propostas.	Equipe de Planejamento da Contratação
	3	Verificar se os procedimentos adotados estão em conformidade com os requisitos normativos.	Equipe de Planejamento da Contratação
	4	Considerar os questionamentos das empresas concorrentes.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Seguir os procedimentos da lei 14.133 e Resolução de contratações do CNJ, ao refazer a pesquisa de preços.	Equipe de Planejamento da Contratação

Risco 06	**Risco:**	Impugnações ou interposições de recursos.	
	Probabilidade:	Alto	
	Impacto:	Baixo	
	Dano 1:	Atraso no processo de contratação.	
	Dano 2:	Suspensão da contratação.	
	Dano 3:	Impossibilidade de contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Revisar e elaborar criteriosamente os artefatos de planejamento da contratação de acordo com os normativos vigentes.	Equipe de Planejamento da Contratação

	2	Realizar e avaliar os ajustes recomendados pela Consultoria Jurídica a fim de sanar inconformidades dos documentos de planejamento da contratação com a legislação vigente.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Buscar nos repositórios legais e jurisprudenciais os elementos de sustentação das opções adotadas para a contratação, empenhando-se no atendimento aos pedidos de esclarecimento.	Equipe de Planejamento da Contratação
	2	Revisar a elaboração dos documentos de planejamento da contratação com estrita observância à legislação e normativos complementares.	Equipe de Planejamento da Contratação

Risco 07	**Risco:**	Interrupção da execução ou rescisão do contrato	
	Probabilidade:	Baixo	
	Impacto:	Alto	
	Dano 1:	Comprometimento dos serviços de detecção e resposta a incidentes	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar criteriosamente a execução dos serviços, assegurando o cumprimento dos requisitos de qualidade exigidos e identificando problemas de execução em sua origem, a fim de evitar maiores impactos no contrato.	Fiscal Técnico
	2	Verificar se os serviços prestados satisfazem as expectativas da contratação.	Fiscal Técnico e Gestor do Contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Recomeçar o processo de contratação, empregando os artefatos de planejamento produzidos, com as atualizações fundamentadas na infraestrutura e experiência obtida no processo de gestão e fiscalização.	Área demandante e Gestor do Contrato

Risco 08	**Risco:**	Falta de pessoal técnico competente para fiscalização do contrato
	Probabilidade:	Muito baixo
	Impacto:	Muito alto
	Dano 1:	Deficiência na fiscalização do contrato com comprometimento na aferição dos níveis de serviço.
	Dano 2:	Baixa qualidade nas entregas dos serviços.

	Dano 3:	Não atendimento das expectativas da contratação.	
	Dano 4:	Atrasos no pagamento, pagamento indevido e sem o devido desconto das glosas.	
	Dano 5:	Inexecução parcial ou total do contrato.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Utilizar indicadores de fácil mensuração e que possam ser monitorados por meio da ferramenta de gestão de serviços de TIC.	Equipe de Planejamento da Contratação
	2	Prever Plano de Fiscalização, descrevendo como realizará a fiscalização dos contratos, incluindo modelos de planilhas de aferição e listas de verificação.	Equipe de Planejamento da Contratação
	3	Verificar se há servidores com habilidades e competências adequadas em TIC e em quantidade suficiente para atuar na fiscalização dos serviços contratados e medir sistematicamente os indicadores e a qualidade dos serviços.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Priorizar a demanda de atividades críticas que envolvam a disponibilidade do ambiente tecnológico.	Fiscal Técnico

Risco 09	**Risco:**	Prestação de serviço por profissionais inexperientes ou sem conhecimento técnico adequado	
	Probabilidade:	Médio	
	Impacto:	Alto	
	Dano 1:	Baixa qualidade nas entregas dos serviços.	
	Dano 2:	Atraso na entrega dos serviços.	
	Dano 3:	Indisponibilidade de serviços de monitoramento, detecção e resposta a incidentes.	
	Dano 4:	Descumprimento dos requisitos contratuais.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Adequar requisitos de qualificação técnica e experiência profissional conforme a complexidade de cada tipo de serviço.	Equipe de Planejamento da Contratação
	2	Verificar o cumprimento dos requisitos de qualificação técnica e experiência profissional exigidos por meio da fiscalização.	Fiscal técnico e Gestor do Contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Notificar formalmente a Contratada quando os requisitos do contrato não forem cumpridos.	Fiscal técnico e Gestor do Contrato

	2	Coibir a reincidência através da aplicação de glosas e penalidades previstas no instrumento convocatório.	Fiscal técnico e Gestor do Contrato

Risco 10	**Risco:**	Não atendimento dos Níveis Mínimos de Serviços	
	Probabilidade:	Baixo	
	Impacto:	Alto	
	Dano 1:	Não atendimento aos requisitos de negócio.	
	Dano 2:	Ineficiência e não efetividade da contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Estabelecer penalidades pelo descumprimento dos Níveis Mínimos de Serviços.	Fiscal técnico e Gestor do Contrato
	2	Monitorar e controlar proativamente a qualidade dos serviços por meio de estabelecimento de meios.	Fiscal técnico
	3	Intervir ativamente e de forma contínua na aferição da qualidade dos serviços executados, corrigindo os desvios identificados.	Fiscal técnico
	Id	**Ação de Contingência**	**Responsável**
	1	Executar as intervenções que se fizerem necessárias para o reestabelecimento imediato do atendimento e dos serviços.	Fiscal técnico
	2	Revisar o cumprimento das cláusulas do contrato, notificando formalmente a contratada quando forem descumpridas ou violadas.	Fiscal técnico e Gestor do Contrato
	3	Coibir a reincidência através da aplicação de glosas e penalidades previstas no instrumento convocatório.	Fiscal técnico e Gestor do Contrato

Risco 11	**Risco:**	Falha na estimativa de volume de serviços	
	Probabilidade:	Alto	
	Impacto:	Alto	
	Dano 1:	Não atendimento das expectativas da contratação.	
	Dano 2:	Superdimensionamento ou subdimensionamento do contrato.	
	Dano 3:	Contratação antieconômica e sobrepreço.	
	Dano 4:	Rescisão contratual.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**

	1	Para serviços profissionais, estimar o volume previsto realizando o levantamento do volume de serviços executados em outros órgãos.	Equipe de Planejamento da Contratação
	2	Para serviços que usem ferramentas tecnológicas (SIEM), estimar o volume usando aplicações de estimativa (planilhas e sites).	Equipe de Planejamento da Contratação
	3	Elaboração minuciosa da memória de cálculo.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Solicitar a adição ou supressão contratual através de aditivo.	Fiscal técnico e Gestor do Contrato
	2	Elaborar, caso seja negada a continuidade da contratação, um documento de oficialização da demanda para instituir uma nova equipe de planejamento da contratação e realizar uma nova contratação.	Fiscal técnico e Gestor do Contrato

Risco 12	**Risco:**	Contingenciamento orçamentário	
	Probabilidade:	Muito baixo	
	Impacto:	Alto	
	Dano 1:	Descontinuidade dos serviços.	
	Dano 2:	Redução da qualidade dos serviços entregues.	
	Tratamento:	Aceitar	
	Id	**Ação Preventiva**	**Responsável**
	1	Explorar outras alternativas de orçamento para efetuar a contratação.	Equipe de Planejamento da Contratação
	2	Apresentar a necessidade e a relevância do contrato para manutenção e sustentação dos serviços de TIC suportados e custodiados contratados.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Apresentar de forma clara à alta gestão a importância da contratação.	Fiscal técnico e Gestor do Contrato
	2	Identifique os pontos que causarão menor impacto caso sejam suprimidos, caso seja extremamente necessário o contingenciamento no contrato.	Fiscal técnico

Risco 13	**Risco:**	Descumprimento de cláusulas contratuais pela Contratada
	Probabilidade:	Baixo
	Impacto:	Alto

	Dano 1:	Não entrega dos serviços.	
	Dano 2:	Atraso na entrega dos serviços.	
	Dano 3:	Baixa qualidade dos serviços entregues.	
	Dano 4:	Descontinuidade dos serviços.	
	Dano 5:	Falta de efetividade da contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar a execução dos serviços, assegurando se os requisitos exigidos no contrato estão sendo cumpridos de acordo com a qualidade exigida.	Fiscal técnico
	2	Verificar se os serviços prestados satisfazem as expectativas da contratação.	Fiscal técnico
	3	Adequar o dimensionamento do corpo de fiscalização e gestão contratual.	Fiscal técnico
	4	Aprimorar a capacitação da equipe de fiscalização e gestão contratual.	Fiscal técnico
	5	Fiscalizar e gerir contratos de forma intensificada.	Fiscal técnico
	Id	**Ação de Contingência**	**Responsável**
	1	Informar devidamente a contratada quando cláusulas do contrato forem descumpridas.	Fiscal técnico e Gestor do Contrato
	2	Coibir a reincidência, aplicando glosas e penalidades previstas no instrumento convocatório.	Fiscal técnico e Gestor do Contrato
	3	Promover uma nova contratação e instituir uma equipe de planejamento da contratação, a fim de evitar o comprometimento da continuidade dos serviços do TJCE, caso as inconformidades não possam ser resolvidas.	Área demandante e Gestor do Contrato

Risco 14	**Risco:**	Irregularidade no cumprimento de questões trabalhistas	
	Probabilidade:	Baixo	
	Impacto:	Médio	
	Dano 1:	Desmotivação dos profissionais prestadores de serviços	
	Dano 2:	Aumento da rotatividade dos profissionais.	
	Dano 3:	Baixa qualidade dos serviços entregues.	
	Dano 4:	Corresponsabilização de equipe de gestão e fiscalização.	
	Dano 5:	Descontinuidade dos serviços.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**

	1	Verificar a elaboração da lista que deverá ser observada pela fiscalização administrativa durante a execução do contrato.	Fiscal técnico
	2	Verificar o cumprimento das obrigações trabalhistas conforme legislação vigente.	Fiscal técnico
	Id	**Ação de Contingência**	**Responsável**
	1	Identificar irregularidades trabalhistas e notificar formalmente a Contratada.	Fiscal técnico e Gestor do Contrato
	2	Executar glosas e penalidades previstas no instrumento convocatório.	Fiscal técnico e Gestor do Contrato

Risco 15	**Risco:**	Risco de dependência excessiva do fornecedor (*vendor lock-in*).	
	Probabilidade:	Baixo	
	Impacto:	Médio	
	Dano 1:	Dificuldade de troca de fornecedor	
	Dano 2:	Descontinuidade dos serviços.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**
	1	Estabelecer critérios claros para uma seleção de tecnologia oferecida por muitas empresas	Equipe de Planejamento da Contratação
	2	Realizar estudo das tecnologias existentes.	Equipe de Planejamento da Contratação
	3	Realizar estudo de mercado com múltiplas empresas.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Estabelecer o uso de funcionalidades padronizadas e presentes nas ferramentas tecnológicas.	Fiscal técnico

Risco 16	**Risco:**	Problemas de integração e compatibilidade de sistemas entre o serviço contratado e o parque tecnológico do TJCE.	
	Probabilidade:	Médio	
	Impacto:	Muito alto	
	Dano 1:	Descontinuidade dos serviços.	
	Dano 2:	Baixa qualidade dos serviços entregues.	
	Dano 3:	Não entrega dos serviços.	
	Dano 4:	Falta de efetividade da contratação.	
	Tratamento:	Mitigar	
	Id	**Ação Preventiva**	**Responsável**

	1	Realizar uma análise detalhada dos requisitos de integração e compatibilidade durante a fase de planejamento da contratação, identificando possíveis conflitos e lacunas.	Equipe de Planejamento da Contratação
	2	Estabelecer critérios claros de compatibilidade técnica e interoperabilidade nos termos do contrato, garantindo que o serviço contratado seja compatível com o parque tecnológico do TJCE.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Manter uma comunicação aberta e constante com a equipe responsável pelo parque tecnológico do TJCE, para identificar rapidamente qualquer problema de integração e buscar soluções em conjunto.	Fiscal técnico
	2	Identificar rapidamente problemas de compatibilidade entre as ferramentas tecnológicas contratadas e o parque tecnológico do TJCE para implementar soluções.	Fiscal técnico

4. ACOMPANHAMENTO DAS AÇÕES DE TRATAMENTO DE RISCOS

Data	Id. Risco	Id. Ação	Registro e acompanhamento das ações de tratamento dos riscos
16/03/2023 a Atualmente	R01, R02 e R03	P01	Dedicação prioritária do Integrante Técnico para elaboração do DOD. ETP, MGR, PSU e TRF.
20/04/2023	R01, R02 e R03	P02	Envio da primeira versão do DOD.
27/04/2023	R01, R02 e R03	P03	Envio da primeira final do DOD.
12/06/2023	R01, R02 e R03	P04	Envio da primeira versão do ETP.
27/03/2023	R01, R02, R03, R04, R05 e R16	P05	Reunião de projeto SOC com a empresa Network Secure.
13/04/2023	R01, R02, R03, R04, R05 e R16	P06	Reunião de projeto SOC com a empresa Decatron.
14/04/2023	R01, R02, R03, R04, R05 e R16	P07	Reunião de projeto SOC com a empresa QOS Tecnologia.
26/04/2023	R01, R02, R03 e R11	P08	Reunião de projeto SOC com a Gartner para tirar dúvidas da caracterização do objeto e escolha da solução.
26/04/2023	R01, R02, R03, R04, R05 e R16	P09	Reunião de projeto SOC com a empresa Oi Soluções.
08/05/2023	R01, R02, R03, R04,	P11	Reunião de projeto SOC com a empresa Fortinet.

	R05 e R16		
08/05/2023	R01, R02, R03, R04, R05 e R16	P12	Reunião de projeto SOC com a empresa Fortinet.
10/05/2023	R01, R02, R03, R05 e R11	P13	Reunião interna para preenchimento de planilha de dimensionamento.
15/05/2023	R01, R02, R03, R04, R05 e R16	P14	Reunião de projeto SOC com a empresa Network Secure.
16/05/2023	R01, R02, R03, R04, R05 e R16	P15	Reunião de projeto SOC com a empresa NTSec.
17/05/2023	R01, R02, R03, R04, R05 e R16	P16	Reunião de projeto SOC com a empresa TrendMicro.
17/05/2023	R01, R02, R03, R04, R05 e R16	P17	Reunião de projeto SOC com a empresa Viwsec.
18/05/2023	R01, R02, R03, R04, R05, R11 e R16	P18	Reunião de projeto SOC com a empresa QOS Tecnologia – Dimensionamento.
19/05/2023	R01 e R05	P19	Reunião de projeto SOC com Cristiano e Heldir (TJCE).
20/05/2023	R01, R02, R03, R04, R05, R11 e R16	P20	Reunião de projeto SOC com a empresa Decatron – Dimensionamento.
20/05/2023	R01, R02, R03, R04, R05, R11 e R16	P21	Reunião de projeto SOC com a empresa Oi – Dimensionamento.
25/05/2023	R01, R02, R03, R04, R05 e R16	P22	Reunião de projeto SOC com a empresa Lanlink.
25/05/2023	R01, R02, R03, R04, R05, R11 e R16	P23	Reunião de projeto SOC com a empresa Network Secure – Dimensionamento.
30/05/2023	R01, R02, R03, R04, R05 e R16	P24	Reunião de projeto SOC com a empresa Stefanini.
30/05/2023	R01, R02, R03, R05, R08, R11, R14	P25	Reunião interna para verificação da modalidade de contratação via UST e USTD com George Pereira.
31/05/2023	R01, R02, R03, R05, R08, R11, R14	P26	Reunião interna para verificação da modalidade de contratação de mão de obra com Francisco Moacir Medeiros.

02/06/2023	R01, R02, R03, R04, R05 e R16	P27	Reunião de projeto SOC com a empresa Embratel.
07/06/2023	R01, R02, R03, R04, R05, R11 e R16	P28	Reunião de projeto SOC com a empresa NTSec – Dimensionamento.
12/06/2023	R01, R02, R03, R05 e R11	P29	Reunião com Heldir para o fechamento da primeira versão do ETP.
15/06/2023	R01, R02, R03, R04, R05, R11 e R16	P30	Reunião de projeto SOC com a empresa Stefanini – Dimensionamento e proposta comercial.
16/06/2023	R01, R02, R03, R05 e R11	P31	Reunião com Heldir para apresentação das correções do ETP solicitadas pelo Moacir.
20/06/2023	R01, R02, R03, R05 e R11	P32	Reunião com Heldir e Moacir para validação das correções do ETP solicitadas pelo Moacir.
21/06/2023	R01, R02, R03 e R11	P33	Reunião com Heldir e Ederley da Silva para validação do uso do ITSM Assyst no projeto SOC.
04/07/2023	R01, R02, R03, R04, R05, R11 e R16	P34	Reunião com a TrendMicro – Dimensionamento e proposta comercial.
07/07/2023	R01, R02, R03, R04, R05, R06, R07, R10, R11, R13 e R16	P35	Reunião com a Network Secure e com a IBM para dimensionamento e proposta comercial.
17/07/2023	R01, R02, R03, R04, R05, R06, R07, R10, R11, R13 e R16	P36	Reunião com a Gartner dos Estados Unidos contendo o Feedback deles da documentação técnica contida no ETP. O Feedback conteve elogios da documentação técnica completa e com projeto pronto para ser licitado.
24/07/2023	R01, R02, R03, R04, R05, R06, R07, R10, R11, R13 e R16	P37	Reunião com a Davi para esclarecer quantidade de EPS, possibilidade de divisão do Lote único e referenciar o edital do MPSP.
26/07/2023	R01, R02, R03, R04, R05, R11 e R16	P38	Reunião com a ServiceIT – Dimensionamento e proposta comercial.
26/07/2023	R01, R02, R03, R04, R05, R11 e	P39	Reunião com a ESY – AT&T – Dimensionamento e proposta comercial. Eles não contam com SIEM, contam com outra ferramenta XDR com arquitetura diferente de

	R16		EPS, coletor e funcionamento
02/08/2023	R01, R02, R03, R04, R05, R11 e R16	P40	Reunião com a IBM – Dimensionamento e proposta comercial.
30/08/2023	R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15 e R16	P41	Aprovação da documentação por parte do BID (Santiago Paz).
05/09/2023	R01, R02, R03, R05, R06, R14.	P42	Reunião com Elaine da CONJUR do TJCE para tirar dúvidas das observações da documentação.

5. APROVAÇÃO E ASSINATURA		
Max Eduardo Vizcarra Melgar - 48994 Integrante Técnico	Heldir Sampaio Silva – 9630 Integrante Demandante	Fábio de Carvalho Leite – 9594 Integrante Administrativo
Fortaleza, 7 de outubro de 2023.		