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.