TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ

SG-STI-CGP-DSEG - DIVISÃO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DA COORDENADORIA DE GESTÃO DIGITAL E PLANEJAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Nº SEI!TJPR 0090885-81.2023.8.16.6000
Nº SEI-DOC 12398584

À SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ESTUDO TÉCNICO PRELIMINAR DE STIC

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1 NECESSIDADE

No mundo moderno, onde a dependência da tecnologia e da internet é cada vez maior, os ataques cibernéticos se tornaram uma das maiores ameaças às instituições, inclusive as governamentais. Esses ataques estão evoluindo em sofisticação e frequência, trazendo riscos iminentes que podem comprometer a segurança, a privacidade e a integridade das informações e dos serviços prestados.

Os ataques cibernéticos não são mais incidentes isolados realizados por indivíduos solitários. Eles evoluíram para operações organizadas e altamente sofisticadas, muitas vezes patrocinadas por estados ou por redes criminosas internacionais. Essas operações têm como alvo infraestruturas críticas, dados financeiros, informações pessoais e outros ativos valiosos.

As instituições governamentais estão entre os alvos preferidos dos hackers devido à sensibilidade e à criticidade dos dados que armazenam e dos serviços que prestam. Ataques bem-sucedidos podem resultar em vazamento de informações confidenciais, interrupção de serviços essenciais e até mesmo comprometer a segurança nacional. Exemplos recentes incluem ataques ao Supremo Tribunal Federal, ao Tribunal de Justiça do Estado do Rio Grande do Sul, e a outras instituições judiciais brasileiras.

O crescimento dos ataques cibernéticos apresenta riscos iminentes às instituições governamentais de várias maneiras:

- Interrupção de Serviços: Ataques podem paralisar serviços essenciais, como sistemas judiciais e administrativos, causando caos e prejudicando a população.
- Vazamento de Informações: Dados sensíveis podem ser roubados e usados para chantagem, espionagem ou outras atividades ilícitas.

- Perda de Confiança: Falhas na segurança cibernética podem minar a confiança do público nas instituições governamentais e na sua capacidade de proteger informações e prestar serviços.

O crescimento dos ataques cibernéticos representa uma ameaça real e constante às instituições governamentais. É imperativo que essas instituições estejam preparadas para enfrentar e mitigar esses riscos, garantindo a segurança e a continuidade dos serviços que são vitais para a sociedade.

1.2 JUSTIFICATIVA

O Poder Judiciário vem avançando tecnologicamente a cada ano, trazendo mais agilidade aos serviços prestados à sociedade e ampliando o acesso à Justiça. Dessa forma, os ambientes tecnológicos que suportam os serviços, sistemas e infraestrutura de TIC estão se tornando maiores e mais complexos.

Com este cenário, os Tribunais passaram a ser alvos de ataques, riscos, ameaças, e vulnerabilidades que antes não existiam ou não eram exploradas, aumentando a superfície para ataques hackers. Nos últimos anos, diversos Tribunais sofreram ataques, como por exemplo, os ataques ocorridos no Supremo Tribunal Federal (2021), Superior Tribunal de Justiça (2021), Tribunal de Justiça do Estado do Rio Grande do Sul (2021), Tribunal de Justiça do Estado do Amazonas (2021), TRT 4 Região (2021), TRF 3 Região (2022), TRT-ES (2022), Tribunal de Contas do Ceará (2022), Justiça Federal de Pernambuco (2022).

Todos estes fatores e ataques motivaram o CNJ, através de Resoluções, Portarias e Protocolos, a apoiar os órgãos do Judiciário, estabelecendo diretrizes, recomendações e padrões mínimos para proteção da infraestrutura de TIC.

A Resolução Nº 370 de 28/01/2021, estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), onde orientada em seu preâmbulo pelos objetivos dos seguintes componentes:

“Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados”.

A Resolução Nº 396 de 07/06/2021 do CNJ, institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF). Destacam-se o artigo:

"Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

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;

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;

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;

V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos.

XI – realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; "

Além disso, existem demandas trazidas pela Lei Geral de Proteção de Dados - LGPD, através da Lei Nº 13.709 de 14/08/2018. Destacando-se:

“os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

Dessa forma, todos os fatores acima apresentados apontam para que os Tribunais evoluam continuamente na segurança cibernética, proteção de Infraestrutura Críticas de TIC, gerenciamento de risco, gerenciamento de vulnerabilidade, proteção de identidade, continuidade de serviços essenciais, tratamento e resposta a incidentes de segurança, pentest e forense digital.

O Tribunal de Justiça do Paraná utiliza o método de proteção em camadas de segurança, criando várias camadas de proteção distintas e complementares, sendo que cada uma especializada em algum componente de segurança, como por exemplo, segmentação de rede, Firewalls, IPS (*Intrusion Prevention System*), Filtro de conteúdo Web, Análise de Malware, WAF (*Web Application Firewall*), além de normas e procedimentos de segurança. No entanto, o universo de cibersegurança ou segurança cibernética é amplo e complexo. Esta tarefa exige o investimento contínuo em tecnologias, processos e pessoas, além de conhecimento altamente

especializado, atuando em regime de 24x7.

A tarefa de proteção de ativos de informação altamente expostas na Internet se torna árdua, devido à falta de pessoal especializado para proteger os ativos de forma eficaz. De acordo com o estudo da Cybersecurity Workforce Study 2022, realizado pela (ISC)², organização internacional de treinamento e certificações para profissionais de cibersegurança, somente no ano de 2022 o Gap global de mão de obra qualificada na área de segurança cibernética aumentou em 26,2%, elevando o número em torno de 3,4 milhões. Ref. https://www.cisoadvisor.com.br/gap-de-profissionais-de-ciberseguranca-cresce-26-neste-ano/.

Considerando que o mercado de trabalho é muito mais dinâmico em relação ao serviço público, permitindo a contratação de profissionais de forma mais rápida e eficiente, e que já encontra dificuldades para manter as equipes especializadas, muito menos os Tribunais que dependem de concursos públicos para fazer a contratação, licitações para treinamento, entre outras questões. Isso sem considerar as necessidades normativas para atuação de servidores internos em regime de 24x7 com pagamento de horas-extras ou escala de plantão.

Além disso, segundo o Gartner, até o ano de 2025, a falta de profissionais de segurança ou a falha humana será responsável por mais da metade dos incidentes de segurança cibernética. Diante desse cenário complexo, como fazer frente às necessidades de monitoramento e resposta a incidentes no menor tempo possível, administração de soluções de segurança, e acalcar a excelência em segurança da cibernética exigida pelo CNJ, através das resoluções e portarias?

O universo de segurança da informação é complexo e muito amplo. Dessa forma, traz a exigência de conhecimentos especializados, atuação dinâmica e eficaz de equipes, atualização e treinamentos constante, trabalhando de forma orquestrada entre padrões internacionais, normativos do CNJ, Governança do TJPR, processos, pessoas e soluções de segurança.

A solução viável para somar esforços, junto ao TJPR, para ampliar os mecanismos de segurança, aumentar a capacidade de monitoramento, e diminuindo o tempo de resposta a incidentes, esta relacionada com a contratação de uma equipe dedicada ao monitoramento, prevenção e resposta a incidentes de segurança. Partindo dessa percepção, uma equipe de SOC (*Security Operations Center*) é um time centralizado com a função de monitoramento contínuo, análise dessas ameaças, prevenção e mitigação de incidentes de cibersegurança.

A crescente demanda pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais estratégica. A formação de equipes Blue Team e de Red Team são um bom exemplo dessa preocupação. Com atribuições específicas, as equipes promovem um trabalho de cibersegurança em nível técnico elevado. Cada uma delas com sua importância e respectivos benefícios.

O Red Team é um time formado com o objetivo de realizar testes de ciberataque. Composto por profissionais com alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de ataque, penetrando em rede corporativa, infraestrutura e sistemas. Com isso, o Red Team é capaz de identificar vulnerabilidades antes do atacante e, consequentemente, propõem a solução para eliminá-las, trazendo o benefício da atuação preventiva. Em resumo, esta equipe assume o papel do atacante que tentaria atacar a infraestrutura — o que geralmente pode envolver a contratação de pessoas que não trabalham no Tribunal, sem o viés conhecido sobre o ambiente tecnológico. Os ataques podem envolver engenharia social para envio de *phishing* aos funcionários internos, por exemplo.

Por outro lado, o papel do Blue Team é justamente a defesa aos ataques, inclusive aqueles ensaiados ou simulados pelo Red Team. Assim, o Blue Team deve desenvolver estratégias para aumentar os mecanismos de proteção contra-ataques, visando aumentar capacidade de resiliência e de resposta ao incidente. Este time deve também possuir um alto nível de conhecimento sobre a natureza das ameaças cibernéticas.

Podemos extrair o que se entende por Blue Team, Red Team a partir das definições da autoridade mundial no tema, SANs:

"[...] focus is to defend the organization from digital/cyber attacks. In truth, while everything that improves the defensive security posture could be construed as Blue Team, there is an overt emphasis on discovering and defending against attacks". (https://wiki. sans.blue/#!index.md)

"[...] focado em defender a organização de digital/cyber ataques. Na verdade, enquanto tudo que promova a postura defensiva de segurança possa ser entendida como Blue Team, há uma ênfase na descoberta e defesa contra esses ataques. " (Tradução Livre)

"[...] would be those playing the role of the adversary. [...] So Red Team acts as Offense and Blue Team as Defense." (https://wiki.sans.blue/#!index.md)

"[...] serial, aqueles que atuam o papel de adversários. [...] Então o Red Team atua como ofensiva e Blue Tema como defensiva." (Tradução Livre)

De acordo com o modelo de arquitetura de segurança adaptativa proposto pelo Gartner, uma organização somente obterá sucesso na luta contra os crimes cibernéticos se a equipe de SOC for capaz de predizer, prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 1:

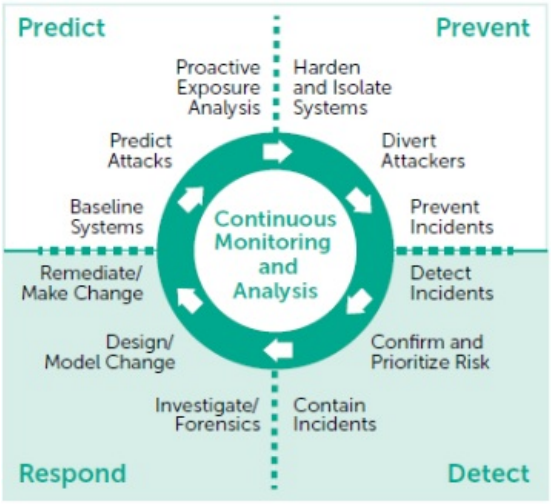

Figura 1 - Gartner, Designing an Adaptive Security Architecture for Protection

Esta contratação objetiva contemplar as equipes de Blue Team, Red Team, de forma 24h por dia e 7 dias por semana e 365 dias por ano para o monitoramento e defesa, através da estrutura de SOC para que se possa **monitorar, analisar, detectar e responder à incidentes de segurança** no ambiente do Tribunal.

A presente contratação permite que um parceiro preste **Serviços Gerenciados de Segurança (*Managed Service Security - MSS*),** permitindo realizar tarefas cotidianas de forma mais ostensiva, com mais eficiência e com custo orçamentário e temporal menor que o próprio Tribunal.

A contratação do SOC objetiva também **aliviar a carga de serviço das equipes de infraestrutura do Tribunal, realizando o gerenciamento e operação das atividades rotineiras de soluções relacionadas a segurança, reduzindo o tempo de resposta** aos incidentes identificados pelo próprio Centro de Operações de Segurança.

Espera-se que a contratação possa agregar junto ao SOC **serviços sob demanda de testes de penetração (*Pentest*), a fim de validar a proteção dos ativos do Data Center do TJPR e avaliar as possíveis fragilidades nos mecanismos de proteção, visando o aperfeiçoamento e melhoria contínua na segurança dos ativos**. Destaca-se que serviços especializados em teste de penetração (*Pentest*) são capazes de prover uma visão detalhada das falhas, vulnerabilidades e possíveis fraquezas eventualmente existentes na infraestrutura de tecnologia, sistemas de informação e aplicações, tais como o Projudi. Desta maneira, é possível atuar de forma proativa nas correções e implantação de controles necessário à mitigação dos riscos de concretização de ataques.

2. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

A presente contratação está prevista no Plano de Contratações de Soluções de TIC para o exercício financeiro de 2025 versão 1.2, devidamente apresentado no expediente administrativo SEI nº 0039457-26.2024.8.16.6000, o qual, foi aprovado pelo Comitê Gestor de Tecnologia da Informação e Comunicação (SEI nº 0033045-60.2016.8.16.6000, Ata 11449185 item 2) e pelo Comitê de Governança de Tecnologia da Informação e Comunicação na 1ª reunião de 2025 (SEI nº 0017736-81.2025.8.16.6000, Ata 11671204 item 6).

A demanda está registrada na categoria licitações no item "SETI-23.2025 SOC - Security Operations Center", sob o valor estimado de R$ 4.000.000,00 (quatro milhões reais) para 2025.

2.1 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA

A demanda está registrada na categoria licitações no item "SETI-23.2025 SOC - Security Operations Center", sob o valor estimado de R$ 4.000.000,00 (quatro milhões reais) para 2025.

Ainda, relativamente à Resolução n.º 195/2014 do CNJ, a distribuição orçamentária para o objeto em questão constará no Plano de Contratações na proporção de 50% para o 1.º Grau e 50% para o 2.º Grau.

2.2 ALINHAMENTO ESTRATÉGICO

2.2.1 PEI - Planejamento Estratégico do Poder Judiciário (PEI 2021 – 2026)

A contratação objeto deste estudo visa atender aos seguintes Objetivos Estratégicos Institucionais, constantes no Plano Estratégico Institucional vigente:

02 – Fortalecimento da Relação Institucional do Judiciário com a Sociedade;

04 – Agilidade e Produtividade na Prestação Jurisdicional;

12 – Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

2.2.2 PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)

A contratação objeto deste estudo visa atender aos seguintes Objetivos Estratégicos, constantes no Plano Diretor de Tecnologia da Informação e Comunicação vigente:

OE.TIC-1: Aprimorar a entrega de serviços e o valor para os clientes internos e externos;

OE.TIC-2: Ampliar mecanismos de Infraestrutura e Segurança da Informação de TIC;

3. REQUISITOS DA CONTRATAÇÃO

Tipo	Requisito (A solução contratada deve...)
	Serviços de Governança e Conformidade de Segurança Identificação de Gaps, diagnóstico e avaliação da maturidade de segurança da informação, analisando processos, normas, políticas, procedimentos, planos, indicadores, métricas, pessoas, papéis, responsabilidades e soluções de segurança existente no Tribunal, considerando alinhamento com normas ISO, frameworks NIST e CIS Control, leis e normativos do CNJ, propondo adequação, melhoria e aperfeiçoamento contínuo durante a vigência da contratação. Alinhamento e aprimoramento do Plano de Continuidade de Serviços Essenciais, Plano de Administração de Crise - PAC, Plano de Recuperação de Desastres - PRD, apoio na elaboração, planejamento e execução de testes, exercícios e simulações. Alinhamento e aprimoramento da Política de Segurança da Informação - PSI, adequando as necessidades do Tribunal, resoluções do CNJ, normas ISO e melhores práticas de Segurança da Informação. Apoio na elaboração, implantação, execução e melhoria contínua de um Plano de Resposta a Incidentes e Processo de Tratamento e Resposta a Incidentes de segurança cibernética, incluindo um plano específico para o gerenciamento de crises cibernéticas. Elaboração, documentação e melhoria contínua de painéis (dashboard) com visão operacional com foco em tecnologia e painéis estratégicos com foco no negócio, além de indicadores de desempenho KPI, apresentação mensal de relatórios do status do ambiente e o respectivo desempenho. Elaboração, documentação e melhoria contínua de métricas, indicadores chave de desempenho (KPI), painéis (dashboards) técnico-operacional (foco em tecnologia) e estratégico-gerencial (foco no negócio) e lições aprendidas, com relatórios mensais de situação e desempenho. Análise, elaboração, documentação, acompanhamento e avaliação de um plano de ação de controles e salvaguardas de segurança cibernética, medidas de remediação e mitigação, planejando ações para aplicação de atualizações de segurança, regras, barreiras e hardening de ativos de TIC, a partir dos resultados dos diagnósticos, análises, testes, eventos e incidentes de segurança, tanto proativos/preventivos (gestão de vulnerabilidades e melhores práticas internacionais) quanto reativos (tratamento de ameaças e incidentes).
	Monitoramento, detecção e resposta a incidentes Centro de Operações de segurança - SOC para monitoramento, detecção, análise, investigação e resposta a incidentes de segurança cibernética em regime 24x7x365, contendo o SOC ao menos 02 centros, sendo 01 principal e outro redundante.

Estabelecer a equipe de tratamento e resposta a incidentes de segurança (ETIR) remotamente, incluindo Nível 1 (fase inicial), Nível 2 (fase avançada e em crises) e Nível 3 (fase especialista).

Elaboração, análise, e melhoria e expansão dos casos de uso de monitoramento e detecção, playbooks de tratamento, resposta e automação.

Realizar os procedimentos cabíveis de análise e investigação forense pós-incidentes, aderentes com Portaria 162 do CNJ de 10/06/2021.

Coordenar as ações de investigação e de comunicação, interna e externa, de forma centralizada, através do responsável/gerente do SOC.

Documentar os incidentes de segurança, registrar os procedimentos e as soluções encontradas para mitigação, lições aprendidas e possíveis necessidades de aperfeiçoamento.

A solução de gerenciamento e seus serviços devem abranger não só o monitoramento, mas a detecção contínua de ameaças e ataques, agregando inteligência de segurança, incluindo análise comportamental de usuários e entidades (user and entity behavioral analysis – UEBA) com inteligência artificial e aprendizado de máquina, identificação autônoma de táticas, técnicas e procedimentos (TTPs) mapeando automaticamente com o framework MITRE ATT&CK;

Gerenciamento de eventos de segurança, através de solução Security Information Event Management - SIEM, incluindo serviços de coleta, consolidação, correlação e análise de logs.

O monitoramento dos ativos deve ser realizado com a capacidade de atender a estimativa de ativos de TIC do TJPR, conforme tabela abaixo:

Item	**Ativo**	**Quantidade**
1	Servidores físicos	80
2	Servidores virtuais	700
3	Estação de trabalho	16.000
4	Notebooks	3.000
5	Impressoras	3.000
6	DNS	4
7	Links de Internet	3
8	Site WAN	215
9	Ativos de rede (switch, roteadores, etc)	1.200
10	VPN	4
11	Serviço de Diretório	6
12	Storages	4
13	Usuários internos	18.000

Para o licenciamento da solução de monitoramento há no mercado algumas opções de contratação. A primeira opção é licenciada por ativo protegido ou monitorado, além disso, o mercado dispõe das opções de eventos por segundo (EPS) e volumetria.

Negócio	Devido à complexidade e diversidade tecnológica do ambiente do Tribunal com um número estimado de 25.000 (vinte e cinco mil) ativos a serem monitorados, a equipe técnica da SETI optou realizar a contratação da modalidade de licenciamento da solução de monitoramento por ativo. Trata-se da primeira contratação desse porte no Tribunal, uma vez que não há um estudo para demonstrar a quantidade de eventos por segundo gerado pelos ativos de TIC e cada solução contém diferentes tipos de filtros que podem otimizar a quantidade de eventos processados. Por outro lado, a contratação por EPS (Eventos Por Segundo) pode gerar prejuízo ao Tribunal, caso os eventos de segurança por segundo possam ser superestimados ou subestimadas, levando a contratação possuir um mais elevado que o necessário ou não atender as demandas do projeto. Além disso, ao realizar a contratação através de ativos a empresa terá autonomia de projetar os estudos para melhor otimização do custo e benefício para atender o projeto, de acordo com a solução ofertada. No entanto, para que haja ampla participação na disputa e com base no exemplo de contratação de outros órgãos como, por exemplo, TRT17, conforme TR SEI 0001056-58.2022.5.17.0500, para soluções cuja subscrição seja baseada em EPS (Eventos Por Segundo), a empresa deve licenciar a solução para uma quantidade mínima de EPS suficiente para atender 100% dos ativos do Tribunal e garantir a escalabilidade da solução, independentemente da quantidade de EPS gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de EPS igual a 2 vezes por ano a referida quantidade de ativos monitorados. A empresa deverá aferir mensalmente o consumo de EPS e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para o Tribunal. Triagem, análise, investigação, threat hunting, threat research e inteligência de ameaças (threat intelligence) estratégica, tática e operacional, e validação, identificando atividades anômalas e, dentre essas, candidatos a incidentes, além da triagem, tratamento, priorização e categorização de incidentes de segurança. Monitoramento e Detecção de Resposta de Rede (Network Detection and Response - NDR). Orquestração, Automação e Resposta, através de solução Security Orchestration, Automation and Response - SOAR, licenciada pela empresa Contratada, sendo do mesmo fabricante do SIEM ou com homologação comprovada pelo fabricante, quando houver. Além da capacidade de integrar, consolidar, agregar e correlacionar informações provenientes de outras fontes de telemetria a ativos de TIC e soluções de segurança do Tribunal. Monitoramento de proteção da marca e da reputação institucional na internet, na deep web e na dark web, incluindo redes sociais, repositórios de informação e lojas de aplicativos, identificando fraudes e golpes, operações se passando como legítimas em nome do Tribunal, conteúdo malicioso, vazamentos de dados e ameaças externas, com capacidade de realizar takedown em nome do Tribunal mediante procuração e autorização.
	Do Monitoramento **Marca**: Tribunal de Justiça do Estado do Paraná, Tribunal de Justiça do Paraná, Poder Judiciário do Paraná, TJPR, TJ-PR, TJ/PR; **Domínios**: tjpr.jus.br, tjpr.net, incluindo subdomínios (www, projudi, sei, mail, webmail, entre outros); **Perfis**: Youtube @TJPRoficial | @TJPR - Sessões, Instagram: @tjproficial | @2vicetjpr | @tjpr1vice e X (antigo Twitter):@TJPRoficial; As fontes de monitoramento devem incluir: Registros de domínios nacionais e internacionais, incluindo TLDs e gTLDs; Sites na internet, deep web e na dark web; Grupos, canais e comunidades em serviços de comunicação por mensagens e fóruns: WhatsApp, Telegram, Signal, Discord, Reddit; Repositórios e serviços de conteúdo e informação de grande abrangência: Github, Scribd, Reclame Aqui; Lojas de aplicativos (catálogo ou repositório de distribuição de software instalável para

determinada plataforma de sistema operacional): Microsoft Store (Windows), Google Play (Android), Apple App Store (iOS/iPadOS), Samsung Galaxy Store (Android), Amazon Appstore (Android), F-Droid (Android);

O serviço de monitoramento deve identificar:

Fraudes, phishing, leilões e outros tipos de golpes, conteúdo malicioso e ameaças relacionadas, réplicas, conteúdos ilegítimos, abusos e violações aos serviços utilizando nome, marca e/ou identidade visual institucionais do Tribunal.

Identificação de variação de nomes ou domínio, incluindo permutação de caracteres.

Vazamento de dados e informações sensíveis da instituição.

Monitoramento de ameaças globais e com foco em Brasil, Governo e Judiciário.

Sustentação de Operações de Soluções e Resposta a Requisições de Segurança

Serviço contínuo e proativo para sustentação, administração, operação, suporte técnicos das soluções de segurança do Tribunal.

01 - Cluster de Firewall Palo Alto - PA 5220.

01 - Cluster de Firewall Palo Alto - PA 5420.

01 - Solução de Gerência Centralizada Panorama.

01 - Microsoft Defender - Soluções de Segurança Microsoft licenciadas com: Microsoft 365 E3 com Add-on E5 Security

01 - Microsoft Defender - Soluções de Segurança Microsoft licenciadas com: Microsoft 365 F3 com Add-on F5 Security

01 - Solução de Gestão de Vulnerabilidades Tenable, licenciada para 2.000 ativos.

Cada solução deve fornecer os serviços de suporte técnico e de atualização do fabricante, com níveis de serviços alinhados com os serviços contratados pelo Tribunal, permanecendo durante toda vigência do contrato.

As soluções de segurança fornecidas pela empresa Contratada devem constar como parceiros oficiais, de modo que permita o acesso completo de recursos e serviços junto ao fabricante, a fim de possuir acesso ao suporte técnico especializado e centros de inteligências.

Gestão de Vulnerabilidades e testes de segurança

Gestão de Vulnerabilidades

Gestão contínua e proativa para identificação de possíveis vulnerabilidades com exposição a ameaças baseada em riscos, na rede, infraestrutura e aplicações do TJPR, a fim de evitar que ataques cibernéticos direcionados tenham sucesso. A execução deverá ser realizada através de SCAN contínuo de ativos de TIC e aplicações monitoradas indicados pela equipe de segurança do TJPR, identificando, avaliando, categorizando, priorizando e tratando vulnerabilidades, avaliando configurações e conformidade com o devido apontamento para mitigação ou resolução.

A solução de Gestão de Vulnerabilidades deverá ser utilizada da fabricante Tenable licenciada para 2.000 ativos. Sendo 1.800 licenças para servidores/IPs e 200 licenças para uso de FQDN.

Deve realizar varreduras automatizadas de vulnerabilidade completas em ativos de TIC com periodicidade mínima de 90 dias, e reteste após aplicação de atualizações, patches e mitigação, incluindo varreduras autenticadas e não autenticadas, com compatibilidade no mínimo com o protocolo Security Content Automation Protocol – SCAP.

Agregação de recursos de inteligência de ameaças (threat intelligence) para rastreamento do uso ativo de TIC e priorização de vulnerabilidades, incluindo fontes estratégicas (relatórios, bases de conhecimento, feeds, fóruns e comunidades abertos, da Deep e da Dark Web etc.), táticas (correlação com táticas, técnicas e procedimentos – TTPs) e operacionais (correlação com indicadores de comprometimento – IOCs), do fabricante da ferramenta combinada com fontes abertas e da contratada.

Acompanhamento de comunicados, alertas de segurança, atualizações, zero day, referenciais de vulnerabilidades e melhores práticas de higienização de segurança e de hardening para ativos de TIC, incluindo: NIST, MITRE, OWASP Top 10, CIS Control, Cert.BR,

fornecedores/fabricantes de tecnologia aplicáveis aos ativos de TIC do Tribunal como Microsoft, Palo Alto, VMWare, Cisco, Google, Red Hat, Trend Micro, entre outros.

Testes de Segurança automatizados

Planejamento, execução, análise e relatório de testes automatizados continuados de segurança com ferramenta de simulação de brechas e ataques (breach and attack simulation – BAS):

Deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno; e endpoint, com comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, cobrindo no mínimo o sistema operacional Microsoft Windows;

As simulações devem garantir ambiente controlado e sem impacto nocivo real;

Os resultados devem validar e indicar controles de prevenção e proteção ineficazes e/ou suplantados, vulnerabilidades exploradas, caminhos de ataque e TTPs (táticas, técnicas e procedimentos) envolvidos.

Teste de invasão (Pentest)

Planejamento, execução e relatório com resultados de testes de invasão, com periodicidade estimada semestral, com planejamento de objetivos e escopo, definição de atuação black box, gray box, ou white box.

Os alvos dos testes de invasão devem ser aprovados pela equipe técnica do Tribunal.

Planejamento, execução, análise e relatório/apresentação de resultados de testes de invasão, com periodicidade estimada semestral, com planejamento de objetivos e escopo, definição de atuação black box, gray box, ou white box.

Gestão de identidade

Serviço contínuo na Gestão de Acesso Privilegiado no acesso aos ativos críticos do TJPR, licenciado para 80 (oitenta) usuários administrativos.

Serviço que contempla operações e respostas às requisições de segurança quanto a administração, dúvidas, status, ações, correções, diagnósticos, relatórios, documentação, análises, procedimentos, falhas, eventos, incidentes, problemas de segurança, entre outros aspectos relativos à segurança da informação.Para o atendimento do serviço desta categoria, a empresa CONTRATADA deverá disponibilizar ferramenta de Gestão de Acesso Privilégiado - PAM, devidamente licenciado.

As soluções de segurança fornecidas pela empresa Contratada devem constar como parceiros oficiais, de modo que permita o acesso completo de recursos e serviços junto ao fabricante, a fim de possuir acesso ao suporte técnico especializado e centros de inteligências.

Serviços técnicos especializados por demanda

Execução de serviços técnicos especializados para atividades não previstas no escopo anteriormente definido, a serem demandados, aprovados e executados sob demanda, mediante ordem de serviço (OS), na forma de um banco de horas técnicas anual.

Alinhamento à Resolução CNJ nº 370/2021, Art. 2º, inciso I, alínea c: Aprimorar a Segurança da Informação e a Gestão de Dados, em processos internos da ENTIC-JUD.

A Resolução Nº 396 de 07/06/2021 do CNJ, institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF). Destacam-se os artigos:

"Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

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;

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;

Conformidade Técnica ou Requisitos Legais	*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;* *V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;* *X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos.* *XI – realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo;* *"* *"Art. 29. Cada tribunal deverá implementar a gestão de usuários de sistemas composta de:* *I – gerenciamento de identidades.* *II - gerenciamento de acessos.* *III - gerenciamento de privilégios.*
	Para este projeto não se aplica os padrões de governo **ePing**
	Para este projeto não se aplica os padrões de governo **eMag**
	Para este projeto não se aplica os padrões de governo **ePWG**
	Para este projeto não se aplica os padrões de governo **MoreqJus**
	Para este projeto não se aplica os padrões de governo **e-ARQ Brasil**
	Este projeto não tem necessidade de aderência às regulamentações da **ICP-Brasil**
Temporal	Ter validade 36 meses prorrogável até o limite legal **Fases do contrato** / **Descrição** **Projeto e implantação** — Iniciando a partir do 1º dia de vigência do contrato até o início da fase de Operação **Operação** — Iniciando a partir do 91º dia de contrato até o término do contrato **Transição do Serviço** — Iniciando em até 90 dias antes da data de término do contrato, ocorrendo em paralelo com fase de Operação Os serviços necessários de natureza continuada são de grande complexidade e abrangência, de forma que é esperado um período em torno de 90 dias para a implantação inicial de todos eles e de vários meses para que os processos, recursos e atividades envolvidos sejam gradativa e continuamente estabilizados, ajustados e refinados. Por outro lado, o ineditismo dos serviços, seu impacto cultural e operacional na organização e a intensa e acelerada evolução atual do mercado de cibersegurança levam a consideráveis níveis de incerteza sobre a adequação, eficácia e eficiência da execução dos serviços no longo prazo. Desta forma, quando a execução dos serviços estiver em sua plenitude, o Tribunal precisará de tempo considerável para absorver e avaliar adequadamente os serviços, tecnologias e processos e seus resultados, bem como planejar e executar próximos passos de continuidade ininterrupta, seja por prorrogação ou nova contratação. Além disso, antes do encerramento do contrato, deve haver um prazo de pelo menos três meses para transição contratual. Por todo o exposto, um prazo inicial de 36

	meses, prorrogáveis dentro dos limites legais, se justifica. Deve ser elaborado um plano de implantação após a assinatura do contrato. Deve ser realizado o levantamento e avaliação inicial da infraestrutura e dos ativos de TIC e o primeiro diagnóstico e avaliação de Gap (situação e lacunas) e maturidade dos Serviços estratégicos de governança, risco e conformidade devem ser entregues após a assinatura do contrato. O prazo máximo para operacionalização do serviço de Centro de operações de segurança - SOC e gerenciamento e análise de eventos e informações de segurança - SIEM e SOAR deve ser de 90 dias, a partir da assinatura do contrato.
Capacidade, Configuração e Desempenho	Os níveis mínimos de serviço são critérios mínimos aceitáveis pelo TRIBUNAL de modo a aferir e avaliar diversos fatores relacionados ao cumprimento dos serviços contratados. Os principais critérios a serem considerados são: • Prazos e quantidades de entrega e execução de serviços compatíveis com os resultados esperados; • Disponibilidade dos serviços continuados e de suas soluções; • Alocação de equipe em conformidade com os requisitos; • Qualidade da entrega e execução de serviços compatível com o objeto. Para mensurar esses fatores, deverão ser utilizados indicadores com metas quantificáveis e objetivos a serem cumpridas. Os indicadores devem ser utilizados para medir o resultado da prestação de serviços e, consequentemente, servir de base para cálculo mensal do valor de remuneração. Os Indicadores de Medição de Resultado (IMR) serão apurados mensalmente.
Tecnológico	Os serviços continuados remotos devem ser executados em regime 24x7x365, mantidos em SOC com infraestrutura de alta disponibilidade e com certificação ISO 27001 em pelo menos 01 dos SOCs.
	Deve também haver ambiente redundante de recuperação de desastre (DR) apto a assumir plena e integralmente a execução dos serviços sob emergência; situado em cidade e região metropolitana distinta, como geo-redundância para mitigar o risco de perda total dos dados e interrupção dos serviços em caso de desastres naturais, falhas de energia ou outros eventos adversos.
	As ferramentas utilizadas devem ser providas em infraestrutura própria da contratada ou do fabricante, ou em ambiente de computação em nuvem pública adequado. Se houver a necessidade de implantação de controladores, concentradores, coletores, sensores, agentes, appliances e qualquer outro recurso de hardware e software local na infraestrutura interna do Tribunal, a contratada deve fornecer e sustentar todos os recursos necessários e ser responsável pelo seu fornecimento, implantação, instalação, configuração, sustentação, atualização, administração e operação, sem custo adicional.
	Toda a comunicação de dados entre a infraestrutura interna do Tribunal e a infraestrutura da contratada deve ser criptografada e otimizada de forma a não introduzir latência inadequada ou óbice ao pleno desempenho, disponibilidade e eficácia da execução dos serviços e seus resultados.
	Todos os serviços, ferramentas, controles e camadas de segurança devem ser integrados e consolidados em uma arquitetura unificada e harmonicamente orquestrada e gerida, provendo como resultado uma camada final de centralização, com um ou mais painéis (dashboards) técnico-operacionais e um painel estratégico-gerencial.
Projeto e Metodologia de Trabalho	A modalidade principal de atendimento e execução dos serviços é do tipo remota, realizada nas dependências da empresa, obedecendo, obrigatoriamente, os critérios estabelecidos para a sua execução, conforme previstas no Termo de Referência e seus anexos. Algumas atividades, segundo critérios no Termo de Referência, poderão ser previstas na

	modalidade presencial.
Projeto	Devido à complexidade do projeto de contratação, composta de serviços e soluções informatizadas, entende-se a necessidade de uma fase de Projeto e implantação em que a empresa deverá realizar as atividades de planejamento, instalação, adoção tecnológica, configuração, implantação do serviço e elaboração de documentação técnica em conformidade com o Termo de Referência.
	Serviços técnicos especializados por demanda para atividades aderentes à contratação não previstas no escopo anteriormente definido relacionadas ao tema de segurança da informação e cibernética, a serem demandados, aprovados e executados sob demanda, através de apresentação de projetos.
Ambiental	Por se tratar de contratação de serviços, não se aplica requisitos ambientais nesta contratação.
Entrega	Serviços de Governança e Conformidade de Segurança através de: • Diagnóstico de Maturidade de Segurança da Informação; • Apoio para Política de Segurança da Informação (PSI); • Apoio para Plano de Continuidade de Serviços Essenciais de TIC; • Apoio para Plano de Resposta a Incidentes (PRI).
	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança: • Serviço de Security Operations Center (SOC); • Proteção contra Riscos Digitais (Threat Intelligence). Serviço de Takedown.
	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança para: • Solução de Firewall; • Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps).
	Gestão de Vulnerabilidades e Testes de Segurança através de: • Gerenciamento Contínuo de Vulnerabilidades; • Testes de Segurança Automatizados (BAS); • Serviço de Teste de Invasão (Pentest).
	Serviço de Gerenciamento de Acesso Privilegiado (PAM).
	Serviços Técnicos Especializados por Demanda.
Implantação	Alocação de Gerente técnico de conta (technical account manager – TAM) e de Preposto da implantação e das operações.
	Plano de implantação e operação, cronograma detalhado e relatórios de acompanhamento.
	Mobilização, instalação e adequação inicial de recursos (pessoas, processos e tecnologias).
	Fornecer ampla documentação e treinamento para as ferramentas e soluções implantadas, incluindo configurações e ajustes, para a equipe técnica do Tribunal.
Manutenção e Atualização	As soluções ofertadas para compor os serviços devem ter manutenção e atualização realizada pela própria empresa respeitando os níveis de serviços estipulados no Termo de Referência.

Garantia	Disponibilizar número telefônico, com disponibilidade de 24x7, para fins de abertura de chamados técnicos, assim como para acompanhamento da solução de problemas.
	Oferecer garantia de no mínimo 12 meses, contados da emissão do Termo de Recebimento Definitivo.
Suporte, SLA E ANS	Quanto ao suporte especializado deve: • Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente) e telefone (0800) no regime 24x7x365 com atendimento em português do Brasil; • Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL; • Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos; • Possuir análise técnica documentada pelo N3 do SOC antes do envolvimento dos fabricantes, a fim de garantir o processo de escalação funcional; • Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos, documentados de acordo com as melhores práticas descritas pelo ITIL.
SLA	Para os diversos tipos de incidentes deverão ser especificados no Termo de Referência: TMIA – Tempo Máximo para Início do Atendimento. TMSO – Tempo Máximo para Solução Operacional, requerido para que o serviço ou o sistema impactado volte a funcionar, independentemente de ter sido resolvida a causa raiz do problema. TMSDC – Tempo Máximo para a Solução Definitiva do Chamado, situação em que o serviço esteja plenamente funcional e a causa raiz do problema é eliminada.
	Deverão ser especificadas níveis de severidade CRÍTICO, ALTA, MÉDIA e BAIXA.
Equipe de Profissionais	Deverá ser dimensionado, alocado e mantido equipe para execução adequada dos serviços contratados organizada no mínimo em grupos distintos para: a) Governança e Gestão de Segurança da informação e Cibersegurança; b) Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança; c) Sustentação de Operações de Soluções e Resposta a Requisições de Segurança; d) Gestão de Vulnerabilidades e Testes de Cibersegurança; e) Gerenciamento de Acesso Privilegiado (PAM).
	A formação acadêmica mínima exigida para todo profissional de cada perfil é: curso superior completo de graduação na área de tecnologia da informação ou graduação em qualquer curso superior acrescido de curso de pós-graduação completo em área de tecnologia da informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
	Deverão ser levantados certificações de validação das melhores práticas de marcado para perfis profissionais: • Gerente Técnico do Contrato (Technical Account Manager – TAM); • Governança e Gestão de Cibersegurança; • Monitoramento, Detecção e Resposta Gerenciados de Cibersegurança; • Analista de Inteligência de Ameaças (Threat Intelligence) e Caçada Contínua a Ameaças

	(Threat Hunting); • Analista de Resposta a Incidentes e Forense Digital (DFIR); • Analista de Gestão de Vulnerabilidades e Testes de Segurança; • Analista de Segurança.
Experiência Profissional	• Gerente Técnico do Contrato (Technical Account Manager - TAM): Mínimo de 03 (três) anos de experiência em gestão de segurança da informação. • Governança e Gestão de Cibersegurança: Experiência mínima de 03 (três) anos em acompanhamento, auditoria e controles de conformidade, normas e riscos de TI. • Monitoramento, Detecção e Resposta Gerenciados de Cibersegurança: Mínimo de 03 (três) anos de experiência no monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e resposta a incidentes. • Analista de Inteligência de Ameaças (Threat Intelligence) e Caçada Contínua a Ameaças (Threat Hunting): Experiência comprovada de no mínimo 12 (doze) meses em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e Advanced threat detection (ATD). • Analista de Resposta a Incidentes e Forense Digital (DFIR): Experiência comprovada de no mínimo 12 (doze) meses em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e Advanced threat detection (ATD). • Analista de Gestão de Vulnerabilidades e Testes de Segurança: Experiência comprovada de no mínimo 2 (dois) anos. • Analista de Segurança: Experiência comprovada de no mínimo 24 meses para cada solução.
Capacitação E Transferência de Conhecimento	Promover a transferência de conhecimento aos indicados pelo TRIBUNAL, de forma a permitir a plena gestão, entendimento, operação, monitoramento e otimização dos serviços e soluções objeto do contrato, na forma de reuniões, apresentações, documentação, relatórios e outros meios que se façam adequados.
	Ser ministrada de forma a cobrir toda estrutura e topologia projetada para atendimento aos requisitos da contratação, e deve estar contemplada nas fases de Projeto e implantação, Operação e Transição.
	Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades.
Segurança	As exigências do termo de sigilo e confidencialidade visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TIC.

4. ESTIMATIVAS DAS QUANTIDADES PARA CONTRATAÇÃO

A demanda prevista contém o conjunto de serviços e soluções de segurança que melhor atendem as demandas do projeto pelo período de 36 meses. A vigência contratual de 36 (trinta e seis) meses será dividida em 03 etapas, a primeira fase compreende o **Projeto e implantação** com duração de 03 (três) meses, iniciada a partir da assinatura do contrato, seguida pela fase de **Operação**, que abrangerá os 33 (trinta e três) meses subsequentes do contrato. Sendo os últimos 03 meses denominados fase de **Transição do final de contrato.**

Projeto e implantação

Devido à complexidade do projeto de contratação, composta de serviços e soluções informatizadas, entende-se a necessidade da contemplação da fase de **Projeto e implantação** em que a CONTRATADA deverá realizar as atividades de planejamento, instalação, adoção tecnológica, configuração, implantação do serviço e elaboração de documentação técnica em conformidade com este Termo. A execução será de apenas 01 vez, iniciando a partir da assinatura de contrato e com término máximo de até 90 (noventa) dias corridos.

Serviços de Governança e Conformidade de Segurança

A contratação do serviço de **Governança de Segurança da Informação** é de atuação contínua e proativa, objetivando apoiar na avaliação, proposição, revisão de políticas, normas e procedimentos de segurança, além

de auxiliar na conformidade (*compliance*) com as melhores práticas de mercado nos temas de segurança da informação e cibernética, normas do CNJ e requisitos internos do TRIBUNAL.

Para este item estão previstas as demandas:

- 03 (três) avaliações de **Diagnóstico de Maturidade de Segurança da Informação**, com objetivo de realizar uma avaliação com ciclo anual durante a vigência do contrato, a fim de avaliar a maturidade e progresso nos temas de segurança da informação e cibernética.
- 01 (um) serviço mensal de apoio de aprimoramento e acompanhamento da **Política de Segurança da Informação - PSI**, para aperfeiçoamento, adequação e monitoramento da política, pelo período de 33 (trinta e três) meses durante a fase de **Operação**.
- 01 (um) serviço mensal de apoio de aprimoramento e acompanhamento de **Plano de Continuidade de Serviços Essenciais de TIC com foco no SOC,** pelo período de 33 (trinta e três) meses durante a fase de **Operação**.
- 01 (um) serviço mensal de apoio de aprimoramento e acompanhamento de **Plano de Resposta a Incidentes - PRI** e planos de mitigação e recuperação, pelo período de 33 (trinta e três) meses durante a fase de **Operação**, aderente as necessidades estabelecidas pela Portaria Nº 162 e seus anexos do CNJ.

Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança

01 (uma) prestação mensal de serviço contínuo e ininterrupto de **Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**, por meio de um *Security Operations Center* (SOC), contemplando: equipe, processos, documentação, gestão de eventos, incidentes e crises, incluindo solução informatizada para gerenciamento, monitoramento, detecção e resposta de informações, eventos e incidentes de segurança, licenciado pela empresa. A unidade de contratação é de periodicidade mensal por ativo protegido, sendo necessária a comprovação ao final de cada mês do serviço prestado para o efetivo pagamento. A quantidade estimada de ativos do TRIBUNAL é de 25.000 (vinte e cinco mil), conforme tabela de estimativa abaixo, como a vigência do contrato é 33 (trinta e três) meses, reduzindo 03 (três) meses do Projeto e implantação, a demanda prevista é de 825.000 ativos (oitocentos e vinte e cinco mil), durante a vigência do contrato.

Item	Descrição	Quantidade
1	Servidores físicos	80
2	Servidores virtuais	700
3	Estação de trabalho	16.000
4	Notebooks	3.000
5	Impressoras	3.000
6	DNS	4
7	Links de Internet	3
8	Site WAN	215
9	Switches/roteadores	1.200
10	VPN	4
11	Serviço de Diretório	6
12	Storages	4

A estimativa de ativos foi criada com base em entrevista as equipes da Divisão de Infraestrutura e Divisão de Serviços Colaborativos, no período do segundo semestre de 2024. Durante as entrevistas foram considerados os ativos em uso, sobre contrato e/ou garantia, bem como possível crescimento em cada item.

01 (uma) prestação mensal de serviço contínuo e ininterrupto de **Proteção contra Riscos Digitais (*Threat Intelligence*),** pelo período de 33 (trinta e três) meses. A demanda de proteção atuará sobre o monitoramento dos perfis oficiais de redes sociais do TRIBUNAL, no mínimo os indicados na tabela abaixo:

Rede Social	**Nome do Perfil**	**@**
Instagram	Tribunal de Justiça do Paraná	@TJPRoficial
Youtube	Tribunal de Justiça do Paraná	@TJPRoficial
Facebook	Tribunal de Justiça do Paraná	@TJPRoficial
X (Twitter)	Tribunal de Justiça do Paraná	@TJPRoficial
Threads	Tribunal de Justiça do Paraná	@TJPRoficial
Bluesky	Tribunal de Justiça do Paraná	@TJPRoficial
Instagram	Escola Judicial do Paraná	@ejud.tjpr
Instagram	Adoção-Encontro Online TJPR	@adocao_encontroonlinetjpr
Instagram	2ª Vice-Presidência do TJPR	@2vicetjpr
Instagram	CEVID TJPR	@cevidtjpr
Instagram	1ª Vice-Presidência do TJPR	@tjpr1vice
Instagram	CONSIJ/CIJ do TJPR	@consij_cij.tjpr
Instagram	GMF - TJPR	@gmf_tjpr
Instagram	Corregedoria da Justiça do Paraná – TJPR	@corregedoria_tjpr
Instagram	Ouvidoria da Justiça Paraná	@ouvidoria_justica_pr
Youtube	2a Vice-Presidência do TJPR	@2vicetjpr
Youtube	Tribunal do Júri TJPR	@TribunaldoJuriTJPR
Youtube	TJPR - Sessões	@TJPRsessoes
Youtube	EJUD TJPR	@EJUDTJPR
Youtube	CEVID TJPR	@cevidtjpr7240
Facebook	2ª Vice-Presidência TJPR	@2vicetjpr
Facebook	CEVID	@cevidparana

A lista de perfis sociais foi obtida através da consulta à Coordenadoria de Comunicação Social através do SEI 0065374-47.2024.8.16.6000, em maio de 2024.

01 (uma) prestação de **Serviço de *Takedown* de sites** de 60 (sessenta) unidades, considerando que não há registro estatístico sobre incidentes que envolvem a necessidade de takedown, a equipe técnica entende que o valor de 20 (vinte) *Takedowns* por ano é adequado para este período de contratação, totalizando 60 (sessenta) durante a vigência do contrato, sendo o pagamento realizado por *Takedown* executado.

Sustentação de Operações de Soluções e Resposta a Requisições de Segurança

01 (uma) prestação mensal de serviço contínuo de **Sustentação de Operações de Soluções e Resposta a Requisições de Segurança** para gerenciar, sustentar e operar soluções de segurança do parque tecnológico do TRIBUNAL, administrando e gerenciando ferramentas e soluções de Firewall Palo Alto Networks, 02 (dois) Firewalls PA-5220, 02 (dois) Firewalls PA-5420 e 02 (duas) gerencias centralizadas, totalizando 06 (seis) ativos de Firewall pelo período de 33 (trinta e três) meses, com uma quantidade prevista de 198 ativos (cento e noventa e oito), sendo necessária a comprovação ao final de cada mês do serviço prestado para o efetivo pagamento.

01 (uma) prestação mensal de serviço contínuo e proativo para **gerenciar, sustentar e operar soluções de segurança do parque tecnológico do TRIBUNAL**, administrando, sustentando e gerenciando ferramentas e soluções Microsoft 365 E3 com Add-on E5 Security, contendo os recursos de Defender for Office Plan 1 e 2, Entra ID Plan 1 e 2, Defender for Endpoint Plan 2. Para o licenciamento de soluções de segurança Microsoft o TRIBUNAL possui 18.018 (dezoito mil e dezoito) ativos/licenças, totalizando para os 33 (trinta e três) meses 594.594 (quinhentos e noventa e quatro mil e quinhentos e noventa e quatro) ativos/licenças. Por questões de oscilação no crescimento e arredondamento, onde ativos são inseridos e removidos da infraestrutura de TIC do TRIBUNAL, foram estimados a quantidade de 660.000 (seiscentos e sessenta mil) ativos, sendo pagos efetivamente por aferição mensal através de comprovação pela empresa.

A sustentação, administração, operação, suporte técnico e atualização das ferramentas fornecidas pela empresa, como SIEM, BAS, PAM e qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos, serão serviços de natureza continuada de responsabilidade da empresa.

Item	Ativo	Descrição	Quantidade
1	Solução de Firewall 01	Palo Alto - PA 5220	02
2	Solução de Firewall 02	Palo Alto - PA 5420	02
3	Solução de Gerência Centralizada	Palo Alto Panorama	02
4	Microsoft Defender	Soluções de Segurança Microsoft licenciadas com: Microsoft 365 E3 com Add-on E5 Security	4.000
5	Microsoft Defender	Soluções de Segurança Microsoft licenciadas com: Microsoft 365 F3 com Add-on F5 Security	14.018
6	Solução de Gestão de Vulnerabilidades	Tenable, licenciado para 2.000 ativos	01

A lista de quantidades para o serviço de sustentação e operação foi dimensionada com base nos contratos das soluções de segurança que serão atendidas pela contatação, listados no segundo semestre de 2024.

Gestão de Vulnerabilidades e Testes de Segurança

Uma prestação mensal de Gerenciamento Contínuo de Vulnerabilidades e proativo para identificação de possíveis vulnerabilidades na rede, infraestrutura e aplicações do TJPR, a fim de evitar que ataques cibernéticos direcionados tenham sucesso, com sustentação e operação de solução fornecida pelo TRIBUNAL. Esta demanda é com pagamento mensal, após comprovação do serviço prestado pelo prazo de 33 (trinta e três) meses.

Uma prestação de serviço de Testes de Segurança Automatizados (BAS), sendo realizados 30 (trinta) baterias de testes por mês, prestado pelo prazo de 33 (trinta e três) meses, totalizando 990 (novecentos e noventa) baterias de testes.

A definição de 30 baterias de testes por mês baseia-se em critérios técnicos e de conformidade que garantem cobertura adequada da superfície de ataque digital do TRIBUNAL.

Distribuição estimada:

- Aplicações Web Críticas: 8 testes mensais (sistemas de alta criticidade);
- APIs e Web Services: 6 testes mensais (integração e dados sensíveis);
- Infraestrutura de Rede: 4 testes mensais (perímetro e acessos);
- Aplicações Móveis: 4 testes mensais (apps corporativos);
- Ambientes de Desenvolvimento: 4 testes mensais (pipeline DevSecOps);
- Compliance e Auditoria de controles: 4 testes mensais (LGPD, PCI-DSS, ISO 27001).

Um serviço de Teste de Invasão (Pentest) sob demanda, previsto para um consumo médio de 60 (sessenta) horas por teste, sendo realizado 01 (um) teste a cada 06 (seis) meses, totalizando 360 (trezentos e sessenta) horas durante a vigência do contrato. Conforme necessidade de aderência ao Art.11, item X, da Resolução Nº 396 do CNJ.

A alocação de 60 (sessenta) horas para a realização do teste de intrusão é justificada pela abrangência e complexidade moderada do escopo, que contempla uma aplicação web com funcionalidades críticas, autenticação de usuários, integração com APIs e possíveis vetores de ataque comuns. Esse tempo permite a execução de uma abordagem híbrida, combinando ferramentas automatizadas com análise manual, garantindo a identificação de vulnerabilidades relevantes sem comprometer a profundidade da avaliação. Além disso, contempla a elaboração de um relatório técnico detalhado com evidências, recomendações e, se necessário, uma sessão de apresentação dos resultados para as partes interessadas.

Gestão de Identidade

01 (uma) prestação mensal de serviço contínuo de **Gestão de Acesso Privilegiado - PAM** aos ativos e serviços de TIC do TRIBUNAL, licenciado para 80 (oitenta) usuários administrativos, contemplando os usuários administrativos da SETI que realizam o gerenciamento de ativos Data Center e Nuvem sob a responsabilidade do TRIBUNAL, totalizando 2.640 (dois mil e seiscentos e quarenta) usuários protegidos considerando 33 (trinta e três) meses durante a fase de **Operação**.

O quantitativo para as licenças deste serviço foi obtido através da lista de servidores que atuam na administração dos ativos que serão controlados, somado as contratações que estão em andamento para terceirização, considerando que estas licenças somente serão pagas após uso.

Serviços Técnicos Especializados por demanda

Serviços técnicos especializados por demanda para atividades aderentes à contratação não previstas no escopo anteriormente definido, relacionadas ao tema de segurança da informação e cibernética, a serem demandados, aprovados e executados sob demanda, mediante Ordem de Serviço (OS), na forma de um banco de horas técnicas. Estão sendo estimadas a contratação eventual de até 400 (quatrocentos) horas por ano de vigência do contrato, podendo totalizar até 1.200 (um mil e duzentos) horas durante a vigência do contrato.

A segurança cibernética é um campo dinâmico, sujeito a constantes mudanças regulatórias, evolução tecnológica e surgimento de novas ameaças. Dessa forma, é comum que surjam demandas pontuais e especializadas, como:

- Apoio técnico em incidentes de segurança;
- Revisões e atualizações de políticas e procedimentos;
- Análises de vulnerabilidades e testes de segurança;
- Consultorias específicas em conformidade com normas e boas práticas;
- Apoio em auditorias internas e externas;
- A tabela abaixo sumariza a demanda prevista.

O valor de 400 horas por ano representa uma média ponderada entre a previsibilidade orçamentária e a capacidade de resposta técnica, permitindo atender a múltiplas frentes de trabalho sem comprometer a qualidade ou a tempestividade das entregas.

Item	Categoria	Descrição	Qtde	Tipo
1	**Projeto e implantação**		01	Unitário
2	**Serviços de Governança e Conformidade de Segurança**			
	2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Unitário
	2.2	Política de Segurança da Informação (PSI)	33	Mês
	2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês

	2.4	Plano de Resposta a Incidentes (PRI)	33	Mês
3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**			
	3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos
	3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês
	3.3	Serviço de Takedown de sites	60	Takedown executado
4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**			
	4.1	Solução de Firewall	198	Ativos protegidos
	4.2	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos
5	**Gestão de Vulnerabilidades e Testes de Segurança**			
	5.1	Gerenciamento Contínuo de Vulnerabilidades	33	Mês
	5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas
	5.3	Serviço de Teste de Invasão (Pentest)	360	Horas sob demanda
6	**Gestão de Identidade**			
	6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos
7	**Serviços Técnicos Especializados por Demanda**		1.200	Horas sob demanda

5. LEVANTAMENTO DE MERCADO

5.1 CONTRATAÇÕES SIMILARES

Encontram-se identificadas abaixo as contratações realizadas por outros órgãos ou entidades da Administração Pública, cuja necessidade ou problema se assemelham à necessidade objeto deste estudo:

Conselho Nacional de Justiça (CNJ)

Processo SEI Número: 00131/2020

Pregão Eletrônico Número: 03/2021

Contrato 08/2021 - Contratação de Serviços Gerenciados de Segurança da Informação.

Tribunal de Contas do Estado do Paraná (TCE-PR)

Processo Número: 356352/22

Pregão Eletrônico Número: 02/2023

Contrato 24/2023 - Contratação de empresa especializada para prestação de serviço de Security Operations Center (SOC), sem dedicação exclusiva de mão de obra.

Poder Judiciário do Estado do Rio de Janeiro (PJERJ)

Processo Número: 0621520/2021

Pregão Eletrônico Número: 50/2022

Contrato 003/528/2022 - Contratação de empresa especializada em Serviços Gerenciados de Segurança da Informação (GSTI) para implementação e execução de serviços de Segurança da Informação, cibernética e da proteção de dados incluindo ferramentas e alocação de mão de obra dedicada nas dependências do PJREJ pelo prazo de 24 meses.

5.2 SOLUÇÕES DE SOFTWARE LIVRE OU PÚBLICO

Não se aplica por tratar-se de contratação de prestação de serviço e não de soluções de softwares.

5.3 SOLUÇÕES DISPONÍVEIS NO MERCADO

Encontram-se identificadas na tabela abaixo as soluções encontradas após pesquisa de mercado e prospecção com empresas da área, visando à necessidade descrita neste estudo:

Solução 1	
Solução:	Serviços prestados SOC por servidores internos da SETI
Descrição:	Esta solução considera a utilização do corpo de servidores da SETI para desempenhar as atividades de cibersegurança, aquisição e integração de soluções de mercado para as ferramentas e tecnologias necessárias, incluindo hardware (equipamentos) e software (licenças ou subscrições), serviços de implantação, garantia, atualização e suporte técnico, incluindo monitoramento 24x7, Blue Team e Red Team, sustentação de novos soluções de segurança e aplicação de Pentest.
Vantagem:	Sem necessidade de contratação
Desvantagem:	Insuficiência de servidores para prestar os serviços de SOC. Incapacidade técnica das equipes ou falta da expertise na matéria de cibersegurança. Necessidade de treinamento robusto de segurança da informação. Curva de aprendizado elevada para apresentação de resultados, sendo uma formação adequada em torno de 03 anos. Custos para pagamento ou diária de plantão de servidores, a fim de manter o monitoramento de 24 horas podia, 7 dias por semana e 365 dias por ano. Visão amplamente conhecida da infraestrutura do Tribunal, dificultando a execução de pentest. Falta de servidores para implementar e operacionalizar a solução de Privileged Access Management - PAM. Falta de servidores para operacionalizar a ferramenta de Gestão de Vulnerabilidades (Tenable).
Solução 2	
Solução:	Contratação de empresa especializada para prestação de serviços de segurança da informação
Descrição	Contratação de empresa especializada para prover os serviços de segurança da informação
	Monitoramento contínuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos os incidentes de segurança. Número de membros da equipe contratada suficiente para atender ao TJPR, frente aos desafios atuais.

Vantagem:	Equipe altamente capacitada e com expertise em segurança cibernética. Agregação de novas ferramentas e soluções trazidas ao ambiente do TJPR. Equipe para operacionalizar as ferramentas de segurança do Tribunal, realizando a sustentação contínua. Elevação do nível de segurança do Tribunal. Maximizar a disponibilidade dos serviços de TIC oferecidos pelo TJPR.
Desvantagem:	Necessidade e Custo de Contratação. Tempo de adequação. Transição entre empresas contratadas, após o término ou rompimento do contrato.

5.4 ANÁLISE COMPARATIVA DAS SOLUÇÕES

AT: Atende, **N AT**: Não Atende, **N AP**: Não se Aplica, **V**: Viável, I: Inviável

Requisito (A solução contratada deve...)	**SM1**	**SM2**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública	**Não há conhecimento**	**AT**
A Solução está disponível no **Portal do Software Público Brasileiro**	**N AP**	**N AP**
A Solução é composta por **software livre ou software público**	**N AP**	**N AP**
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo **ePing, eMag**, **ePWG?**	**N AP**	**N AP**
A Solução é aderente às políticas, 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**)	**N AP**	**N AP**
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (**MNI**) do Poder Judiciário	**N AP**	**N AP**
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo **MoreqJus**	**N AP**	**N AP**
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do **e-ARQ** Brasil (quando o objetivo da solução abranger documentos arquivísticos)	**N AP**	**N AP**
A Solução é aderente às regulamentações da **ICP-Brasil**	**N AP**	**N AP**
Possuir equipe de profissionais qualificados disponíveis	**N AT**	**AT**
Resultado da Análise	I	**V**

5.4.1 Soluções inviáveis

A SETI não dispõe de quantitativos e nem de perfis profissionais suficientes para fornecer um serviço de segurança em regime de 24x7x365 dias, nem tem expectativa de contratação a curto prazo, inviabilizando a solução 1.

5.4.2 Análise comparativa de custos das Soluções viáveis

Após a análise detalhada das opções disponíveis, conclui-se que existe apenas uma solução viável para atender às necessidades de segurança. Dado que a SETI não possui recursos humanos suficientes e não há expectativa de contratação a curto prazo, a comparação de custos não se aplica quando há somente uma solução viável.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

6.1 CRONOGRAMA FÍSICO FINANCEIRO

Abaixo apresentamos a tabela com propostas apresentadas por empresas:

				Under Protection		**Future Technologies LTDA**	
Item	**Descrição**	**Qtd**	**Tipo**	**Valor Unitário**	**Valor Total**	**Valor Unitário**	**Valor Total**
1	**Projeto e implantação**	1	Unitário	57.260,00	57.260,00	1.890.000,00	1.890.000,00
2	**Serviços de Governança e Conformidade de Segurança**						
2.1	Diagnóstico de Maturidade de Segurança da Informação	03	Mês	15.960,00	47.880,00	48.667,00	207.999,00
2.2	Política de Segurança da Informação (PSI)	33	Mês	14.000	462.000,00	6.30,00	207.999,00
2.3	Plano de Continuidade de Serviços Essenciais de TIC	33	Mês	15.714,79	518.588,07	4.697,00	155.991,00
2.4	Plano de Resposta a Incidentes (PRI)	33	Mês	1.680,00	55.440,00	4.727,00	155.991,00
3	**Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança**						
3.1	Serviço de Security Operations Center (SOC)	825.000	Ativos protegidos	27,88	23.001.000,00	19,62	16.186.500,00
3.2	Proteção contra Riscos Digitais (Threat Intelligence)	33	Mês	35.455,62	1.170.035,46	55.939,39	1.846.000,00
3.3	Serviço de Takedown de sites	60	Takedown executado	2.616,24	156.974,40	4.317,00	259.020,00
4	**Sustentação de Operações de Soluções e Resposta a Requisições de Segurança**						
4.1	Solução de Firewall	198	Ativos protegidos	6.000,00	1.188.000,00	1.031,00	204.138,00

4.1	Solução Microsoft Defender (Office, Endpoint, Entra ID, Cloud Apps)	660.000	Ativos protegidos	1,20	792.000,00	0,50	333.000,00
5	**Gestão de Vulnerabilidades e Testes de Segurança**						
5.1	Gestão de Vulnerabilidades e Testes de Segurança	33	Mês	87.815,18	2.897.900,94	5.031,00	166.023,00
5.2	Testes de Segurança Automatizados (BAS)	990	Baterias realizadas	205,90	203.841,00	1.693,94	1.677.000,60
5.3	Serviço de Teste de Invasão (Pentest)	360	Horas sob demanda	308,00	110.880,00	371,00	133.560,00
6	**Gestão de Identidade**						
6.1	Gerenciamento de Acesso Privilegiado (PAM)	2.640	Usuários administrativos protegidos	1056,30	1.742.895,00	1.622,42	2.676.993,00
7	**Serviços Técnicos Especializados por Demanda**						
7.1	Serviços técnicos especializados por demanda	1.200	Horas sob demanda	350,00	420.000,00	277,50	333.000,00
Investimento total					**R$ 32.824.694,87**		**R$ 26.112.196,00**

Com base nas projeções do andamento da contratação, espera-se que o gasto estimado para o ano corrente se concentre apenas na fase de implantação do projeto.

6.2 VALOR TOTAL ESTIMADO

Conforme análise comparativa das soluções, o valor médio estimado total para a contratação é de R$ 29.000.000,00 (vinte e nove milhões).

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A contratação do modelo de serviços gerenciados de Segurança da Informação e Cibernética pelo Tribunal visa responder ao aumento da complexidade e criticidade do ambiente tecnológico do tribunal, garantindo proteção contínua, monitoramento especializado e resposta ágil a incidentes. O objetivo é elevar o nível de maturidade em segurança, atender às exigências normativas nacionais e fortalecer a resiliência institucional frente às ameaças cibernéticas, por meio de uma solução integrada, escalável e alinhada às melhores práticas de mercado.

Projeto e Implantação: Esta etapa inicial contempla o planejamento, instalação, adoção tecnológica, configuração e documentação técnica de todos os serviços e soluções contratados. É fundamental para garantir que a transição para o novo modelo ocorra de forma estruturada, segura e alinhada às necessidades do tribunal, estabelecendo as bases para a operação eficiente do SOC.

Serviços de Governança e Conformidade de Segurança: Inclui diagnósticos anuais de maturidade em segurança da informação, revisão e aprimoramento contínuo da Política de Segurança da Informação (PSI), do Plano de Continuidade de Serviços Essenciais de TIC e do Plano de Resposta a Incidentes (PRI). O objetivo é garantir conformidade com normas do CNJ, ISO e melhores práticas, promovendo governança efetiva e melhoria contínua dos processos de segurança.

Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança: Prevê a operação de um SOC 24x7x365, com equipe dedicada para monitoramento, detecção, análise, investigação e resposta a incidentes de segurança cibernética. Inclui também serviços de proteção contra riscos digitais (Threat

Intelligence) e execução de takedown de sites maliciosos, ampliando a capacidade de defesa e resposta do tribunal.

Sustentação de Operações de Soluções e Resposta a Requisições de Segurança: Abrange a administração, operação e suporte contínuo das soluções de segurança do parque tecnológico do TJPR, como firewalls, Microsoft Defender e demais ferramentas críticas. O objetivo é desafogar as equipes internas, garantir a disponibilidade e a atualização das soluções e manter o ambiente protegido contra ameaças emergentes.

Gestão de Vulnerabilidades e Testes de Segurança: Envolve o gerenciamento contínuo de vulnerabilidades, com varreduras periódicas, análise de riscos, recomendações de remediação e execução de testes automatizados (BAS). Essa abordagem proativa visa antecipar e corrigir falhas antes que sejam exploradas por atacantes.

Gestão de Identidade: Implanta e opera uma solução de Gerenciamento de Acesso Privilegiado (PAM), protegendo credenciais administrativas e garantindo rastreabilidade e controle rigoroso dos acessos a ativos críticos do tribunal. Isso reduz riscos de uso indevido de privilégios e atende requisitos da LGPD e das melhores práticas de segurança.

Serviços Técnicos Especializados por Demanda: Disponibiliza um banco de horas técnicas para execução de serviços especializados sob demanda, como consultorias, mentorias, workshops, produção de documentação técnica e apoio em projetos de segurança da informação e cibersegurança, conforme necessidades específicas do tribunal.

Serviço de Teste de Invasão (Pentest): Prevê a realização de testes de invasão sob demanda, com planejamento, execução e relatório detalhado, visando identificar vulnerabilidades e riscos em sistemas e aplicações do TJPR, além de apoiar a correção e validação das remediações implementadas.

Em síntese, a contratação do modelo de SOC representa um avanço estratégico para o TJPR, promovendo uma abordagem integrada, contínua e especializada para a segurança da informação e cibernética. Ao combinar governança, monitoramento avançado, gestão de vulnerabilidades, proteção de identidade e serviços sob demanda, o tribunal fortalece sua capacidade de prevenir, detectar e responder a ameaças, garantindo a continuidade dos serviços, a conformidade normativa e a proteção dos dados e sistemas sob sua responsabilidade.

7.1 ASPECTOS DE SUSTENTAÇÃO DA SOLUÇÃO

7.1.1 Estratégia de Independência Tecnológica

Deverá ser elaborada Fase de Transição do Serviço relacionada ao processo de finalização da prestação dos serviços contratados, visando estabelecer critérios de **Transição do Serviço**, pelo tempo necessário e de forma a garantir a transferência de conhecimento e adaptação de eventual nova empresa contratada e/ou equipes do TRIBUNAL que vierem a absorver os serviços.

A empresa deve exportar e fornecer, em formato completo, aberto e interoperável:

- Uma consolidação completa de todas as políticas, estratégias, planos, processos, procedimentos, métricas, indicadores e painéis elaborados, revisados e/ou propostos pela empresa;
- Todos os dados, informações, registros, relatórios e configurações relevantes da solução Informatizada para Gerenciamento, Monitoramento, Detecção e Resposta de Informações, Eventos e Incidentes de Segurança, incluindo os registros (logs) consolidados e repositórios de dados e metadados de eventos e incidentes, casos de uso de monitoramento, playbooks, regras e scripts de resposta, orquestração e automação, dentre outros relevantes;
- Todos os dados, informações, registros, relatórios e configurações relevantes da solução Informatizada de Gestão de Acesso Privilegiado - PAM, incluindo os registros (logs) consolidados e repositórios de dados e metadados de eventos, políticas, estratégias, planos, processos, procedimentos, métricas, dentre outros relevantes;
- Consolidação completa de todas as políticas, estratégias, planos, topologias, processos, procedimentos, métricas, indicadores e painéis elaborados, metodologia de trabalho e configurações relevantes relacionados aos serviços de sustentação e operação;
- Todos os dados, informações, registros, relatórios e configurações relevantes do serviço de Proteção contra Riscos Digitais;
- Todos os dados, informações, registros, relatórios e configurações relevantes da solução informatizada de testes de segurança, incluindo catálogo atualizado de ativos de software identificados e suas configurações, vulnerabilidades identificadas, remediações aplicadas, regras e exceções adotadas, critérios e métricas de priorização de riscos, dentre outros relevantes;
- Todos os dados, informações, registros, relatórios e configurações relevantes da Solução informatizada de simulação de violações e ataques.

A empresa deverá elaborar e atualizar toda a documentação que porventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.

7.1.2 Transição Contratual

A empresa deve elaborar planejamento e realizar o repasse integral e irrestrito de informações, dados, documentos e conhecimentos necessários e suficientes para promover a continuidade dos serviços.

Ao término da vigência do contrato, deve haver:

- A revogação de todas as credenciais e autorizações de acesso da empresa aos serviços e soluções informatizadas;
- A suspensão ou eliminação de caixas postais e outros recursos de tecnologia que eventualmente tenham sido criados ou destinados para a empresa.

A devolução de recursos materiais que eventualmente tenham sido destinados para a empresa.

7.1.3 Descontinuidade do Fornecimento

Se, por qualquer eventualidade, a empresa contratada frustrar total ou parcialmente o objeto da avença, será necessária a aplicação de penalidades e chamamento do subsequente na ordem de classificação, caso tenha, ou elaboração de novo processo de licitação.

8. PARCELAMENTO E ADJUCAÇÃO

8.1 PARCELAMENTO DO OBJETO

O objeto da licitação, embora divisível em termos técnicos, apresenta características que tornam a contratação por item individual complexa e prejudicial à qualidade dos serviços a serem prestados. A fragmentação da contratação dificultaria a integração das soluções de proteção com os serviços de cibersegurança e a implementação de uma estratégia de segurança holística. Com um único fornecedor, a responsabilidade pela integração, operação e suporte das soluções MSS e Proteção recai sobre uma única empresa. Isso facilita a cobrança de resultados, a resolução de problemas e a garantia do cumprimento das obrigações contratuais.

O agrupamento também permite o aumento da eficiência administrativa por meio da otimização do gerenciamento do serviço, pois neste caso, não seria conveniente e oportuno a prestação desses serviços por partes distintas, considerando que lidar com um único ou poucos prestadores diminui o custo administrativo de gerenciamento de todo o processo de contratação (Acórdão 861/2013-TCU Plenário).

Destaca-se que o agrupamento não implica prejuízo à ampla competitividade, pois existem, no mercado, diversas empresas com capacidade de fornecer os produtos e serviços na forma estabelecida neste Termo de Referência.

Considerando as características dos itens, buscando garantir a qualidade dos serviços e otimizar a gestão da contratação, entende-se que há possibilidade em particionar o objeto da licitação em dois agrupamentos, um composto dos serviços essenciais e outro para o serviço de Pentest.

8.2 ADJUCAÇÃO DO OBJETO

A contratação será composta por 07 (sete) itens agrupados e 01 (um) item não agrupado, possibilitando a adjudicação do objeto por mais de uma empresa participante da licitação, conforme detalhado na tabela abaixo:

Grupo	Item	Descrição
1	1	Projeto e implantação
	2	Serviços de Governança e Conformidade de Segurança
	3	Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança
	4	Sustentação de Operações de Soluções e Resposta a Requisições de Segurança
	5	Gestão de Vulnerabilidades e Testes de Segurança
	6	Gestão de Identidade

	7	Serviços Técnicos Especializados por Demanda
Item avulso	**8**	PenTest

Deve ser vedada a contratação de uma mesma empresa para os itens do Grupo 01 e item 1 do Grupo 2 devido sua natureza, pois estes serviços exigem a segregação de funções. Esta separação de funções assegura que os testes de invasão sejam conduzidos de forma independente e rigorosa, proporcionando uma avaliação honesta e precisa das defesas de segurança.

9. RESULTADOS E BENEFÍCIOS PRETENDIDOS

Aumentar a capacidade de monitoramento, detecção e resposta à incidentes de segurança cibernética no ambiente do TRIBUNAL de modo contínuo e ininterrupto.

Agregar a expertise de mão de obra altamente capacitada e especializada em segurança da informação e cibernética ao time do TRIBUNAL.

Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes, visando minimizar o tempo de atuação e possíveis danos causos por ataques cibernéticos, mesmo fora do horário regimental do TRIBUNAL.

Aumento da robustez nos principais sistemas do TRIBUNAL, através da realização de testes de invasão sob demanda, antecipando a identificação de vulnerabilidade de modo proativo.

Implantação de um SOC (Security Operations Center) com a capacidade de identificar, proteger, detectar, responder e recuperar, atuando na segurança defensiva e reativa. Prestando apoio direto às diversas áreas da SETI na investigação, remediação e melhorias de cibersegurança.

Prover a melhoria contínua em segurança da informação e cibersegurança de acordo com indicadores e relatórios de acompanhamento.

Redução de superfície de ataque através da ampliação de soluções de segurança e os mecanismos de proteção cibernética no TRIBUNAL com as soluções de SIEM, BAS, PAM.

Estar em conformidade com as recomendações e exigências do CNJ contidas nas Resoluções Nº 396 e Portaria Nº 162 e seus anexos.

10. PROVIDÊNCIAS PREVIAS À CELEBRAÇÃO DO CONTRATO

10.1 ADEQUAÇÃO DO AMBIENTE E ESPAÇO FÍSICO

Os serviços contratados serão realizados predominantemente de forma remota. Para este caso, o TRIBUNAL dispõe de recursos como Internet, rede de comunicação e Datacenter para comportar os serviços prestados.

O acesso ao ambiente do Tribunal deverá ser realizado através de enlace (link) de comunicação dedicado, com acesso restrito e criptografado, no qual deverá ser provido e mantido pela empresa:

a) A utilização deste link de comunicação não deverá ultrapassar 80% (oitenta por cento) de sua capacidade, podendo ser utilizado VPN via internet como redundância.

b) Caso a capacidade do link, dimensionada pela empresa, seja considerada insuficiente para a prestação dos serviços a empresa deverá providenciar o seu aumento, sem custos para o Tribunal.

c) Devido a limitação para adicionar novas operadoras, a empresa deve consultar o Tribunal antes de contratar o serviço.

10.2 INFRAESTRUTURA TECNOLÓGICA

Será disponibilizará, nos casos de instalação de hardware, tão somente a estrutura física básica de data center ou sala de dados: espaço físico e fornecimento de energia elétrica e refrigeração.

Compete à empresa todos os serviços e equipamentos para instalação, manutenção (preventiva e corretiva) e gerenciamento do enlace de dados dedicado e de sua infraestrutura, garantindo sua disponibilidade e seu adequado funcionamento de forma segura.

10.3 INFRAESTRUTURA ELÉTRICA

Por se tratar de contratação de soluções de segurança, não foram identificadas necessidades de adequações de infraestrutura elétrica.

10.4 LOGÍSTICA DE IMPLANTAÇÃO

Por tratar-se de serviços, não se aplica um planejamento logístico de implantação.

10.5 CAPACITAÇÃO OU TREINAMENTO

A empresa deve promover a capacitação e treinamento aos indicados pelo TRIBUNAL, de forma a permitir a plena gestão, entendimento, operação, monitoramento e otimização dos serviços e soluções objeto do contrato, na forma de reuniões, apresentações, documentação, relatórios e outros meios que se façam adequados.

11. CONTRATAÇÕES CORRELATAS

Durante os estudos não foram identificadas contratações correlatas ou interdependente que afetem a presente contratação pretendida.

12. IMPACTOS AMBIENTAIS

Durante os estudos não foi identificado nenhum impacto ambiental significativo.

13. POSICIONAMENTO CONCLUSIVO

O modelo atual de segurança está baseado em contratações de soluções de segurança. No entanto, a simples contração de soluções de segurança não exime a necessidade de pessoas para operá-los, monitoramento das ferramentas, integração, entre outros. Não é razoável que as soluções apresentem diversos alarmes e indicadores sem que se tenha o um servidor da SETI para tratar os alarmes ou observar os indicadores para identificação das ameaças no ambiente do Tribunal.

Verifica-se que o atual modelo de contratações, por meio da compra de produtos e contratação de serviços de operação, não é suficiente para fazer frente à velocidade com surgem novos tipos de ameaças.

No momento atual, a Divisão de Infraestrutura - DINFRA e a Divisão de Gestão de Segurança da Informação de TIC - DSEG não dispõem de quantitativos e nem de perfis profissionais suficientes para fornecer um serviço de segurança em regime de 24x7x365 dias.

Dessa forma, a contratação de empresa especializada para prestação de serviços de gerenciamento de soluções de segurança, de operação e resposta a requisições de segurança, monitoramento e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de risco e conformidade de segurança e privacidade, de inteligência aplicada à segurança, de testes de intrusão (*pentest*) é de fundamental importância para expansão dos mecanismos de proteção do Tribunal.

A solução de contratar empresa especializa traz a oportunidade do Tribunal de obter equipe técnica especializada para monitoramento de incidentes de segurança no período de 24x7 e 365 dias, com o objetivo de monitorar, identificar, avaliar e responder a incidentes de segurança da informação. É primordial aprimorar a atuação preventiva, elevando o grau de detecção de comportamentos anômalos e o desenvolvimento do processo de gestão de incidentes de segurança, agilizar a resposta a incidentes de segurança e melhorar a percepção de segurança perante os usuários do TJPR.

A contratação pretendida traz vantagens consideráveis, tais como:

- Maior flexibilidade com relação à aquisição de soluções de segurança da informação.
- Permite maior velocidade de inserção de soluções de segurança.
- Utilização de profissionais altamente capacitados e especialistas em cibersegurança, que dificilmente atuariam em um único cliente de pequeno porte.
- Monitoramento contínuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos os incidentes de segurança.
- Número de membros da equipe contratada suficiente para atender ao TJPR, frente aos desafios atuais.
- Equipe altamente capacitada e com expertise em segurança cibernética.
- Agregação de novas ferramentas e soluções trazidas ao ambiente do TJPR.
- Equipe para operacionalizar as ferramentas de segurança do Tribunal, realizando a sustentação contínua.
- Elevação do nível de segurança do Tribunal.
- Maximização da disponibilidade dos serviços de TIC oferecidos pelo TJPR.

Para que todo esse ecossistema funcionar, entre processos, ferramentas e especialistas é necessário de 08 a 12 pessoas, assim com o Gartner recomenda:

Baseado nas recomendações da Gartner, o estudo "Como planejar, projetar, operar e evoluir um SOC" publicado em 6 de setembro de 2018 (https://www.gartner.com/document/3889122?ref=cust_reco_sdemail&docType=RESEARCH), um dos pré-requisitos para implantar o SOC:

"um SOC 24/7 interno exigirá uma equipe de oito a 12 pessoas no mínimo. Se não houver esses recursos, comece seu planejamento de SOC com uma opção híbrida que depende substancialmente de um ou mais provedores de serviços, em particular para funções que precisam de cobertura 24 horas por dia, 7 dias por semana."

Outro ponto de convergência que justifica a expansão da segurança da informação no Tribunal é o alinhamento com diretrizes proferidas pelo Conselho Nacional de Justiça publicadas na Resolução nº 396, a qual instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Esta Resolução, visa garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro.

A Resolução nº 396/CNJ torna obrigatórias, entre outras medidas ligadas à segurança cibernética:

"Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

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;

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;

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;

V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos.

XI – realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; "

Para evolução da Segurança da Informação e Cibernética e aderência às recomendações do CNJ, o TRIBUNAL precisa realizar investimentos em pessoas, processos, soluções de segurança e gestão. O caminho visualizado pela SETI é a contratação de empresas especializadas, por meio de processo licitatório, onde já estão provedores de serviços capazes de prover e operacionalizar o estado da arte em tecnologias e processos para cibersegurança, atuando com equipes de profissionais especializados e experientes.

Por fim, entende-se que a contratação de empresa para serviços técnicos especializados de Segurança da Informação, é forma mais viável e adequada para atender as necessidades atuais na matéria de cibersegurança do Tribunal, permanecendo sob responsabilidade do quadro de servidores, as funções de gestão e de planejamento, intransferíveis para empresas terceirizadas.

14. ANEXOS

ANEXO I – LISTA DE POTENCIAIS FORNECEDORES

Fornecedor	Sítio	Telefone	E-mail	Contato
ISH	http://www.ish.com.br	61 9 8588-8888	helio.ferreira@ish.com.br	Hélio Ferreira
Under Protection	http://underprotection.com.br	48 99107-1843	emerson.ravaglio@underprotection.com.br	Emerson Ravaglio
Tripla Service	http://tripla.com.br	31 9 9878-0406	tveloso@tripla.com.br	Thiago Veloso
Future Tech	http://www.future.com.br	48 9 9164-8253	alexandre.seibert@future.com.br	Alexandre Seibert

Teletex	http://www.teletex.com.br	41 9 9155-7107	daniel.augusto@teletex.com.br	Daniel Augusto
Compwire	https://compwire.com.br	41 9 9914-0277 41 9 8801-1392	carlos.kuretzki@compwire.com.br	Carlos Henrique Kuretzki
Stefainini	http://www.stefaninirafael.com	41 9 9956-5687	lsbrasil@stefaninirafael.com	Linconln Brasil

Documento assinado eletronicamente por **LAURO ANDREY DE SOUZA BUENO**, **Chefe da Divisão de Gestão da Segurança da Informação**, em 13/11/2025, às 14:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ADRIANO WITKOVSKI**, **Técnico em Computação**, em 13/11/2025, às 14:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EDER SIBIRKIN**, **Técnico em Computação**, em 13/11/2025, às 14:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjpr.jus.br/validar informando o código verificador **12398584** e o código CRC **A8F44C0D**.