DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA (DOD) - TIC

1. IDENTIFICAÇÃO DA DEMANDA

Contratação de Serviços Gerenciados de Segurança da Informação, através de um Centro de Operações de Segurança (Security Operations Center - SOC), abrangendo atividades de monitoramento, detecção, análise e resposta de incidentes cibernéticos, incluindo gestão de vulnerabilidades, gerenciamento de patches, administração e supervisão de ferramentas de segurança (em modelo SaaS), testes de intrusão e simulações de ataques, dentre outros itens relacionados à segurança da informação, conforme exigências estabelecidas no Termo de Referência e seus Anexos.

1.1. Previsão para conclusão da contratação da Solução de TIC

PRAZOS NP 1.01 (Pregão Eletrônico)		
Descrição	**Prazo (dias úteis)**	**Previsão tramitação Processo**
Elaboração dos Artefatos da Contratação	20	18/09/2025
Pesquisa de Preços	11	03/10/2025
Solicita Reserva Orçamentária	2	07/10/2025
Impacto Orçamentário e Financeiro / Crédito Adicional	2	09/10/2025
Emissão da Reserva Orçamentária	2	13/10/2025
Elaboração do Edital e Anexos + Ratificação	5	20/10/2025
Parecer Jurídico sobre o Edital	3	23/10/2025
Verificação final e autorização da fase externa	2	27/10/2025
Publicação do Edital (**Pregão**)	10	10/11/2025
Parecer jurídico sobre a licitação (fase externa concluída)	4	14/11/2025
Adjudicação e Homologação	3	19/11/2025
Publicação do resultado + inserção do contrato	2	21/11/2025
Indicação de fiscais/gestores + solicitação de empenho	2	25/11/2025
Autorização para emissão de empenho + assinatura do contrato	3	28/11/2025
Emissão do empenho + assinatura da contratada	3	03/12/2025
Publicação do resumo do contrato/ARP	2	05/12/2025

Publicação do Ato de Designação dos Gestores/Fiscais	3	10/12/2025
PRAZO MÁXIMO DE 76 DIAS ÚTEIS		

1.2. Tipo de contratação da Solução de TIC

☑ Licitação ☐ Dispensa ☐ Inexigibilidade

1.3. Justificativa da necessidade

A presente contratação de serviços gerenciados de segurança da informação, com implantação e operação de Centro de Operações de Segurança, mostra-se necessária para elevar o nível de maturidade cibernética do TJES, assegurando a continuidade da prestação jurisdicional e a proteção de dados. O Tribunal possui Política de Segurança da Informação instituída, com objetivos e diretrizes voltados à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações, e com responsabilidades explícitas da STI quanto à implementação de controles e ao tratamento de incidentes. A contratação do SOC é instrumento para viabilizar, na prática, esses deveres institucionais e para consolidar a governança prevista na PSI (Política de Segurança da Informação).

Em âmbito nacional, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário, instituída pela Resolução CNJ nº 396/2021, tem por objetivo aprimorar o nível de maturidade em segurança cibernética nos órgãos do Judiciário, com abordagem de aspectos fundamentais de gestão de riscos, prevenção, detecção e resposta a incidentes. Os respectivos protocolos e manuais foram aprovados pela Portaria CNJ nº 162/2021, conferindo diretrizes operacionais para a implementação da ENSEC-PJ. A adoção do SOC alinha-se diretamente a esse marco normativo, como mecanismo estruturante para monitoramento contínuo, correlação de eventos e resposta coordenada.

No plano interno, o TJES instituiu a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais, por meio do Ato Normativo nº 124/2024, com atribuições de tratamento de incidentes, análise de artefatos maliciosos, gestão de vulnerabilidades e emissão de alertas. Trata-se de uma estrutura essencial, porém incipiente, cuja atuação ainda é tímida diante do crescente volume e sofisticação das ameaças. A contratação do SOC, com monitoramento 24x7 e serviços gerenciados especializados, funcionará como força multiplicadora da ETIR, provendo sensores, telemetria, orquestração, trilhas de auditoria e *playbooks* de resposta, de modo a acelerar a contenção de incidentes e a identificação de tendências.

A contratação também é necessária para robustecer a atuação do quadro técnico da STI. Hoje a equipe dedicada à segurança da informação é reduzida e acumula atividades críticas de gestão e fiscalização contratual, apoio técnico à elaboração de termos de referência, além do atendimento a incidentes e problemas operacionais. Mesmo com eventual ingresso de profissionais por designação temporária, não se obtém, no curto prazo, a especialização e a cobertura ininterrupta requeridas para atividades de *intelligence*, *threat hunting*, gestão contínua de vulnerabilidades e resposta a incidentes. A operação do SOC tende, inclusive, a revelar vulnerabilidades e correlações antes não monitoradas de forma integral, o que reforça a necessidade de investimento recorrente em segurança para tratamento e mitigação sustentados ao longo do tempo.

A solução proposta contribui diretamente para o cumprimento da Resolução TJES nº 06/2018, ao oferecer meios tecnológicos e processuais para a STI implementar controles, analisar e tratar incidentes e promover a continuidade dos serviços em caso de falhas graves, tudo em consonância com a PSI institucional. O SOC consolida práticas de controle de acesso, registro e auditoria, resposta a incidentes, gestão de continuidade e melhoria contínua, alinhando operação e governança às diretrizes internas.

A contratação está igualmente alinhada ao PROMOJUES, instituído pela Resolução nº 006/2023, que prevê investimentos em modernização tecnológica e segurança, inclusive com a implantação de serviços SOC, gestão de continuidade, gestão de vulnerabilidades e outras soluções em cibersegurança, financiadas no âmbito do Contrato de Empréstimo nº 5883/OC-BR. O SOC, portanto, é uma entrega coerente com o portfólio do Programa, elevando a resiliência do ecossistema de justiça eletrônico e contribuindo para a eficiência operacional na gestão judicial.

Em síntese, a necessidade é patente por razões técnicas e institucionais: atendimento às diretrizes da ENSEC-PJ, fortalecimento da ETIR, superação de restrições de pessoal e de ferramentas, cumprimento da PSI do TJES, e aderência ao escopo do PROMOJUES. O SOC proverá a camada de monitoração, correlação e resposta que hoje falta para assegurar a continuidade dos sistemas judiciais e a proteção das informações sob guarda do Tribunal.

1.4. Caracterização da demanda

Contratação de Serviços Gerenciados de Segurança da Informação, através de um Centro de Operações de Segurança (Security Operations Center - SOC), abrangendo atividades de

monitoramento, detecção, análise e resposta de incidentes cibernéticos, incluindo gestão de vulnerabilidades, gerenciamento de patches, administração e supervisão de ferramentas de segurança (em modelo SaaS), testes de intrusão e simulações de ataques, dentre outros itens relacionados à segurança da informação.

1.4.1. Descrição da demanda

Contratação de Serviços Gerenciados de Segurança da Informação, através de um Centro de Operações de Segurança (Security Operations Center - SOC).

1.4.2. Resultados a serem alcançados com a contratação

Com a contratação do Centro de Operações de Segurança (SOC), espera-se alcançar resultados concretos que fortaleçam a resiliência cibernética e assegurem a continuidade da prestação jurisdicional, dentre os quais destacam-se:

i. Elevação da maturidade em segurança da informação, mediante a adoção de práticas sistemáticas de monitoramento, detecção e resposta a incidentes;
ii. Redução do tempo de indisponibilidade de sistemas judiciais eletrônicos, em especial o Processo Judicial Eletrônico (PJe), por meio da resposta rápida e coordenada em eventuais ataques cibernéticos;
iii. Proteção contínua dos dados pessoais e sensíveis sob guarda do Tribunal, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
iv. Aprimoramento da atuação da ETIR do TJES, que contará com suporte especializado, telemetria avançada e processos de resposta estruturados, ampliando sua efetividade;
v. Identificação preventiva de vulnerabilidades e ameaças antes não monitoradas de forma integral, possibilitando mitigação antecipada de riscos;
vi. Fortalecimento do quadro técnico da STI, com apoio de serviços especializados que complementam a atuação interna e promovem a transferência de conhecimento;
vii. Cumprimento das diretrizes da Política de Segurança da Informação e da Resolução nº 06/2018, que estabelecem a necessidade de controles efetivos, análise e tratamento de incidentes;
viii. Alinhamento às estratégias nacionais de TIC no Judiciário (ENTIC-JUD e ENSEC-PJ), contribuindo para o incremento da governança e da proteção cibernética em nível institucional.

1.4.3. Alinhamento Estratégico

A presente demanda encontra-se plenamente alinhada ao Planejamento Estratégico do TJES (2021-2026), instituído pela Resolução nº 12/2021, atendendo aos seguintes objetivos e iniciativas estratégicas:

- AC.12.01 – Aperfeiçoar a governança e a gestão de TIC
- AC.12.01.002 – Aumentar o índice de Governança de TIC
- AC.12.01.003 – Buscar conformidade com normas e boas práticas de TIC
- AC.12.01.004 – Gerenciar e aprimorar os serviços de TI
- AC.12.02 – Aprimorar a segurança da informação e a gestão de dados
- AC.12.02.001 – Aprimorar a Segurança da Informação
- AC.12.02.002 – Implantar e gerenciar o atendimento à LGPD
- AC.12.03.001 – Elaborar e executar o Plano de Contratações de TIC
- AC.12.04.001 – Reduzir o tempo de atendimento às demandas de TIC dos usuários
- AC.09.01.003 – Dispor de infraestrutura que satisfaça as exigências operacionais

1.4.4. Quantidade prevista

Os itens são:

Torre de serviços 01 - Purple Team - Atendimento de requisições	
Item	**Descrição**
1	Serviço de Administração, Operação, Manutenção e Atendimento de Requisições
Torre de serviços 02 - Blue Team - Gestão de incidentes de segurança e monitoramento de ataques cibernéticos	
Item	**Descrição**
2	Serviço de gestão de vulnerabilidades
3	Serviço Gerenciado de Monitoramento, triagem, tratamento e resposta a ataques cibernéticos e incidentes de segurança
4	Gerenciamento da Orquestração e Automação de Resposta a incidentes (*Security Orchestration, Automation and Response* – SOAR)
5	Gerenciamento de Proteção Contra Riscos Digitais (*Digital Risk Protection* – DRP)

6	Gerenciamento de Patches (Patch Management)

Torre de serviços 03 - Red Team - Serviço de Testes de invasão (também conhecidos como Pentests ou Testes de Intrusão)	
Item	Descrição
1	*Gray Box* (Caixa Cinza)
2	*Black Box* (Caixa Preta)

1.4.5. Estimativa de custo

A estimativa de custos da contratação do Centro de Operações de Segurança (SOC) foi elaborada com base em parâmetros de mercado, considerando contratações recentes realizadas por outros Tribunais e propostas recebidas de fornecedores especializados em serviços de segurança cibernética.

Essas referências indicam que o custo global de soluções de SOC em regime de serviços gerenciados, com duração de 24 (vinte e quatro) meses, situa-se na faixa de R$ 14.000.000,00 (quatorze milhões de reais) a R$ 17.000.000,00 (dezessete milhões de reais). Esse montante corresponde a uma estimativa mensal entre R$ 583.000,00 (quinhentos e oitenta e três mil reais) e R$ 708.000,00 (setecentos e oito mil reais), abrangendo escopo que inclui monitoramento contínuo 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, gestão de vulnerabilidades, resposta a incidentes, threat intelligence, execução periódica de testes de intrusão e suporte técnico especializado.

Dessa forma, projeta-se que a contratação do SOC pelo TJES deverá se enquadrar nessa ordem de grandeza, cabendo ao Estudo Técnico Preliminar (ETP) consolidar a estimativa final a partir de pesquisa de preços atualizada junto ao mercado, em conformidade com a Resolução CNJ nº 468/2022.

1.4.6. Objetos interdependentes

Existe algum projeto em andamento relacionado a esta contratação?

☑ Não. ☐ Sim. Qual?

2. IDENTIFICAÇÃO DA DEMANDA NO PLANO DE CONTRATAÇÕES DE TIC 2025

2.1. Identificação da demanda no Plano de Contratações de STIC

Os itens que compõem a contratação estão previstos no Plano de Contratações da Secretaria de Tecnologia da Informação - PJES?

☑ Sim. Qual?

- Contratação de serviço especializado de Segurança da Informação

☐ Não. Motivo: Projeto previsto no PROMOJUES

2.2. Grau de Priorização

☐ Baixo ☐ Médio ☑ Alto

3. FONTE DE RECURSOS

Fonte(s) de Recursos	Elemento(s) de Despesa
☐ FUNEPJ - Fundo Especial do Poder Judiciário ☐ Tribunal de Justiça ☑ PROMOJUES	3.3.90.40.35

4. ÁREAS E INTEGRANTES DO PLANEJAMENTO DA CONTRATAÇÃO

4.1. Área Demandante

Secretaria de Tecnologia da Informação e Comunicação (STIC)

Responsável Área Demandante: Marcianne Ribeiro Antunes Lima

Matrícula: Telefone:

E-mail: mrlima@tjes.jus.br

4.2. Integrantes da Equipe de Planejamento da Contratação

4.2.1. Integrante Demandante

Nome: Marcianne Ribeiro Antunes Lima

E-mail: mrlima@tjes.jus.br

4.2.2. Integrante Técnico

Nome: Robson Limaverde Valença da Silva

gov.br Documento assinado digitalmente
ROBSON LIMAVERDE VALENCA DA SILVA
Data: 30/09/2025 13:25:23-0300
Verifique em https://validar.iti.gov.br

E-mail: rlsilva@tjes.jus.br

Nome: Luciano Carlos do Nascimento

gov.br Documento assinado digitalmente
LUCIANO CARLOS DO NASCIMENTO
Data: 30/09/2025 14:50:22-0300
Verifique em https://validar.iti.gov.br

Email: lucnascimento@tjes.jus.br

4.2.3. Integrante Administrativo

Nome: Marcia Marion Ballarini

gov.br Documento assinado digitalmente
MARCIA MARION BALLARINI
Data: 30/09/2025 13:11:41-0300
Verifique em https://validar.iti.gov.br

Email: mmballarini@tjes.jus.br

Nome: David Sudre de Andrade

gov.br Documento assinado digitalmente
DAVID SUDRE DE ANDRADE
Data: 30/09/2025 13:09:05-0300
Verifique em https://validar.iti.gov.br

Email: dasandrade@tjes.jus.br

gov.br Documento assinado digitalmente
MARCIANNE RIBEIRO ANTUNES LIMA
Data: 30/09/2025 16:10:38-0300
Verifique em https://validar.iti.gov.br

5. DISPOSITIVO FINAL

Os integrantes da Equipe de Planejamento da Contratação DECLARAM que tiveram ciência formalmente, via e-mail funcional, das suas indicações e das suas respectivas atribuições antes de serem formalmente designados.

Na oportunidade, submetemos à Autoridade Superior para decidir motivadamente sobre o prosseguimento da contratação, na forma que se pretende.

6. MANIFESTAÇÃO AUTORIDADE SUPERIOR

Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades identificadas pela área requisitante.

Encaminhem-se os autos à Secretaria Geral, a fim de que seja instituída a Equipe de Planejamento da Contratação, conforme indicação supra, com vistas ao cumprimento das demais etapas da Fase de Planejamento.