



TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR - ETP - TI - 25792271

(para contratação de soluções de TIC por licitação)

Para orientações quanto ao preenchimento do ETP, consultar o Guia de Contratações de TIC do Poder Judiciário ([anexo](#) da Resolução CNJ 468, de 2022) e, subsidiariamente, o Guia Referencial de Preenchimento do ETP do TRF1 (20487579)

ID (PAC):
1. Esta demanda está prevista no <i>Plano de Contratações Anual</i> - PCA 2026: • Link do PCA: https://www.trf1.jus.br/trf1/compras-licitacoes-e-contratos/plano-de-contratacoes-anual----pca • Unidade Requisitante: SECIN - DITEC - DIVISÃO DE TECNOLOGIA. • Id da Futura Contratação: TRF1_DITEC_0021_2026 • Classificação: TIC - Serviços de TIC - Serviços contínuos sem regime de dedicação exclusiva de mão-de-obra. • Descrição: Contrato de serviços gerenciados de segurança cibernética - Gestão de vulnerabilidades
1. DESCRIÇÃO SUCINTA DA NECESSIDADE
1.1. O presente Estudo Técnico Preliminar tem por objetivo demonstrar a necessidade de elevar a capacidade institucional do órgão gerenciador e dos órgãos participantes da futura IRP para identificar, avaliar, priorizar e acompanhar o tratamento de riscos relacionados às vulnerabilidades de segurança cibernética, ampliando a visibilidade sobre a exposição dos ambientes tecnológicos e reduzindo os riscos de incidentes de segurança, conforme descrito no Documento de Formalização da Demanda - DFD 1ª Região (20294280).
2. JUSTIFICATIVA EXPRESSA PARA A CONTRATAÇÃO
2.1. A segurança da informação é um pilar fundamental para a garantia da prestação jurisdicional contínua, íntegra e confiável. O Tribunal Regional Federal da 1ª Região (TRF1) manuseia um volume massivo de dados sensíveis e opera sistemas críticos para o funcionamento da Justiça Federal. O cenário de ameaças cibernéticas está em constante evolução, com ataques cada vez mais sofisticados direcionados a órgãos públicos, visando a interrupção de serviços, o sequestro de dados (<i>ransomware</i>) e a exploração de vulnerabilidades para ganhos ilícitos. 2.2.1. Além desse contexto, a ausência de um programa contínuo e estruturado de gestão de vulnerabilidades, conforme preconizado pelo Controle 7 do CIS Controls 8.1, impede que o Tribunal mantenha uma visão unificada dos riscos existentes em seus ativos tecnológicos. Esse cenário compromete a capacidade de resposta preventiva, aumenta o tempo de exposição a falhas críticas e impacta diretamente a continuidade da prestação jurisdicional, interferindo no acesso à justiça pelos cidadãos. 2.2. A ausência de uma ferramenta integrada e proativa para o gerenciamento de vulnerabilidades expõe o Tribunal a riscos significativos, como: 2.2.1. Interrupção de Serviços Críticos: A exploração de uma vulnerabilidade pode levar à indisponibilidade de sistemas judiciais, afetando o andamento

processual e o acesso à justiça.

2.2.2. Vazamento de Dados Sigilosos: Falhas de segurança podem permitir o acesso não autorizado a informações processuais, dados pessoais de magistrados, servidores e jurisdicionados, em violação à Lei Geral de Proteção de Dados (LGPD).

2.2.3. Danos à Imagem Institucional: Um incidente de segurança pode abalar a confiança da sociedade na capacidade do Judiciário de proteger suas informações.

2.3. A abrangência da solução proposta, que engloba quatro módulos essenciais, justifica-se pela complexidade do ambiente tecnológico do Tribunal e pela diversidade dos vetores de ataque modernos. Essa abordagem holística é crucial para garantir uma proteção completa e eficaz dos ativos críticos do TRF1. Cada componente aborda uma necessidade crítica e específica de segurança:

2.3.1. Análise de Ativos de Rede: Constitui a base da gestão de vulnerabilidades, permitindo identificar falhas em servidores, estações de trabalho, bancos de dados e dispositivos de rede. Sem essa visibilidade, o Tribunal permanece vulnerável a ataques tradicionais que exploram falhas de software não corrigidas.

2.3.2. Análise Dinâmica de Aplicações Web (DAST): Os sistemas web e portais do Judiciário são a principal interface com o público e advogados, tornando-se alvos primários. O módulo DAST é essencial para identificar vulnerabilidades específicas de aplicações, como injeção de código (*SQL Injection*) e *Cross-Site Scripting (XSS)*, que podem levar ao vazamento de dados processuais sigilosos e à desfiguração de páginas.

2.3.3. Segurança de Contêineres: Com a modernização e a adoção de práticas de DevOps, o uso de contêineres e orquestradores como Kubernetes torna-se comum. Este módulo é vital para garantir a segurança desde a imagem do contêiner até o ambiente de execução (*runtime*), prevenindo que vulnerabilidades no ecossistema de contêineres sejam exploradas para comprometer aplicações críticas.

2.3.4. Monitoramento de Identidades do Active Directory (AD): O AD é o coração da autenticação e autorização na rede do TRF1. Ataques sofisticados frequentemente visam explorar configurações inadequadas no AD para escalar privilégios e obter controle total do ambiente. Este módulo permite a identificação proativa de desvios de configuração, senhas fracas, contas privilegiadas em risco e outras falhas que poderiam ser a porta de entrada para um ataque devastador, como o "*Golden Ticket*". Neste requisito outros controles ainda serão implementados de forma complementar com a contratação de uma solução de PAM (*Privileged Access Management*).

2.4. Esta contratação é, portanto, essencial para elevar a maturidade da segurança cibernética do TRF1. A implementação de uma solução unificada permitirá a identificação e a priorização inteligente de vulnerabilidades, o que é fundamental para direcionar os esforços de correção pela equipe técnica, reduzindo a superfície de ataque e fortalecendo as defesas do Tribunal.

2.5. Adicionalmente, a aquisição está alinhada à **Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)**, instituída pela Resolução CNJ nº 396/2021. A ENSEC-PJ estabelece diretrizes para que os tribunais aprimorem seus níveis de maturidade em segurança, aumentem a resiliência contra ameaças e fortaleçam a governança de segurança. A solução a ser contratada é um instrumento direto para o cumprimento desses objetivos, em especial no que tange à prevenção e mitigação de ameaças.

2.6. O objetivo principal é elevar a maturidade da segurança cibernética da JF1, implementando uma solução unificada que permita identificar, priorizar e gerenciar vulnerabilidades de forma inteligente e automatizada, em conformidade com o Controle 7 do CIS Controls 8.1. Esta iniciativa visa reduzir a superfície de ataque, proteger os ativos de informação, assegurar a conformidade com normativas do CNJ (ex.: ENSEC-PJ) e otimizar o trabalho da equipe de segurança, direcionando o foco para a mitigação estratégica dos riscos mais relevantes. A presente contratação atenderá à demanda formalizada no Documento de Formalização da Demanda (DFD) Nº 20294280.

2.7. A proteção da infraestrutura de TI do TRF1 é fundamental para o interesse público, pois garante a continuidade, integridade e confiabilidade da prestação jurisdicional. A implementação desta solução visa assegurar que os sistemas judiciais permaneçam disponíveis e que o acesso à justiça não seja interrompido por incidentes cibernéticos. Além disso, a medida protege os dados sensíveis de magistrados, servidores e, principalmente, dos cidadãos, fortalecendo a confiança da sociedade na capacidade do Poder Judiciário de resguardar suas informações e cumprir sua missão de garantir uma prestação jurisdicional acessível, rápida e efetiva.

3. ALINHAMENTO COM OS INSTRUMENTOS DE PLANEJAMENTO

3.1. Plano Estratégico de Tecnologia da Informação da Justiça Federal – PETI para 2021-2026, aprovado pela resolução CJF-RES-2020/00685 de 15 de dezembro de 2020.

3.1.1. A ação está alinhada ao planejamento estratégico de TI da JF1.

3.1.2. Objetivo estratégico relacionado:

3.1.2.1. ID. 4 - Promover e fortalecer a segurança da informação digital na Justiça Federal.

3.2. Plano Diretor de Tecnologia da Informação da Justiça Federal da Primeira Região – PDTI-TRF1 2024-2026 (20506167), aprovado pelo Comitê de Governança de Tecnologia da Informação da Justiça Federal da 1ª Região – CGTI-JF1 - (0009898-93.2021.4.01.8000).

3.2.1. Iniciativa do PDTI relacionada: PDTI-2024-058 - Prover segurança da informação e sua sustentação.

3.3. Plano de Contratações de Soluções de TI da JF1 - PCSTI-JF1 2026 (25746759), aprovado pelo Comitê de Governança de Tecnologia da Informação da Justiça Federal da 1ª Região – CGTI-JF1 (0009898-93.2021.4.01.8000):

3.3.1. ID 60461 - Contrato de serviços gerenciados de segurança cibernética - Gestão de vulnerabilidades.

3.4. PLANEST 2021-2026 - Plano Estratégico da Justiça Federal da 1ª Região (13331340):

3.4.1. A iniciativa contribui diretamente para o alcance do objetivo estratégico "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados", que visa aprimorar a segurança e a governança da tecnologia da informação. Também suporta a missão do Tribunal de "Garantir à sociedade uma prestação jurisdicional acessível, rápida e efetiva", o que pressupõe a disponibilidade e a integridade dos sistemas judiciais.

3.5. Política de Governança e Gestão das Contratações da Justiça Federal da 1ª Região (13331340).

4. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS QUALITATIVOS

4.1. Análise das contratações anteriores

4.1.1. Não há registro de contratação anterior de uma solução com a abrangência e a integração pretendidas. A presente iniciativa representa um avanço estratégico, consolidando em uma única plataforma capacidades que antes eram tratadas de forma fragmentada ou inexistente.

4.2. Identificação das necessidades de negócio

4.2.1. Proteger os ativos de informação e a infraestrutura de TI do TRF1 contra ameaças cibernéticas.

4.2.2. Garantir a continuidade e a disponibilidade dos serviços judiciais digitais.

4.2.3. Assegurar a conformidade com a LGPD e com as normativas de segurança do CNJ (ENSEC-PJ).

4.2.4. Reduzir o risco operacional e de imagem associado a incidentes de segurança.

4.2.5. Otimizar o trabalho da equipe de segurança, automatizando a detecção e a

priorização de vulnerabilidades.

4.3. Identificação das necessidades tecnológicas

4.3.1. As necessidades tecnológicas estão detalhadas no **ANEXO I - Especificações Técnicas**. Em resumo, a solução deverá ser composta por uma plataforma integrada, podendo contemplar módulos de um ou mais fabricantes, desde que gerenciados de forma centralizada por meio de interface única ou integração nativa que assegure a consolidação das informações em console unificado, permitindo a correlação de dados e a automação de fluxos de forma transparente, não sendo aceito o simples compartilhamento de credenciais (Single Sign-On - SSO) sem a efetiva centralização e integração dos dados. A solução deverá ser baseada em nuvem e contemplar os módulos e capacidades requeridos neste Termo de Referência e em seu Anexo I.

4.3.1.1. **Gestão de Vulnerabilidades - Ativos de Rede:** Varreduras autenticadas e não autenticadas, agentes para coleta contínua, monitoramento passivo, cobertura de mais de **100.000 CVEs** e priorização de risco baseada em múltiplos fatores (CVSS, idade, exploits, etc.).

4.3.1.2. **Gestão de Vulnerabilidades -Análise Dinâmica de Aplicações Web (DAST):** Análise de aplicações web e APIs, suporte a tecnologias modernas (SOAP, REST), integração com Selenium e Postman, e fornecimento de evidências detalhadas de vulnerabilidades.

4.3.1.3. **Gestão de Vulnerabilidades - Segurança de Contêineres:** Análise de imagens e de ambientes de execução (*runtime*) em clusters Kubernetes, com suporte a ambientes on-premises e em nuvem.

4.3.1.4. **Gestão de Vulnerabilidades - Monitoramento de Identidades do MS Active Directory:** Análise contínua de configurações do AD para identificar falhas de segurança, como senhas fracas, contas inativas, delegações perigosas e verificação da idade da senha da conta KRBTGT.

4.3.1.5. **Requisitos Gerais:** A solução deve ser em nuvem pública (SaaS), com autenticação multifatorial (MFA), logs de auditoria imutáveis, APIs para integração, segregação de acesso (RBAC) e hospedagem em nuvem no Brasil ou em país com decisão de adequação da Autoridade Nacional de Proteção de Dados (ANPD). A Contratada e o fabricante devem garantir a submissão exclusiva dos dados à jurisdição brasileira.

4.4. Demais requisitos necessários e suficientes à escolha da solução de TI

4.4.1. Identificação de critérios e práticas sustentáveis

4.4.1.1. Por se tratar de contratação de empresa especializada na disponibilização de **Solução de Gestão de Vulnerabilidades, na modalidade de Software como Serviço (SaaS)**, observadas as normas vigentes relativas ao desenvolvimento sustentável nas licitações e contratações públicas, bem como o Plano de Sustentabilidade do Tribunal Regional Federal da 1ª Região (PORTARIA PRESI 340/2021), disponível no sítio: <https://portal.trf1.jus.br>. Destaca-se que a própria natureza do SaaS contribui intrinsecamente para as práticas de sustentabilidade, ao otimizar o uso de recursos computacionais e reduzir a pegada de carbono da infraestrutura on-premises do Tribunal, tornando-se, assim, uma escolha alinhada aos princípios de sustentabilidade.

4.4.2. Identificação de critérios de acessibilidade

4.4.2.1. Considerando a natureza técnica especializada da solução de gerenciamento de vulnerabilidades, que consiste em ferramenta de análise e diagnóstico de segurança cibernética destinada exclusivamente a técnicos qualificados da área de segurança da informação;

4.4.2.2. Considerando que a interface principal da solução compreende dashboards técnicos com visualizações complexas (mapas de superfície de ataque, grafos de dependências, tabelas de vulnerabilidades com múltiplas

dimensões) que não possuem tradução adequada para tecnologias assistivas sem perda substancial de funcionalidade crítica;

4.4.2.3. Considerando que o público-alvo restringe-se a profissionais técnicos de segurança cibernética, não incluindo cidadãos, jurisdicionados ou servidores sem conhecimento especializado na área;

4.4.2.4. Declare-se que os requisitos de acessibilidade eMAG e WCAG não se aplicam ao objeto desta contratação, por tratar-se de ferramenta técnica especializada com interface restrita a usuários qualificados, em conformidade com o princípio da proporcionalidade e mediante fundamentação técnica expressa.

4.4.3. Contratações correlatas e/ou interdependentes

4.4.3.1. Contrato Nº 29/2022 (0008841-11.2019.4.01.8000), celebrado com a **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, para prestação de serviços de soluções de tecnologia voltadas à segurança da informação.

4.4.3.1.1. Prazo de vigência previsto até **01/08/2027**, conforme Termo Aditivo Nº 4 (documento SEI 25580955).

4.4.3.1.2. O objeto desse contrato inclui serviços de pentest externo, cuja descoberta de vulnerabilidades no ambiente integram-se ao processo de gestão de vulnerabilidades previsto no escopo dessa nova contratação.

4.4.3.2. Contrato Nº 42/2022 (0022754-84.2024.4.01.8000), celebrado com a **INTEROP INFORMÁTICA LTDA**, para prestação de serviços técnicos avançados na área de Tecnologia da Informação - TI e sustentação da infraestrutura de TI do Contratante e de suas Seções e Subseções Judiciárias, com pagamento fixo mensal, vinculado aos níveis mínimos de serviços, conforme especificações e condições constantes.

4.4.3.2.1. Este instrumento tem seu término previsto para **12/03/2027**.

4.4.3.2.2. Relação específica com o **Item 6**, que abrange serviços de segurança de redes para toda a JF1, considerando que a solução a ser contratada terá interdependência com toda a infraestrutura de rede e segurança existente no TRF1. Salienta-se a necessidade de configuração de regras de firewall para permitir a comunicação entre os sensores/agentes internos e a plataforma em nuvem. Além disso, um dos requisitos da solução é possuir uma API robusta para futuras integrações com outras ferramentas de segurança, como SIEM (Security Information and Event Management) e EDR (Endpoint Detection and Response), potencializando o ecossistema de cibersegurança do Tribunal.

4.4.4. Requisitos Legais

4.4.4.1. Leis e Decretos:

4.4.4.1.1. [Lei n. 14.133/2021](#) - Lei de Licitações e Contratos Administrativos.

4.4.4.1.2. [Lei n. 13.709/2018](#) - Lei Geral de Proteção de Dados Pessoais (LGPD).

4.4.4.2. Normas específicas para contratações de TI:

4.4.4.2.1. [Instrução Normativa n. 65/2021 SGD/ME](#) - Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

4.4.4.2.2. [Instrução Normativa n. 94/2022 SGD/ME](#) - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de

4.4.4.3. Normas do Conselho Nacional de Justiça - CNJ:

4.4.4.3.1. [Resolução CNJ n. 347/2020](#) - Dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário.

4.4.4.3.2. [Resolução CNJ n. 363/2021](#) - Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

4.4.4.3.3. [Resolução CNJ n. 370/2021](#) - Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

4.4.4.3.4. [Resolução CNJ n. 468/2022](#) - Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.

4.4.4.3.5. [Resolução CNJ n. 400/2021](#) - Dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

4.4.4.3.6. [Resolução Nº 396](#) - Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

4.4.4.4. Normas do Conselho de Justiça Federal - CJF:

4.4.4.4.1. [Resolução CJF n.685/2020](#) - Dispõe do Plano Estratégico de Tecnologia da Informação da Justiça Federal (PETI) para 2021-2026.

4.4.4.4.2. [Resolução CJF n. 687/2020](#) - Dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus.

4.4.4.4.3. [Resolução CJF n. 709/2021](#) c/c [Portaria CJF n. 96/2023](#) - Dispõe sobre a Política de Sustentabilidade da Justiça Federal – PSJF e o Manual de Sustentabilidade nas Compras e Contratações do Conselho da Justiça Federal – 2ª Edição.

4.4.4.4.4. [Portaria CJF n. 232/2023](#) - Dispõe sobre as etapas do planejamento das contratações de bens e serviços fundamentadas por meio da Lei n. 14.133, de 1º de abril de 2021, no âmbito do Conselho da Justiça Federal.

4.4.4.4.5. [Instrução Normativa CJF n. 12/2022](#) - Dispõe sobre a definição dos serviços e fornecimentos contínuos no âmbito do Conselho da Justiça Federal, para fins de aplicação à Lei n. 14.133, de 1º de abril de 2021.

4.4.4.5. Normas da Justiça Federal da 1ª Região:

4.4.4.5.1. [Resolução PRESI n. 36/2021](#) - Institui a Política de Governança e Gestão das Contratações da Justiça Federal da 1ª Região.

4.4.5. Requisitos de manutenção

4.4.5.1. O serviço de suporte técnico deverá garantir o funcionamento e a manutenção dos produtos contratados, além do fornecimento de novas versões, atualizações (updates) e aprimoramentos (upgrades).

4.4.5.2. O atendimento do suporte, incluindo telefone, e-mail e outros canais que se fizerem necessários, deverá ser prestado no idioma português do Brasil.

4.4.5.3. Os prazos de atendimento e informações sobre Níveis Mínimos de Serviço estão descritos no subitem 4.4.9.

4.4.5.4. A Contratada deverá informar à Contratante a página na Internet que hospeda as informações do fabricante do software, contendo as últimas versões dos softwares, informações sobre correções de falhas, procedimentos para reporte de problemas e documentação técnica detalhada dos produtos

contratados.

4.4.5.5. Demais requisitos de manutenção estão detalhados no Anexo I.

4.4.6. Requisitos temporais

4.4.6.1. O início da execução ocorrerá a partir da emissão da correspondente ordem de fornecimento e/ou ordem de serviço pelo órgão demandante, observado o prazo de disponibilização previsto no Termo de Referência e no futuro instrumento contratual decorrente da ata de registro de preços.

4.4.6.2. Nos casos de contratação pelos órgãos participantes, o marco inicial da execução será contado da respectiva formalização contratual, preservadas as condições registradas em ata.

4.4.7. Requisitos de segurança

4.4.7.1. Na execução do objeto, além das cláusulas padrão de conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018) e a Lei de Acesso à Informação (Lei 12.527/2011), a solução e os serviços prestados devem atender aos seguintes requisitos de segurança:

4.4.7.1.1. **Jurisdição e Soberania de Dados:** A solução deve ser hospedada em nuvem pública com data centers no Brasil ou em países com decisão de adequação da ANPD. A CONTRATADA e o fabricante devem assegurar que todos os dados gerados e armazenados estão sujeitos exclusivamente à jurisdição das leis e tribunais brasileiros. Qualquer solicitação de acesso por entidades estrangeiras será considerada ilegítima, sendo a CONTRATADA integralmente responsável por quaisquer danos ou prejuízos decorrentes de sua violação ou não cumprimento.

4.4.7.1.2. **Proibição de Backdoors:** A CONTRATADA e o fabricante devem declarar que a solução não possui mecanismos ocultos de acesso (*backdoors*) e se comprometer a não inserir tais funcionalidades.

4.4.7.1.3. **Criptografia:** A solução deve fornecer criptografia de ponta a ponta para todas as comunicações entre agentes, scanners e a plataforma em nuvem.

4.4.7.1.4. **Auditoria Imutável:** Os registros de auditoria das atividades dos usuários na plataforma devem ser livres de alteração e deleção.

4.4.7.2. A contratada obriga-se a dar conhecimento formal a seus prepostos, empregados ou colaboradores das disposições relacionadas à proteção de dados e a informações sigilosas, na forma da Lei 13.709/2018 (LGPD), da Resolução/ CNJ 363/2021 e da Lei 12.527/2011.

4.4.7.2.1. Obriga-se também a comunicar à Administração, em até 03 (três) dias úteis, contadas do instante do conhecimento, a ocorrência de acessos não autorizados a dados pessoais, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer outra forma de tratamento inadequado, suspeito ou ilícito, sem prejuízo das medidas previstas no art. 48 da Lei 13.709/2018 (LGPD).

4.4.7.3. O tratamento de dados pessoais dar-se-á de acordo com os princípios e as hipóteses previstas nos arts. 6º, 7º e 11 da Lei 13.709/2018 (LGPD), limitado ao estritamente necessário à consecução do objeto, na forma deste instrumento e seus anexos.

4.4.7.4. É vedado, na execução do ajuste, revelar, copiar, transmitir, reproduzir, transportar ou utilizar dados pessoais ou informações sigilosas a que tiver acesso prepostos, empregados ou colaboradores direta ou indiretamente envolvidos na realização de serviços, produção ou fornecimento de bens. Para tanto, devem ser observados as medidas e os procedimentos de segurança das informações resultantes da aplicação da Lei 13.709/2018 (LGPD) e do parágrafo único do art. 26 da Lei 12.527/2011.

4.4.7.5. Em razão do vínculo mantido, na hipótese de dano patrimonial, moral,

individual ou coletivo decorrente de violação à legislação de proteção de dados pessoais ou de indevido acesso a informações sigilosas ou transmissão destas por qualquer meio, a responsabilização dar-se-á na forma da Lei 13.709/2018 (LGPD) e da Lei 12.527/2011.

4.4.7.6. Extinto o ajuste ou alcançado o objeto que encerre tratamento de dados, estes serão eliminados, inclusive toda e qualquer cópia deles porventura existente, seja em formato físico ou digital, autorizada a conservação conforme as hipóteses previstas no art. 16 da Lei 13.709/2018 (LGPD).

4.4.7.7. Parcela importante dos dados que circulam nos sistemas de informações do TRF1 são de caráter sigiloso e, portanto, os processos de tratamento de incidentes cibernéticos, precisam ser seguros e resilientes a ataques cibernéticos.

4.4.7.8. É extremamente necessário que sejam observadas todas as diretrizes de segurança da informação definidas pelo TRF1, bem como os normativos, padrões e processos internos e da Justiça Federal aplicáveis. Devem ser seguidas boas práticas de tratamento de incidentes cibernéticos.

4.4.8. Requisitos de capacitação

4.4.8.1. Os requisitos de capacitação técnica estão especificados no **item 5 do Anexo I** deste documento.

4.4.9. Requisitos de Níveis Mínimos de Serviço

4.4.9.1. O suporte técnico da contratação será prestado em duas camadas complementares:

I – suporte tecnológico inerente às subscrições dos itens 1, 2,3 e 4;

II – suporte técnico unificado especializado, objeto do item 6, prestado conforme demanda da Administração.

4.4.9.2. O suporte técnico especializado deverá ser prestado por profissionais qualificados, por canais de atendimento adequados à abertura, acompanhamento e encerramento de chamados, com registro das ocorrências e rastreabilidade dos atendimentos, observados os níveis de serviço, prazos, horários, canais e demais condições estabelecidas no item 10.5 deste Termo de Referência.

4.4.9.3. Os chamados deverão ser tratados e encerrados conforme os procedimentos, critérios de atendimento, prazos e condições estabelecidos no item 10.5 deste Termo de Referência.

4.4.9.4. No contexto da IRP, a prestação do suporte deverá ser compatível com a utilização da solução pelo órgão gerenciador e pelos órgãos participantes, observados os quantitativos contratados por cada órgão.

5. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

A estimativa da demanda foi elaborada com base na consolidação das necessidades do órgão gerenciador (TRF1) e dos órgãos participantes, fundamentada em inventários institucionais, bases corporativas de ativos e portfólio de aplicações. Para mitigar o risco de superdimensionamento e atender ao **Acórdão 2.569/2018-TCU-Plenário**, a contratação utilizará o **Sistema de Registro de Preços (SRP)**, permitindo que a aquisição ocorra no momento oportuno e de acordo com a evolução real do parque tecnológico e as condições de implantação das equipes envolvidas.

5.1. Comparativo Histórico e Evolução do Parque Tecnológico: Os quantitativos foram projetados considerando a série histórica de ativos e o crescimento vegetativo esperado para os próximos 36 meses, incluindo projetos estratégicos como a migração do SEI para a nuvem e a construção do novo Datacenter.

5.1.1. ITEM 1 - Quantidade de Ativos de Rede:

5.1.1.1. O quantitativo estimado de **4.000 (quatro mil) ativos** foi definido com base no levantamento do parque tecnológico atualmente existente na

Justiça Federal da 1ª Região, utilizando-se informações fornecidas pelas unidades técnicas responsáveis pela gestão dos ativos de rede, servidores e estações de trabalho.

5.1.1.2. Os levantamentos realizados demonstram que a JF1 possui um universo significativamente superior ao quantitativo previsto para contratação. Entretanto, o objeto não pressupõe, necessariamente, a análise integral e simultânea de todos os ativos existentes, uma vez que a execução dos serviços será iniciada mediante análise por amostragem, observadas as características, a criticidade e a representatividade dos ambientes avaliados.

5.1.1.3. O quantitativo de 4.000 ativos representa, portanto, uma **estimativa de demanda para execução dos serviços durante a vigência da contratação**, e não o quantitativo total de equipamentos existentes no parque tecnológico da JF1.

5.1.1.4. A estimativa considera:

5.1.1.4.1. O quantitativo de ativos atualmente identificados nos levantamentos realizados pelas áreas técnicas;

5.1.1.4.2. A realização inicial de análise por amostragem dos ambientes;

5.1.1.4.3. A possibilidade de ampliação da amostra sempre que os resultados obtidos demonstrarem a necessidade de aprofundamento ou extensão da análise;

5.1.1.4.4. A inclusão de ativos relacionados a novos projetos, expansões de infraestrutura ou alterações relevantes no ambiente tecnológico;

5.1.1.4.5. O crescimento vegetativo do parque tecnológico durante a vigência da contratação; e

5.1.1.4.5.6. A necessidade de manutenção de margem suficiente para atendimento de demandas supervenientes, sem a necessidade de realização de nova contratação exclusivamente em razão da expansão do ambiente.

5.1.1.5. Dessa forma, embora o levantamento atual identifique um universo superior a **16.856 ativos**, a contratação de **4.000 ativos** corresponde ao quantitativo estimado necessário para atender às análises efetivamente demandadas durante a vigência contratual, considerando a metodologia de amostragem inicialmente prevista e a possibilidade de ampliação do escopo conforme a necessidade técnica identificada.

Tipo de ativo	Fonte do levantamento	Quantitativo atualmente identificado	Critério utilizado para estimativa da contratação	Quantidade solicitada
Ativos de Rede	SERED 25788732	*1.599	Análise inicial por amostragem, com possibilidade de ampliação conforme a necessidade técnica identificada durante a execução contratual.	Composição do quantitativo global
Servidores Virtuais	SETAV 25787619	**1.623	Análise inicial por amostragem dos ambientes e ativos representativos, podendo ser ampliada conforme os resultados obtidos e a necessidade de aprofundamento da análise.	Composição do quantitativo global
Microcomputadores	DIATU 25790352	***13.634	Análise inicial por amostragem, considerando a diversidade dos ambientes e a possibilidade de ampliação do	Composição do quantitativo

			quantitativo analisado conforme a necessidade identificada.	global
Total	Levantamentos das áreas técnicas	16.856	Estimativa da demanda a ser atendida durante a vigência contratual, considerando a metodologia de amostragem, eventual ampliação das análises, novos projetos e crescimento vegetativo do parque tecnológico.	4.000

***Ativos de Rede:** Informação obtida diretamente com a SERED, em 27/08/2026, mediante disponibilização da Planilha Ativos de rede e Circuitos JF1 (25788732), contendo os dados dos ativos de rede e circuitos disponíveis na JF1, levantados com base na última atualização das informações relativas aos equipamentos das Seções e Subseções Judiciárias.

****Servidores Virtuais:** Informação obtida diretamente com a SETAV, em 27/08/2026, por meio do relatório **Inventory Report**, extraído do VMware vCenter, conforme Documento Quantitativo Servidores Virtuais - vCenter - 27-08 (25787619).

*****Microcomputadores:** Considerando que o SICAM disponibiliza à DIATU apenas as informações referentes aos microcomputadores do Tribunal Regional Federal da 1ª Região - TRF1, não abrangendo os equipamentos das Seções e Subseções Judiciárias vinculadas à JF1, a utilização desse sistema não permite a obtenção de um quantitativo consolidado de microcomputadores de toda a Justiça Federal da 1ª Região. Diante dessa limitação, conforme informação prestada pela DIATU em 27/08/2026, adotou-se como parâmetro para estimativa do quantitativo de Microcomputadores da JF1 o número de usuários contemplados no processo administrativo PAe nº (0008493-46.2026.4.01.8000), especialmente no Estudo Técnico Preliminar - ETP - TI nº (25637566), que prevê a contratação de 12.427 licenças Microsoft Office 365 E1 e 1.207 licenças Microsoft Office 365 E3, totalizando 13.634 licenças.

5.1.2. ITEM 2 - Quantidade de Aplicações: A quantidade de licenças para DAST foi fixada em **100 aplicações** visando otimização de custos. Esta decisão foi acompanhada de uma análise de risco que considera a possibilidade de realocar licenças entre as 259 aplicações existentes, permitindo uma cobertura rotativa e priorizada para as mais críticas. Os resultados dos testes são exportados para PDF e armazenados para fins de auditoria e comparativo futuro, gerenciando assim o risco da não cobertura simultânea de todo o parque. Essa abordagem permite uma análise aprofundada das aplicações mais sensíveis, com planos de expansão gradual da cobertura conforme a evolução da maturidade do processo e a disponibilidade orçamentária.

Descrição do Ativo para licitação	Descrição interna do ativo	Quantidade Estimada 2021 (Termo de Referência 12611203 - contratação da GLOBALWEB	Quantidade Estimada 2024 (ETP TI 20200433 - contratação da INTEROP)	Quantidade Estimada na Consolidação 2283529 do PAe (0008258-16.2025.4.01.8000)	Média	Quantidade solicitada
Aplicações Web	Aplicações Web (JBoss, Tomcat, Apache)	147	187	259	198	100

5.1.3. ITEM 3 - Quantidade de worker nodes: Os *worker nodes* representam a quantidade aproximada de máquinas com contêineres necessários, considerando ainda o projeto de ampliação está em andamento, podendo atingir mais de 100 aplicações que hoje rodam em máquinas virtuais tradicionais, conforme estimativa de 145 sistemas atualmente em operação no TRF1 (Despacho 25137508)

Descrição do Ativo para	Descrição interna do ativo	Quantidade Estimada 2021 (Termo de Referência 12611203 -	Quantidade Estimada 2024 (ETP TI 20200433 -	Quantidade Estimada na Consolidação 22835 do PAe (0008258-	Quantidade solicitada
-------------------------	----------------------------	--	---	--	-----------------------

licitação	contratação da GLOBALWEB)		contratação da 16.2025.4.01.8000) INTEROP)		
Worker Nodes	Servidores DOCKER	42	-	42	100

5.1.4. **ITEM 4 - Quantidade de usuários:** Os quantitativos foram verificados por meio do serviço Wazuh para os controladores de domínio e por consulta por scripts para cálculo dos usuários.

Descrição do Ativo para licitação	Descrição interna do ativo	Usuário Ativos em janeiro/2025	Usuário em novembro 01 a 11/2025	Variação	Estimativa de Variação para os próximos 36 meses	Estimativa de Quantidade Total em 36 meses	Quantidade solicitada (36 meses)
Usuários	Usuários do AD	14.180	14.623	+ 443 (3,12%)	456 (3,12%) + 470 (3,12%) + 485 (3,12%)	15.079 (Ano 1) => 15.549 (Ano 2) => 16.034 (Ano 3)	16.000

5.1.5. **ITEM 5 - Treinamento:** Projeta-se a capacitação de 2 (dois) Servidores de cada Seccional e outros 24 servidores pertencentes à COINT/COSIS de forma a integrar o uso da ferramenta aos processos de trabalho das equipes. Para estimar esses valores consideramos o PAe (0008258-16.2025.4.01.8000) - Consolidação (22835297), o qual lista o quantitativo de servidores de TI em cada localidade. Sendo assim, são necessárias cerca de 5 turmas com 10 pessoas cada para suprir a demanda.

5.2. Dimensionamento/Quantitativos:

5.2.1. **Premissas e base de inventário:** O dimensionamento foi elaborado a partir do inventário institucional disponível de cada órgão.

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMADA		
				POR ÓRGÃO		TOTAL
1	1	Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	Licença por ativo de rede/ano	TRF1	4.000	7.000
				TRF2	3.000	
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	Licença por aplicação web/ano	TRF1	100	160
				TRF2	60	
	3	Licenciamento de Segurança de Contêineres	Licença por <i>worker node (kubernetes)</i> /ano	TRF1	100	140
				TRF2	40	
	4	Licenciamento para Gestão de Postura de Identidade (ISPM)	Licença por usuário (grupo de 1000 usuários monitorados)/ano	TRF1	16	32
				TRF2	16	
	5	Treinamento Técnico para Administração da Solução	Turma (grupo de 10 usuários por turma)	TRF1	5	8
				TRF2	3	
	6	Serviço de Suporte Técnico	Unidade de Suporte por Ativo Equivalente (USAE)/mês	TRF1	4.780	8.200
				TRF2	3.420	

5.2.2. **CrITÉrios de contagem de licenÇas:** Para fins de contratação, considere-se:

5.2.2.1. Ativo de rede: qualquer elemento com identificação única (IP/hostname) passível de varredura (autenticada e/ou não autenticada), excluÍdas duplicidades (ex.: interfaces secundárias e IPs temporários) **OU** qualquer dispositivo com endereço IP gerenciado pela soluÇão, incluindo servidores, estaÇões de trabalho, dispositivos de rede e equipamentos de armazenamento.

5.2.2.2. Aplicação web: a unidade identificável por URL base e fluxo de autenticação/teste (incluindo APIs quando aplicável), evitando contagem por páginas ou submódulos **OU** qualquer aplicação web, portal ou API REST/SOAP analisada pelo módulo DAST;

5.2.2.3. Worker node: o nó de execução com capacidade de hospedar workloads do cluster dentro do escopo definido (produção e, quando aplicável, homologação) **OU** cada nó de processamento em ambiente de contêineres ou cluster Kubernetes gerenciado pela solução;

5.2.2.4. Usuário: qualquer usuário ativo existente no ambiente do Active Directory (AD) ou do EntraID.

5.2.3. Margem de crescimento: Adotou-se a variação dos últimos anos como margem de crescimento para a estimativa das quantidades.

5.3. Critérios de priorização DAST: como não serão incluídas todas as aplicações, então, definiu-se alguns critérios para priorização delas. Contudo, a lista nominal de aplicações poderá ser atualizada pela fiscalização ao longo da execução, mantendo o limite contratado.

5.3.1. Critérios de priorização de aplicações para DAST (cobertura inicial): Serão priorizadas aplicações com:

5.3.1.1. exposição externa/internet;

5.3.1.2. tratamento de dados pessoais/sensíveis;

5.3.1.3. criticidade institucional (serviços essenciais);

5.3.1.4. maior volume de acessos;

5.3.1.5. histórico de incidentes/vulnerabilidades;

5.3.1.6. maior frequência de mudanças (risco de regressão).

5.4. Justificativa para inclusão do treinamento no mesmo grupo/lote: O treinamento é componente indissociável da solução, pois a operação segura e efetiva da plataforma depende de parametrizações e práticas específicas do fabricante (políticas de varredura, autenticação, gestão de credenciais, RBAC/MFA, integrações e interpretação de evidências). A contratação conjunta assegura transferência de conhecimento no momento adequado (implantação/configuração), reduz risco de implantação e de uso inadequado que comprometa os resultados, e preserva continuidade operacional, evitando que a solução seja disponibilizada sem a capacitação mínima necessária para sua governança e uso seguro.

5.5. Métrica de dimensionamento do Item 6 (USAE): Para fins de dimensionamento do Item 6 – Serviço de Suporte Técnico Unificado, adota-se a métrica USAE – Unidade de Suporte por Ativo Equivalente, destinada a normalizar o esforço técnico de suporte em razão da heterogeneidade dos ativos abrangidos pela contratação.

a) **Ativo de Rede (Host):** Mantém o peso base de 1, representando a complexidade média e servindo como referência para varreduras padrão.

b) **Aplicação Web:** O peso de 3 reflete a alta complexidade devido à diversidade de tecnologias, fluxos de autenticação, análise de código e potencial de impacto em sistemas críticos.

c) **Worker Node Container:** O peso de 4 enfatiza a complexidade adicional advinda da natureza efêmera, orquestração (Kubernetes), integração com pipelines de CI/CD e múltiplas camadas de análise em ambientes de containers.

d) **Identidade (MS Active Directory):** O peso de 5 reforça a classificação de "Muito Alta" complexidade. A criticidade do AD como pilar central de autenticação, a profundidade do conhecimento técnico especializado exigido para compreender suas nuances e vetores de ataque, e o potencial de impacto catastrófico justificam essa ponderação significativamente maior.

5.5.1. Os pesos técnicos da métrica USAE serão:

- a) Ativo de Rede = peso 1;
- b) Aplicação Web = peso 3;
- c) Worker Node = peso 4;
- d) Unidade de Monitoramento AD = peso 5.

5.5.2. O cálculo do total de USAE observará a fórmula: **USAE Total = Σ (Quantidade do Ativo $\times$ Peso de Complexidade).**

5.5.3. O valor mensal estimado do Item 6 corresponderá a: **Valor Mensal do Suporte = Total de USAE contratados $\times$ Preço Unitário do USAE.**

5.5.4. Justificativa técnica da métrica USAE: A adoção da métrica USAE permite normalizar, em uma base única, ativos com diferentes níveis de complexidade de suporte, refletindo de forma mais fiel o esforço operacional exigido para a sustentação da solução. Essa abordagem assegura:

- a) simplificação administrativa, ao evitar a proliferação de itens de suporte por tecnologia;
- b) transparência e comparabilidade entre propostas;
- c) equidade na precificação, ao relacionar custo com complexidade técnica;
- d) escalabilidade contratual, permitindo aumento ou redução de volumetria com impacto financeiro objetivo;
- e) melhor adequação ao contexto da IRP, em que a demanda precisa ser consolidada e, depois, executada por diferentes órgãos sem ruptura da modelagem contratual.

5.5.5. Memória de Cálculo — Quantitativos e USAE

5.5.5.1 Para demonstrar a composição e a memória de cálculo que resulta no total de 4.780 USAEs (Unidades de Suporte e Atendimento Especializado) no item 5.5 do ETP (órgão TRF1), organizamos os quantitativos de ativos (Tabela 5.2.1) aplicados aos respectivos fatores de conversão/ponderação de cada categoria de recurso.

5.5.5.2 A fórmula de conversão aplica o peso/fator de complexidade de suporte sobre o quantitativo de cada ativo/escopo contratado:

USAE Total = Σ (Quantidade do Ativo $\times$ Peso de Complexidade).

5.5.5.3. Tabela Demonstração do Cálculo de USAEs por Categoria de Ativo e Órgão (TRF1 e TRF2)

Item/Categoria do Escopo	Fator de Ponderação (USAE)	Qtd. Ativos (TRF1)	USAE (TRF1)	Qtd. Ativos (TRF2)	USAE (TRF2)	Qtd. Total Ativos	Quantidade Total USAE
Ativos de Rede/ Servidores/Workstations	1,0	4.000	4.000	3.000	3.000	7.000	7.000
Aplicações Web/ Serviços HTTP(S)	3,0	100	300	60	180	160	480
Worker Nodes (Contêineres/ Nuvem)	4,0	100	400	40	160	140	560
Licenciamento para Gestão de Postura de Identidade (ISPM)	5,0	16	80	16	80	32	160
Unidade de Suporte por Ativo Equivalente (USAE)/mês	1,0	-	4.780	-	3.420	-	8.200

6. ANÁLISE DE SOLUÇÕES POSSÍVEIS

6.1. Identificação das soluções

A análise de soluções foi estruturada em três cenários distintos, que representam as principais abordagens para a implementação de uma capacidade de gerenciamento de vulnerabilidades.

Cenário	Descrição das alternativas de solução	Fontes de consulta (órgãos públicos que	Link das consultas
---------	---------------------------------------	---	--------------------

nº	disponíveis no mercado	adotaram a solução, fornecedores etc.)	(doc. SEI)
CENÁRIO 1	UTILIZAÇÃO DE SOLUÇÃO OPEN SOURCE, IMPLEMENTADA E OPERADA PELA EQUIPE DE SEGURANÇA DO TRIBUNAL	INVIÁVEL TECNICAMENTE E ECONOMICAMENTE	-
CENÁRIO 2	CONTRATAÇÃO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES - LICENCIAMENTO PERPÉTUO E INFRAESTRUTURA ON-PREMISES	INVIÁVEL TECNICAMENTE E ECONOMICAMENTE	-
CENÁRIO 3	CONTRATAÇÃO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES - SUBSCRIÇÃO COM PLATAFORMA EM NUVEM (SAAS)	ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: • ÓRGÃO 1 - MPPA - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ ◦ Edital nº 90001/2025 - Ata de Registro de Preços nº 003/2025 • ÓRGÃO 2 - TCE-RJ - TRIBUNAL DE CONTAS DO ESTADO DO RIO DE JANEIRO ◦ PE 90123/2024 - Contrato nº 08353/2024 • ÓRGÃO 3 - SEF SC - SECRETARIA DE ESTADO DA FAZENDA ◦ PE nº 0030-2025/2025 - Contrato nº 095/2025 e Contrato nº 096/2025 • ÓRGÃO 4 - SPGF/GERENCIAL/SEF - SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS ◦ Edital nº 124/2024 e Contrato nº 009456402/2025 PROPOSTAS COMERCIAIS FORNECEDORES: • Proposta Comercial 01 - Blue Eye Soluções • Proposta Comercial 02 - Service IT Security • Proposta Comercial	ÓRGÃO 1 (23348361) (23348390) ÓRGÃO 2 (23348445) (23348617) ÓRGÃO 3 (23613273) (23613281) (23613298) ÓRGÃO 4 (23633329) (23633350) Fornecedores 24950041 24950050 24950052 24950057

6.2. Análise comparativa de soluções

6.2.1. Para atender à necessidade de negócio e tecnológica do Tribunal, foram analisados três cenários distintos, comparados sob múltiplos critérios para fundamentar a escolha da solução mais vantajosa para a Administração Pública.

6.2.1.1. CENÁRIO 1: UTILIZAÇÃO DE SOLUÇÃO OPEN SOURCE, IMPLEMENTADA E OPERADA PELA EQUIPE DE SEGURANÇA DO TRIBUNAL

6.2.1.1.1. **Descrição:** Este cenário envolve a adoção de um ecossistema de ferramentas de código aberto (como Greenbone/OpenVAS, OWASP ZAP, Trivy, Falco, Wazuh, etc.) para construir uma solução de gerenciamento de vulnerabilidades. A implementação, integração, manutenção e operação seriam de responsabilidade exclusiva da equipe técnica do TRF1. O maior desafio seria atender ao requisito de uma "única interface web integrada", o que exigiria um projeto de desenvolvimento de software customizado para criar um portal centralizado.

6.2.1.1.2. Análise:

6.2.1.1.2.1. **Custo de Aquisição (CAPEX):** Não haveria custo com software, mas exige investimento significativo em hardware (servidores, storage, cluster de processamento de dados) para hospedar as diversas ferramentas e seus bancos de dados.

6.2.1.1.2.2. **Custo Operacional (OPEX):** Extremamente elevado. Embora não haja custo de licença, o OPEX se manifesta em horas de trabalho intensivas e contínuas para: instalar, configurar e integrar múltiplas ferramentas que não conversam nativamente; desenvolver e manter scripts de automação e relatórios; atualizar constantemente as ferramentas e suas bases de assinaturas; e gerenciar toda a infraestrutura subjacente.

Módulo Requerido (ANEXO I)	Ferramentas Open Source Sugeridas	Justificativa
Gestão de Vulnerabilidades de Rede (Item 1.3)	Greenbone Community Edition (com OpenVAS): Para varreduras ativas, autenticadas e não autenticadas. Nmap: Para descoberta de ativos e portas. Zeek (anteriormente Bro): Para monitoramento passivo de rede (sensores). OSQuery: Como agente nos endpoints para inventário e conformidade.	Este conjunto cobre a descoberta de ativos, varredura de vulnerabilidades, conformidade com CIS (via scripts customizados) e monitoramento passivo. A base de dados do Greenbone é robusta, mas a priorização avançada de risco exigiria desenvolvimento customizado para correlacionar dados de ameaças externas.
Análise Dinâmica de Aplicações Web (DAST) (Item 2)	OWASP ZAP (Zed Attack Proxy): Ferramenta líder para DAST. Selenium Grid: Para gerenciar a execução de scripts de autenticação complexa.	O ZAP é extremamente poderoso e atende à maioria dos requisitos, incluindo testes de API, integração com Selenium e conformidade com OWASP Top 10. A automação e o agendamento em larga escala (250 aplicações) exigiriam uma orquestração robusta, provavelmente via scripts e

		contêineres.
	Trivy: Para varredura de vulnerabilidades em imagens de contêineres.	<u>Este conjunto de ferramentas da CNCF</u>
Segurança de Contêineres (Item 3)	Falco: Para detecção de ameaças em tempo de execução (runtime). Kube-bench: Para auditoria de conformidade dos clusters Kubernetes com os benchmarks CIS.	(Cloud Native Computing Foundation) cobre o ciclo de vida do contêiner. A integração para bloquear o uso de imagens vulneráveis (item 3.6) precisaria ser implementada em um pipeline de CI/CD (ex: Jenkins, GitLab CI) usando a saída do Trivy.
Monitoramento do Active Directory (Item 4)	Wazuh: Para coleta e análise de logs de segurança dos Domain Controllers. Sysmon: Para monitoramento detalhado de eventos nos endpoints e DCs. PingCastle: Para auditorias periódicas de configuração. PowerShell Scripts Customizados: Para verificações específicas e contínuas (ex: idade da senha do KRBTGT, política de LAPS).	Não existe uma única ferramenta <i>open source</i> que cubra todos os mais de 20 requisitos de AD. Seria necessária uma combinação: Wazuh para monitorar eventos em tempo real (como alterações em grupos) e scripts customizados agendados para auditar configurações estáticas.
Plataforma Central e Integração (Item 1.2.5)	Elastic Stack (Elasticsearch, Logstash, Kibana) ou Grafana: Para agregação de dados, dashboards e relatórios. Python (com Flask/Django) + PostgreSQL: Para desenvolver uma aplicação web customizada que sirva como a "única interface", com API para automação e controle de acesso (RBAC).	Este é o componente mais crítico. Seria necessário construir do zero um portal que: 1) Ingerisse e normalize os dados de todas as ferramentas acima. 2) Apresentasse os dados em uma interface unificada. 3) Implementasse o controle de acesso por grupos. 4) Fornecesse uma API RESTful para integração com SIEM.

6.2.1.1.2.3. Capacitação da Equipe: Muito alta e complexa. Exige que a equipe interna possua conhecimento profundo e especializado em diversas ferramentas distintas, além de habilidades em desenvolvimento de software, engenharia de dados, banco de dados e administração de sistemas. A curva de aprendizado é íngreme e contínua.

6.2.1.1.2.4. Suporte Técnico (SLA): Inexistente. O suporte depende de fóruns comunitários, sem qualquer garantia de tempo de resposta ou de solução para problemas críticos, o que representa um risco inaceitável.

6.2.1.1.2.5. Agilidade e Escalabilidade: Baixa. A expansão da capacidade exige aquisição de mais hardware e um novo projeto de configuração e integração. A adição de novas funcionalidades (como análise de contêineres) significa pesquisar, aprender e integrar uma nova ferramenta do zero.

6.2.1.1.2.6. Foco da Equipe e Pessoal: O foco da equipe de segurança seria criticamente desviado de sua missão principal de análise e gestão estratégica de riscos cibernéticos para a manutenção da ferramenta. Estima-se que a operação de uma solução *open source* na escala requerida demandaria uma equipe multidisciplinar dedicada de aproximadamente 11 profissionais. O custo anual estimado apenas com pessoal, considerando o salário inicial de um analista judiciário (R\$ 15.000,00/mês), seria de R\$ 1.980.000,00, valor que ultrapassa significativamente o de soluções comerciais.

Função da Equipe	Quantidade Estimada	Atividades Principais
Infraestrutura e DevOps	2 Pessoas	Implantação: Provisionar e configurar a infraestrutura de servidores, bancos de dados e storage para todas as ferramentas (cluster Elastic, servidores OpenVAS, etc.). Manutenção: Garantir a disponibilidade, performance, backup e atualização de toda a infraestrutura subjacente. Gerenciar a orquestração dos contêineres para as ferramentas de DAST e segurança de contêineres.
Engenheiros de Ferramentas de Segurança	3 Pessoas	Implantação: Instalar, configurar e "afinar" cada uma das ferramentas de segurança (OpenVAS, ZAP, Falco, Wazuh, etc.). Manutenção: Manter as ferramentas atualizadas, solucionar problemas de funcionamento, otimizar as políticas de varredura e detecção, e garantir a qualidade dos dados gerados. Cada engenheiro seria especializado em um domínio (Rede, Aplicações, Contêineres/AD).
Desenvolvedor de Integração / Engenheiro de Dados	2 Pessoas	Implantação: Desenvolver a plataforma central. Criar parsers para normalizar os dados de todas as ferramentas. Construir a API central. Desenvolver os dashboards e relatórios em Kibana/Grafana. Manutenção: Manter e evoluir a plataforma customizada, corrigir bugs, adicionar novas funcionalidades e garantir a performance da ingestão e consulta de dados.
Analistas de Gestão de Vulnerabilidades	3 Pessoas	Gestão do Processo: Analisar os resultados consolidados na plataforma. Priorizar vulnerabilidades com base no risco (processo que precisaria ser definido internamente). Abrir chamados e interagir com as equipes de infraestrutura, desktops e desenvolvimento para a correção. Acompanhar SLAs de remediação e gerar relatórios gerenciais.
Líder de Equipe / Gerente de Projeto	1 Pessoa	Gestão: Coordenar todas as frentes de trabalho (infra, desenvolvimento, segurança). Gerenciar o backlog de desenvolvimento da plataforma customizada. Fazer a interface com as áreas de negócio e a gestão de TI. Garantir que o programa de gestão de vulnerabilidades atinja seus objetivos.
Total Estimado	11 Pessoas	Salário inicial de um analista judiciário é de aproximadamente R\$ 15.000,00 mensal. Logo, o valor anual gasto com a equipe seria de R\$ 1.980.000,00.

6.2.1.1.2.7. Aderência ao PLS: Baixa. A necessidade de manter uma infraestrutura de servidores dedicada no data center do Tribunal vai contra os objetivos de sustentabilidade, aumentando o consumo de energia e a geração de lixo eletrônico.

6.2.1.1.3. Conclusão: Cenário considerado **inviável**. Altíssimo custo operacional oculto (principalmente com pessoal – estimado em R\$ 1.980.000,00 anuais para 11 profissionais dedicados), falta de suporte garantido, complexidade técnica e baixa agilidade. Não atende ao requisito de plataforma unificada.

6.2.1.2. CENÁRIO 2: CONTRATAÇÃO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES - LICENCIAMENTO PERPÉTUO E INFRAESTRUTURA ON-PREMISES

6.2.1.2.1. Descrição: Este cenário consiste na aquisição de licenças de software perpétuas, com a instalação de toda a infraestrutura necessária (servidores, bancos de dados, appliances) no data center do TRF1.

6.2.1.2.2. Análise:

6.2.1.2.2.1. Custo de Aquisição (CAPEX): Muito elevado. Implica em um grande investimento inicial para a compra das licenças de software e de todo o hardware necessário para suportar a operação e o armazenamento de dados para o período do contrato.

6.2.1.2.2.2. Custo Operacional (OPEX): Médio a Alto. Inclui o custo anual obrigatório de manutenção e suporte do software

(geralmente um percentual do valor da licença), além dos custos contínuos de energia, refrigeração, manutenção de hardware e horas da equipe de infraestrutura para gerenciar os servidores, sistemas operacionais e bancos de dados.

6.2.1.2.2.3. Capacitação da Equipe: Média. A equipe de segurança precisa ser treinada na ferramenta, e a equipe de infraestrutura precisa manter todo o ambiente subjacente, exigindo conhecimento em múltiplas frentes.

6.2.1.2.2.4. Suporte Técnico (SLA): Parcial. O SLA do fabricante cobre apenas o software. Qualquer problema relacionado à infraestrutura (hardware, sistema operacional, rede, banco de dados) é de responsabilidade exclusiva do Tribunal.

6.2.1.2.2.5. Agilidade e Escalabilidade: Baixa. A expansão da capacidade é um processo lento e burocrático, que exige novos ciclos de aquisição de hardware e, possivelmente, de licenças.

6.2.1.2.2.6. Foco da Equipe e Pessoal: Dividido. A equipe de segurança foca na ferramenta, mas depende da equipe de infraestrutura para garantir a disponibilidade e performance da base. Estima-se a necessidade de 1 analista de segurança para a gestão da ferramenta e, no mínimo, 0,5 ETP (Equivalente a Tempo Pleno) de um analista de infraestrutura para a sustentação do ambiente.

6.2.1.2.2.7. Aderência ao PLS: Baixa. Este é o modelo com maior impacto ambiental, maximizando o consumo de recursos (energia, espaço físico, refrigeração) no data center do Tribunal.

6.2.1.2.3. Conclusão: Cenário considerado **inviável**. Alto custo de aquisição inicial (CAPEX), custo operacional médio a alto (OPEX), suporte parcial (apenas software), baixa agilidade e escalabilidade, e alto impacto ambiental. Modelo em desuso no mercado.

6.2.1.3. CENÁRIO 3: CONTRATAÇÃO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES - SUBSCRIÇÃO COM PLATAFORMA EM NUVEM (SAAS)

6.2.1.3.1. Descrição: Este é o cenário proposto para contratação. Consiste na aquisição de uma solução como serviço (SaaS), na qual o licenciamento se dá por subscrição (anual ou plurianual) e toda a infraestrutura de processamento e armazenamento de dados é gerenciada pelo fornecedor em um ambiente de nuvem.

6.2.1.3.2. Análise: Este modelo apresenta a melhor relação custo-benefício para o Tribunal. O investimento é tratado como despesa operacional (OPEX), eliminando a necessidade de um grande desembolso inicial. O TRF1 fica isento de todos os custos e complexidades de gerenciamento da infraestrutura subjacente, que passa a ser responsabilidade do fornecedor, incluindo disponibilidade, escalabilidade e atualizações da plataforma. Isso representa uma significativa transferência de riscos operacionais e tecnológicos para o fornecedor. As atualizações de segurança e novas funcionalidades são aplicadas de forma transparente e contínua pelo fabricante, garantindo que o Tribunal sempre utilize a versão mais recente e segura da ferramenta. Este modelo também se alinha perfeitamente com as diretrizes do Plano de Logística Sustentável (PLS-TRF1), pois reduz o consumo de energia e a pegada de carbono do data center do Tribunal. A segurança dos dados é endereçada pela exigência de que a nuvem do fornecedor esteja no Brasil ou em país com decisão de adequação da ANPD.

6.2.1.3.2.1. Custo de Aquisição (CAPEX): Nulo. O modelo não exige investimento inicial em hardware ou licenças perpétuas.

6.2.1.3.2.2. Custo Operacional (OPEX): Previsível e otimizado. O

custo é diluído em pagamentos recorrentes (subscrição) que cobrem licenciamento, infraestrutura, manutenção, atualizações e suporte técnico em um único valor.

6.2.1.3.2.3. **Capacitação da Equipe:** Baixa. A equipe precisa ser capacitada apenas na operação da ferramenta. Toda a complexidade de gestão da infraestrutura é abstraída e gerenciada pelo fornecedor. O treinamento já está incluso no objeto da contratação.

6.2.1.3.2.4. **Suporte Técnico (SLA):** Completo e de ponta a ponta. O fornecedor é o único responsável pela disponibilidade e performance de toda a solução (software e infraestrutura), garantindo um SLA claro e abrangente.

6.2.1.3.2.5. **Agilidade e Escalabilidade:** Muito Alta. A plataforma em nuvem é naturalmente elástica. Aumentar a capacidade de análise ou adicionar novos módulos é um simples ajuste contratual, sem a necessidade de projetos de infraestrutura. As atualizações e novas funcionalidades são disponibilizadas de forma contínua e transparente pelo fabricante.

6.2.1.3.2.6. **Foco da Equipe e Pessoal:** Totalmente na missão. A equipe de segurança pode se concentrar 100% na sua atividade-fim: analisar dados, identificar riscos, priorizar vulnerabilidades e coordenar as ações de correção. A mesma equipe responsável pela gestão de vulnerabilidades pode operar a ferramenta, sem necessidade de pessoal adicional para sustentação.

6.2.1.3.2.7. **Aderência ao PLS:** Alta. Este é o modelo mais sustentável, pois transfere a demanda computacional para data centers em nuvem, que são mais eficientes energeticamente, reduzindo significativamente o consumo de recursos no data center do Tribunal.

6.2.1.3.2.8. **Pesquisa de mercado:** Foi realizada uma pesquisa de mercado que identificou três plataformas líderes no Quadrante Mágico do Gartner para Gerenciamento de Exposição a Ameaças, cujos representantes e parceiros no Brasil apresentaram propostas comerciais:

6.2.1.3.2.8.1. **Tenable One**, do fabricante Tenable, ofertada pela empresa Blue Eye.

6.2.1.3.2.8.2. **Qualys Enterprise TruRisk Platform**, do fabricante Qualys, ofertada pelas empresas Service IT, ISH e Solo Network.

6.2.1.3.4. As três soluções da pesquisa de mercado são robustas e atendem aos requisitos técnicos. No entanto, uma análise detalhada das especificações técnicas das soluções revela pontos críticos de aderência:

Requisito Chave	Tenable	Qualys
Plataforma Unificada	Aderência Total: Plataforma nativamente integrada (Tenable One) que consolida todos os módulos.	Aderência Total: Plataforma nativamente integrada (Enterprise TruRisk) com módulos como apps.
Suporte a Kubernetes On-Premises	Aderência Total: O módulo Tenable Cloud Security oferece suporte explícito a ambientes híbridos, incluindo on-premises.	Aderência Total: O módulo Qualys Container Security foi projetado para cobrir o ciclo de vida completo em ambientes on-premises e na nuvem.
Gestão de Postura de Identidade (ISPM)	Aderência Total: Possui um produto dedicado (Tenable Identity Exposure) que realiza análises proativas e sem agente, cobrindo nativamente requisitos avançados como a verificação da idade da senha do	Aderência Total: Atende aos requisitos através do módulo Policy Compliance (PC), utilizando varreduras autenticadas e a criação de controles personalizados (UDCs) para cobrir todas as verificações.

	KRBTGT.	
	Aderência Total: O modelo VPR	Aderência Total: O modelo IruRisk é
Modelo de Priorização de Risco	(Vulnerability Priority Rating) utiliza explicitamente a maioria dos fatores exigidos no edital, incluindo a idade da vulnerabilidade e o número de produtos afetados.	robusto e considera criticidade do ativo, inteligência de ameaças e exploits, atendendo à intenção de todos os requisitos.

6.2.1.3.5. **Conclusão:** Cenário mais adequado e **recomendado**. Atende a todos os requisitos técnicos e de negócio, oferece a melhor relação custo-benefício, maior flexibilidade e agilidade, alinha-se às práticas de sustentabilidade e permite que a equipe de segurança do TRF1 foque na análise e gestão dos riscos, em vez de na manutenção de infraestrutura.

6.2.2. Análise Comparativa dos Cenários:

Critério	Cenário 1 (Open Source)	Cenário 2 (On-Premises)	Cenário 3 (SaaS) - Recomendado
Custo de Aquisição (CAPEX)	Baixo (apenas custo com hardware)	Muito elevado (grande investimento inicial = hardware + licenças)	Nulo
Custo Operacional (OPEX)	Extremamente elevado (custo de pessoal estimado em R\$ 1.980.000,00 anuais, além de horas de trabalho intensivas e contínuas)	Médio a Alto (suporte, energia)	Médio (subscrição)
Capacitação da Equipe	Muito alta e complexa	Média	Baixa
Suporte Técnico (SLA)	Inexistente (depende de fóruns comunitários)	Parcial (fabricante cobre o software, mas não infraestrutura)	Completo e de ponta a ponta (Garantido por contrato)
Agilidade e Escalabilidade	Baixa	Baixa	Alta
Foco da Equipe Técnica	Manutenção de ferramenta	Manutenção de infraestrutura	Totalmente na missão (analisar dados, identificar riscos, priorizar vulnerabilidades e coordenar as ações de correção)
Aderência ao PLS (plano de logística sustentável)	Baixa	Baixa	Alta

6.2.2.1. Consiste em uma análise crítica entre as diferentes soluções, considerando o aspecto econômico (TCO) entre a solução e os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação. Como auxílio, o quadro seguinte poderá ser utilizado para comparação de alguns requisitos entre a solução identificada.

REQUISITOS	ID DO CENÁRIO	SIM	NÃO	NÃO SE APLICA
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
	3	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	1		X	
	2		X	

A Solução está disponível no Portal do Software Público Brasileiro?	3	X		
	1		X	
	2		X	
A Solução é um software livre ou software público?	3		X	
	1	X		
	2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	3		X	
	1			X
	2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	3			X
	1			X
	2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário - MoReq - Jus?	3			X
	1			X
	2			X

6.2.3. A análise do ETP demonstra que o modelo SaaS é a única alternativa técnica e economicamente viável para atender às necessidades da Justiça Federal da 1ª Região, permitindo que a equipe de segurança concentre seus esforços na gestão estratégica do risco cibernético.

6.3. Pesquisa de preços de mercado

CENÁRIO 3 - SOLUÇÕES SIMILARES ADOTADAS EM OUTROS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA GESTÃO DE VULNERABILIDADES - SUBSCRIÇÃO COM PLATAFORMA EM NUVEM (SAAS)

ÓRGÃO 1

Órgão: **MPPA** - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ - Número da UASG: 925980
Edital nº 90001/2025 (23348361) - Id contratação PNCP: 05054960000158-1-000009/2025 -
<https://pncp.gov.br/app/editais/05054960000158/2025/9>
Ata nº 003/2025 (23348390) - Vigência: de **24/03/2025** a 24/03/2026 -
<https://pncp.gov.br/app/atas/05054960000158/2025/9/1> - Nome do Fornecedor: IT PROTECT
SERVICOS DE CONSULTORIA EM INFORMATICA LTDA

OBJETO: Registro de Preços para aquisição de solução de gerenciamento de vulnerabilidades de ativos de tecnologia da informação.

***Destaca-se que, embora o preço tenha sido atendido, não foi utilizado por ter ultrapassado o prazo máximo de validade de 1 (um) ano, conforme disposto na Resolução nº 468/2022 do CNJ.**

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	INFORMAÇÃO RELEVANTE (Comparação entre as especificações técnicas do TRF1 em relação a prevista no Edital do órgão similar)	ATENDE? (SIM/NÃO)
	Solução de Gerenciamento de vulnerabilidades para ativos em tecnologia da informação, com análise					A quantidade a ser adquirida do (s) serviços(s) será de 6000 (seis mil) licenças de software de gerenciamento de vulnerabilidades em ativos de tecnologia e	

1	contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 36 meses. TENABLE ONE - Cód. Comprasnet/CATSER: 27502	Unidade	6.000	R\$ 835,22	R\$ 5.001.320,00	aplicações, junto com 36 meses de suporte técnico especializado em virtude da quantidade de ativos em tecnologia da informação, quantidade de usuários de nosso domínio do MPPA e quantidade de aplicações de nosso ambiente. Para o item 01, o pagamento será efetuado em parcela única.	*SIM ATENDE AO ITEM 1
2	Suporte técnico especializado - Cód. Comprasnet/CATSER: 26972	Mês	36	R\$ 18.000,00	R\$ 648.000,00	O item 02 deste edital não atende às especificações do TRF1 para a solução principal, uma vez que se refere apenas à contratação de suporte técnico especializado, enquanto a demanda do TRF1 é a contratação da solução de software como serviço (SaaS) que já inclua o suporte no licenciamento.	NÃO
ÓRGÃO 2 Órgão: TCE-RJ - TRIBUNAL DE CONTAS DO ESTADO DO RIO DE JANEIRO - Número da UASG:925464 Edital nº 90028/2024 (23348445) - Id contratação PNCP: 30051023000196-1-000154/2024 - https://pncp.gov.br/app/editais/30051023000196/2024/154 Contrato nº 66/2024 (23348617) - Vigência: de 01/10/2024 a 18/12/2027 - Nome do Fornecedor: W3CYBERSEC LTDA OBJETO: Aquisição de licença de uso, do tipo subscrição, de uma solução de Software de Gestão de Vulnerabilidades, incluindo serviço de implantação (instalação e configuração), treinamento e garantia / suporte técnico online (remoto) por 36 (trinta e seis meses), no ambiente tecnológico do Tribunal de Contas do Estado do Rio de Janeiro - TCE/RJ, conforme condições, quantidades e especificações contidas no TERMO DE REFERÊNCIA - ANEXO I do edital. *Destaca-se que, embora o preço tenha sido atendido, não foi utilizado por ter ultrapassado o prazo máximo de validade de 1 (um) ano, conforme disposto na Resolução nº 468/2022 do CNJ.							
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	INFORMAÇÃO RELEVANTE (Comparação entre as especificações técnicas do TRF1 em relação a prevista no Edital do órgão similar)	ATENDE? (SIM/NÃO)
						- Assets: É um ativo, um bem, usado para designar itens que alguma entidade possui. - Para o objeto desta contratação,	

1	Solução de Gestão de Vulnerabilidade e Auditoria de Configuração de ativos, com licença do tipo subscrição e suporte técnico do fabricante pelo período de 36 (trinta e seis) meses. Marca: Tenable Modelo: Tenable One/Tenable Vulnerability Managemen	ASSET	812	R\$ 738,90	R\$ 599.986,80	notadamente em relação aos itens 01 a 04, o pagamento será efetuado pelo TCE-RJ em parcela única e de forma integral. Apesar de ser uma solução de gestão de vulnerabilidades, a quantidade de assets (812) e a natureza do licenciamento, ou algum requisito técnico específico do TRF1 (ex: necessidade de módulo de containers, ou monitoramento de AD mais abrangente), não se alinham perfeitamente com a necessidade do Tribunal, resultando em um 'Não' ou 'Não plenamente'.	*SIM ATENDE AO ITEM 1
2	Solução de análise dinâmica de vulnerabilidades para aplicações Web, com licença do tipo subscrição e suporte técnico do fabricante pelo período de 36 (trinta e seis) meses. Marca: Tenable Modelo: Tenable One/Tenable Web App Scanning	FQDN	2	R\$ 760,90	R\$ 1.521,80	- FQDNs: É um nome de domínio completamente qualificado, algumas vezes denominado nome de domínio absoluto, que especifica sua localização exata na árvore hierárquica do Domain Name System (DNS). - Para o objeto desta contratação, notadamente em relação aos itens 01 a 04, o pagamento será efetuado pelo TCE-RJ em parcela única e de forma integral.	NÃO
3	Solução de análise em ambiente Microsoft Active Directory, com licença do tipo subscrição e suporte técnico do fabricante pelo período de 36 (trinta e seis) meses. Marca: Tenable Modelo: Tenable One / Tenable Identity Exposure	USUÁRIO ATIVO	1500	R\$ 748,90	R\$ 1.123.350,00	Para o objeto desta contratação, notadamente em relação aos itens 01 a 04, o pagamento será efetuado pelo TCE-RJ em parcela única e de forma integral.	NÃO
4	Implantação (instalação e configuração) da Solução (itens 1; 2; 3).	SERVIÇO	0	R\$ 176.049,00	R\$ 176.049,00	Para o objeto desta contratação, notadamente em relação aos itens 01 a 04, o pagamento será efetuado pelo	NÃO

						TCE-RJ em parcela única e de forma integral.	
5	Treinamento Oficial do Fabricante para servidores do TCE-RJ.	ALUNO 8		R\$ 10.993,80	R\$ 10.944,00	- O treinamento, item 05 (cinco) do objeto da contratação, será realizado na modalidade online, deverá ter carga horária mínima de 24 (vinte e quatro) horas, sendo 04 (quatro) horas por aula, para 8 (oito) servidores do TCE-RJ - O treinamento deverá ter início em no máximo 15 (quinze) dias corridos após o fornecimento da licença do software, com prazo de início e término de execução tratados através de ordens de serviço, enviadas pelo Contratante à empresa Contratada, desde que anteriormente ao término da etapa da implantação (instalação e configuração), tendo em vista a necessidade de a equipe técnica ter pleno conhecimento das funcionalidades da solução e do atendimento das especificações técnicas que serão implantadas. - O pagamento do item 05 (cinco) – treinamento oficial, será realizado sob demanda, a cada ordem de serviço executada, mediante crédito em conta corrente da contratada, até o 30º (trigésimo) dia consecutivo.	NÃO Unidade de medida diferente
ÓRGÃO 3 Órgão: SEF SC - SECRETARIA DE ESTADO DA FAZENDA Edital nº 0030-2025 (23613273) - Id contratação PNCP: 82951310000156-1-000053/2025 - https://pncp.gov.br/app/editais/82951310000156/2025/53 Contrato nº 095/2025 (23613281) - Data Início Vigência:25/09/2025 - Data Término Vigência:25/09/2028 - Nome do Fornecedor: SERVICE IT SECURITY LTDA Contrato nº 096/2025 (23613298) - Data Início Vigência:25/09/2025 - Data Término Vigência:25/09/2028 - Nome do Fornecedor: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA							

OBJETO: Renovação de licenças para gestão de vulnerabilidades de TI, cofre de senhas, gerenciamento de acesso privilegiado e suporte para 36 meses.

***Destaca-se que, embora o preço tenha sido atendido, não foi utilizado por ter ultrapassado o prazo máximo de validade de 1 (um) ano, conforme disposto na Resolução nº 468/2022 do CNI**

**ATENDE?
(SIM/NÃO)**

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	INFORMAÇÃO RELEVANTE (Comparação entre as especificações técnicas do TRF1 em relação a prevista no Edital do órgão similar)	ATENDE? (SIM/NÃO)
1 - Lote 1	Solução de varredura de vulnerabilidades em ativos TIC Qualys para 36 meses	Licença	1750	R\$ 158,78	R\$ 277.865,00	- A solução deve ser do mesmo fabricante dos demais itens deste grupo, para fins de compatibilidade e adequação da solução como um todo. - A base de conhecimento de fragilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais.	*SIM ATENDE AOS ITENS 1 e 6
2 - Lote 1	Solução de Categorização e Inventário de Ativos Qualys para 36 meses	Licença	1750	R\$ 110,23	R\$ 192.902,50	- A solução deve ser do mesmo fabricante dos demais itens deste grupo, para fins de compatibilidade e adequação da solução como um todo. - A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.	NÃO
3 - Lote 1	Solução de remediação de vulnerabilidades para ativos TIC Qualys para 36 meses	Licença	1750	R\$ 347,90	R\$ 608.825,00	- A solução deve permitir a criação de dashboards para acompanhamento de aplicação de patches. - A solução deve permitir mostrar em um mesmo dashboard a quantidade de ativos que possuem um software	NÃO

						instalado e quantidade de patches relevantes a esse mesmo software.	
4 - Lote 1	Solução de varredura de vulnerabilidades em aplicações Web Qualys para 36 meses	Licença	10	R\$ 4.653,34	R\$ 46.533,50	A solução proposta deve habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem;	*SIM ATENDE AOS ITENS 2 e 7
1 - Lote 2	Solução de cofre de senhas e acesso seguro BeyondTrust para 36 meses	Licença	1750	R\$ 962,00	R\$ 1.683.500,00	- O licenciamento deverá ser por dispositivo e independente da quantidade de usuários privilegiados que necessitem acessar o ambiente. - Os softwares e o virtual appliance deverão ser fornecidos junto com a solução. - A solução deverá incluir um conjunto de softwares licenciados necessários ao atendimento dos requisitos mínimos especificados a seguir, incluindo garantia, manutenção e atualização dos produtos durante o prazo de vigência do contrato sem limite de usuários privilegiados.	NÃO
2 - Lote 2	Solução de gerenciamento de acesso privilegiado BeyondTrust para 36 meses	Licença	1500	R\$ 318,00	R\$ 477.000,00	- O módulo de gerenciamento de elevação e delegação de privilégios deverá ser licenciado como subscrição, em virtual appliance na modalidade on-premises. - Os softwares e o virtual appliance deverão ser fornecido junto com a solução. - O Banco de Dados deverá ser fornecido como parte integrante da solução.	NÃO

3 - Lote 2	Solução de Suporte Remoto BeyondTrust para 36 meses	Licença 20	R\$ 24.000,00	R\$ 480.000,00	- A solução deve ser disponível no formato on-premises. - A solução deve ser disponibilizada com opção de uso na língua portuguesa-Brasil.	NÃO
4 - Lote 2	Suporte Técnico Mensal	Mensal 36	R\$ 12.850,00	R\$ 462.600,00	- Os profissionais devem ser certificados tecnicamente pela fabricante nas soluções oferecidas, devendo a CONTRATADA possuir mais de um profissional habilitado; - Serviço de suporte técnico será de responsabilidade solidária da Fabricante com a CONTRATADA, podendo a SEF abrir chamado de suporte tanto em um quanto em outro. - O serviço de suporte técnico com operação assistida para solução iniciará até o 1º dia útil após a finalização da instalação e configuração da expansão do licenciamento da solução e finalizando até o último dia da primeira vigência do contrato de 36 meses, se repetindo anualmente a cada renovação contratual de período de 12 (doze) meses, até o limite da legislação aplicável.	*SIM ATENDE AOS ITENS 10 e 11
ÓRGÃO 4 Órgão: SPGF/GERENCIAL/SEF - SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS - Número da UASG: 1191001 Edital nº 124/2024 (23633329) - Id contratação PNCP: 16907746000113-1-000157/2024 - https://pncp.gov.br/app/editais/16907746000113/2024/157 Contrato nº 009456402/2025 (23633350) - Vigência: de 11/03/2025 a 10/03/2026 - Nome do Fornecedor: IT-ONE TECNOLOGIA DA INFORMACAO S.A. OBJETO: Contratação 2000 licenças Gestão vulnerabilidade- Tenable. *No contrato nº 009456402/2025, firmado pelo Órgão SPGF/GERENCIAL/SEF – Secretaria de Estado de Fazenda de Minas Gerais, o objeto é a contratação de 2.000 licenças da solução de Gestão de Vulnerabilidade (Tenable), pelo valor total de R\$ 531.551,00, com vigência						

de 11/03/2025 a 10/03/2026.

Entretanto, $531.551,00/2.000\} = R\$ 265,77 =$ Arredondando para duas casas decimais (padrão de apresentação em moeda), o valor unitário anual por licença corresponde a: R\$ 265,77

Portanto, chegou-se ao **valor unitário anual de R\$ 265,77 por licença**, conforme demonstrado na tabela do item 1.

***Destaca-se que, embora o preço tenha sido atendido, não foi utilizado por ter ultrapassado o prazo máximo de validade de 1 (um) ano, conforme disposto na Resolução nº 468/2022 do CNI.**

**ATENDE?
(SIM/NÃO)**

ITEM	DESCRIÇÃO	UNID	QU.	VALOR UNITÁRIO ANUAL	VALOR TOTAL	INFORMAÇÃO RELEVANTE (Comparação entre as especificações técnicas do TRF1 em relação a prevista no Edital do órgão similar)	
1	Subscrição de licenças da solução de Gestão de Vulnerabilidade (2.000unidades)	Unidade	1	*R\$ 265,77 para 12 meses	R\$ 531.551,00	- Solução de Gestão de Vulnerabilidade e Auditoria de Configuração de ativos; análise dinâmica de vulnerabilidades para aplicações Web; e análise de infraestrutura sobre código em ambiente de Imagens em Contêiner, DevOps e GitOps - Fabricante Tenable. - A solução deve ser fornecida na modalidade Software as a Service (SaaS) e licenciamento na modalidade subscrição.	*SIM ATENDE AOS ITENS 1 e 6

CENÁRIO 3 - PESQUISA DE PREÇOS REALIZADA COM FORNECEDORES COMPARATIVOS ENTRE FORMAS DE CONTRATAÇÃO COM BASE NOS VALORES DO TCO (12 x 36 MESES e LICENÇAS COM E SEM SUPORTE INCLUÍDO)

Proposta Comercial 01 (24950041)

Nome do Fornecedor: Blue Eye Soluções em Tecnologia Ltda

Solução (Fabricante): Tenable

OBJETO: Contratação de Solução de Gerenciamento de Vulnerabilidades, na modalidade de Software como Serviço (SaaS), para análise de ativos de rede, análise dinâmica de aplicações web (DAST), segurança de contêineres e monitoramento de identidades do Microsoft Active Directory. A contratação abrange o licenciamento de uso da plataforma por 36 (trinta e seis) meses, serviços de configuração, suporte técnico especializado e treinamento para a equipe técnica do Tribunal.

Observação: Para a Proposta Comercial nº 01 da empresa Blue Eye, referente ao item 6, verificou-se que a empresa apresentou valor incorreto para o valor unitário. Constatou-se inconsistência no valor informado, uma vez que, ao dividir o valor total anual de R\$ 360.000,00 pelo quantitativo de 4.780 unidades, obtém-se o valor unitário de R\$ 43,90. Dessa forma, o valor unitário foi ajustado para R\$ 43,90, por corresponder ao montante necessário para o cálculo do valor total nos períodos de 12 e 36 meses, tratando-se apenas de erro material na proposta apresentada pelo fornecedor.

GRU	ITE	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMATIVA	VALOR	VALOR TOTAL	VALOR TOTAL
-----	-----	-----------	---------	-----------------------	-------	-------------	-------------

				POR ÓRGÃO		TOTAL	UNITÁRIO	12 MESES	36 MESES
1	1	Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	Licença por ativo de rede / ano	TRF1	4000	7000	R\$ 400,00	R\$ 2.800.000,00	R\$ 8.400.000,00
				TRF2	3000				
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	Licença por aplicação web / ano	TRF1	100	160	R\$ 5.000,00	R\$ 800.000,00	R\$ 2.400.000,00
				TRF2	60				
	3	Licenciamento de Segurança de Contêineres	Licença por worker node (kubernetes) / ano	TRF1	100	140	R\$ 1.500,00	R\$ 210.000,00	R\$ 630.000,00
				TRF2	40				
	4	Licenciamento para Gestão de Postura de Identidade (ISPM)	Licença por usuário (grupo de 1000 usuários monitorados) / ano	TRF1	16	32	R\$ 150.000,00	R\$ 4.800.000,00	R\$ 14.400.000,00
				TRF2	16				
	5	Treinamento Técnico para Administração da Solução	Turma (grupo de 10 usuários por turma)	TRF1	5	8	R\$ 30.000,00	R\$ 240.000,00	R\$ 240.000,00
				TRF2	3				
	6	Serviço de Suporte Técnico	Unidade de Suporte por Ativo Equivalente (USAE) / mês	TRF1	4.780	8200	R\$ 43,90	R\$ 359.980,00	R\$ 1.079.940,00
				TRF2	3.420				
VALOR TOTAL								R\$ 9.209.980,00	R\$ 27.149.940,00

Proposta Comercial 02 (24950050)

Nome do Fornecedor: Service IT Security Ltda
Solução (Fabricante): Qualys Enterprise TruRisk

OBJETO: Contratação de Solução de Gerenciamento de Vulnerabilidades, na modalidade de Software como Serviço (SaaS), para análise de ativos de rede, análise dinâmica de aplicações web (DAST), segurança de contêineres e monitoramento de identidades do Microsoft Active Directory. A contratação abrange o licenciamento de uso da plataforma por 36 (trinta e seis) meses, serviços de configuração, suporte técnico especializado e treinamento para a equipe técnica do Tribunal.

GRU	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMATIVA		VALOR UNITÁRIO	VALOR TOTAL 12 MESES	VALOR TOTAL 36 MESES
				POR ÓRGÃO	TOTAL			
	1	Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	Licença por ativo de rede / ano	TRF1	4000	R\$ 61,32	R\$ 429.400,00	R\$ 1.287.720,00
				TRF2	3000			
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	Licença por aplicação web / ano	TRF1	100	R\$ 2.390,48	R\$ 382.476,80	R\$ 1.147.430,40
				TRF2	60			
	3	Licenciamento de Segurança de Contêineres	Licença por worker node (kubernetes) / ano	TRF1	100	R\$ 1.853,12	R\$ 259.436,80	R\$ 778.310,40
				TRF2	40			

1	4	Licenciamento para Gestão de Postura de Identidade (ISPM)	Licença por usuário (grupo de 1000 usuários monitorados) / ano	TRF1	16	32	R\$ 27.481,90	R\$ 879.420,80	R\$ 2.638.262,40
				TRF2	16				
	5	Treinamento Técnico para Administração da Solução	Turma (grupo de 10 usuários por turma)	TRF1	5	8	R\$ 4.498,38	R\$ 35.987,04	R\$ 35.987,04
				TRF2	3				
	6	Serviço de Suporte Técnico	Unidade de Suporte por Ativo Equivalente (USAE) / mês	TRF1	4.780	8200	R\$ 57,60	R\$ 472.320,00	R\$ 1.416.960,00
				TRF2	3.420				
	VALOR TOTAL							R\$ 2.459.041,44	R\$ 7.304.670,24

Proposta Comercial 03 (24950052)

Nome do Fornecedor: Solo Network Brasil SA

Solução (Fabricante): Qualys Enterprise TruRisk

OBJETO: Contratação de Solução de Gerenciamento de Vulnerabilidades, na modalidade de Software como Serviço (SaaS), para análise de ativos de rede, análise dinâmica de aplicações web (DAST), segurança de contêineres e monitoramento de identidades do Microsoft Active Directory. A contratação abrange o licenciamento de uso da plataforma por 36 (trinta e seis) meses, serviços de configuração, suporte técnico especializado e treinamento para a equipe técnica do Tribunal.

Observação: Para a Proposta Comercial nº 03 da empresa Solo Network, referente aos itens 1 e 3, verifica-se que a empresa realizou os cálculos com base no racional apresentado na própria proposta, conforme demonstrado a seguir:

7.000 VMs = 7.000 outputs
140 VMs com containers = 4.200 outputs
Total de QLUs = 11.200

Item 1: Foi realizado o seguinte cálculo:

Valor unitário de R\$ 180,85 × 7.000 = R\$ 1.265.950,00 (para 3 anos)

R\$ 1.265.950,00 ÷ 3 = R\$ 421.983,33 (valor anual)

R\$ 421.983,33 ÷ 7.000 = R\$ 60,28 (valor unitário ajustado)

Item 3: Foi realizado o seguinte cálculo:

Valor unitário de R\$ 180,85 × 4.200 outputs = R\$ 759.570,00 (para 3 anos)

R\$ 759.570,00 ÷ 3 = R\$ 253.190,00 (valor anual)

R\$ 253.190,00 ÷ 140 = R\$ 1.808,50 (valor unitário ajustado)

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMATIVA		VALOR UNITÁRIO	VALOR TOTAL 12 MESES	VALOR TOTAL 36 MESES
				POR ÓRGÃO	TOTAL			
	1	Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	Licença por ativo de rede / ano	TRF1	4000	R\$ 60,28	R\$ 421.960,00	R\$ 1.265.880,00
				TRF2	3000			
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	Licença por aplicação web / ano	TRF1	100	R\$ 2.355,44	R\$ 376.870,40	R\$ 1.130.611,20
				TRF2	60			
	3	Licenciamento de Segurança de Contêineres	Licença por worker node (kubernetes)	TRF1	100	R\$ 1.808,50	R\$ 253.190,00	R\$ 759.570,00
				TRF2	40			

1	4	Licenciamento para Gestão de Postura de Identidade (ISPM)	/ ano Licença por usuário (grupo de 1000 usuários monitorados) / ano	TRF1	16	32	R\$ 27.406,66	R\$ 877.013,12	R\$ 12.631.039,36
				TRF2	16				
	5	Treinamento Técnico para Administração da Solução	Turma (grupo de 10 usuários por turma)	TRF1	5	8	R\$ 11.200,00	R\$ 89.600,00	R\$ 89.600,00
				TRF2	3				
	6	Serviço de Suporte Técnico	Unidade de Suporte por Ativo Equivalente (USAE) / mês	TRF1	4.780	8200	R\$ 70,80	R\$ 580.560,00	R\$ 741.680,00
				TRF2	3.420				
VALOR TOTAL								R\$ 2.599.193,75	R\$ 7.528.780,56

Proposta Comercial 04 (24950057)

Nome do Fornecedor: ISH Tecnologia

Solução (Fabricante): Qualys Enterprise TruRisk

OBJETO: Contratação de Solução de Gerenciamento de Vulnerabilidades, na modalidade de Software como Serviço (SaaS), para análise de ativos de rede, análise dinâmica de aplicações web (DAST), segurança de contêineres e monitoramento de identidades do Microsoft Active Directory. A contratação abrange o licenciamento de uso da plataforma por 36 (trinta e seis) meses, serviços de configuração, suporte técnico especializado e treinamento para a equipe técnica do Tribunal.

Observação: Para a Proposta Comercial nº 04 da empresa ISH, referente ao item 6, considerando que a empresa apresentou três valores para o mesmo item, foi adotado o de menor preço. Entretanto, constatou-se inconsistência no valor unitário informado, uma vez que, ao dividir o valor total anual de R\$ 131.928,00 pelo quantitativo de 4.780 unidades, obtém-se o valor unitário de R\$ 27,60.

Dessa forma, esse valor foi considerado como o menor preço para o referido item na proposta do respectivo fornecedor.

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMATIVA		VALOR UNITÁRIO	VALOR TOTAL 12 MESES	VALOR TOTAL 36 MESES
				POR ÓRGÃO	TOTAL			
1	1	Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	Licença por ativo de rede/ano	TRF1	4000	R\$ 22,03	R\$ 154.210,40	R\$ 462.630,00
				TRF2	3000			
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	Licença por aplicação web/ano	TRF1	100	R\$ 1.762,25	R\$ 281.960,45	R\$ 845.880,00
				TRF2	60			
	3	Licenciamento de Segurança de Contêineres	Licença por worker node (kubernetes)/ ano	TRF1	100	R\$ 2.091,20	R\$ 292.768,00	R\$ 878.304,00
				TRF2	40			
		Licenciamento para Gestão	Licença por usuário	TRF1	16			
				TRF1				

4	de Postura de Identidade (ISPM)	(grupo de 1000 usuários monitorados)/ano	TRF2	16	32	R\$ 31.750,00	R\$ 1.016.080,00	R\$ 31.750,00
5	Treinamento Técnico para Administração da Solução	Turma (grupo de 10 usuários por turma)	TRF1	5	8	R\$ 7.149,14	R\$ 57.193,12	R\$ 57.193,12
			TRF2	3				
6	Serviço de Suporte Técnico	Unidade de Suporte por Ativo Equivalente (USAE)/mês	TRF1	4.780	8200	R\$ 27,60	R\$ 226.320,00	R\$ 226.320,00
			TRF2	3.420				
VALOR TOTAL							R\$ 2.028.451,70	R\$ 170.967,12

Conclusão consolidada da pesquisa de mercado e vantajosidade: A análise de alternativas (*open source*, licença perpétua/*on-premises* e subscrição SaaS) concluiu pela recomendação de solução em modelo SaaS por:

- a) Atualização contínua e tempestiva (bases de vulnerabilidades, *engines* e correções), com redução do risco de obsolescência tecnológica;
- b) Menor necessidade de infraestrutura interna (redução de custo/complexidade operacional e maior previsibilidade de sustentação);
- c) Escalabilidade e rapidez de implantação (*time-to-value*) para atendimento dos prazos de disponibilização e configuração;
- d) Cobertura integrada dos módulos requeridos (ativos, aplicações, contêineres, identidades), com correlação de achados e priorização por risco;
- e) Aderência a requisitos de segurança e conformidade (LGPD, criptografia, logs/auditoria, RBAC/MFA e controles de acesso).

A vantajosidade foi avaliada considerando custos diretos e indiretos (TCO) no horizonte de 36 meses, bem como riscos de implantação e sustentação, concluindo pela maior eficiência do modelo SaaS para o contexto institucional.

Síntese de critérios que justificam as especificações: As especificações técnicas foram estabelecidas para garantir:

- a) cobertura integrada dos quatro domínios (ativos, aplicações, contêineres, identidades),
- b) atualização contínua e suporte com SLA,
- c) evidências e relatórios auditáveis,
- d) integração com processos e ferramentas corporativas (ex.: SIEM / ITSM / API), e
- e) conformidade com requisitos de segurança e LGPD.

O modelo SaaS foi adotado por apresentar maior vantajosidade operacional (menor infraestrutura interna, maior velocidade de implantação e atualização contínua), conforme estudos técnicos do processo.

7. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

7.1. Cenário 1 (Open Source): Conforme análise detalhada na seção 6.2, este cenário foi considerado inviável por seu altíssimo custo operacional oculto (principalmente com pessoal), falta de suporte técnico garantido (SLA), complexidade de integração e manutenção, e por não atender ao requisito fundamental de uma plataforma unificada. Conclui-se que o cenário apresenta alto risco e não atende plenamente às necessidades do Tribunal.

7.2. Cenário 2 - O modelo *on-premises*, com licenciamento perpétuo, atende parcialmente à demanda. Exige alto investimento inicial e transfere à equipe interna a gestão da infraestrutura e das atualizações, além de não permitir escaneamento externo pela nuvem. A escalabilidade é limitada e o modelo está em desuso no

mercado. Por essas razões, o cenário não se mostra o mais adequado frente às necessidades do TRF1.

8. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

8.1. Cálculo dos custos totais de propriedade

8.1.1. Custo Total de Propriedade - TCO (*Total Cost of Ownership*) é o cálculo geral de todos os custos que envolvem a aquisição de um serviço ou produto. Tem como objetivo calcular os custos de vida e aquisição de um produto ou ferramenta e, por fim, determinar se um investimento vale a pena ou não.

8.1.2. Conforme inciso III do art. 11 da IN n. 94/2022, uma análise comparativa de custos deverá considerar apenas as soluções técnicas e funcionalmente viáveis, incluindo: a) comparação de custos totais de propriedade (*Total Cost Ownership - TCO*) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução.

8.1.3. Para uma solução na modalidade SaaS, o Custo Total de Propriedade (TCO) durante o período do contrato para o TRF1 é majoritariamente composto pelos valores pagos à contratada, que já incluem licenciamento, implantação, suporte e treinamento, com pagamento em parcelas anuais. Custos internos, como horas de trabalho da equipe técnica do TRF1 para operar a ferramenta, já fazem parte dos custos operacionais do Tribunal e não representam um acréscimo direto gerado pela contratação. Os órgãos participantes que aderirem à Ata poderão ter modelos de pagamento e suporte distintos, incluindo pagamento total upfront para as licenças e faturamento separado para o suporte técnico mensal. Portanto, a análise de custos do presente ETP se concentra na comparação dos valores totais das propostas para o TRF1.

8.2. Mapa comparativo dos cálculos totais de propriedade (TCO)

RESUMO DO CÁLCULO TOTAL DE PROPRIEDADE (TCO)					
CENÁRIO	DESCRIÇÃO	TCO (ANO - 01)	TCO (ANO - 02)	TCO (ANO - 03)	MEMÓRIA DE CÁLCULO
3 - CENÁRIO 3: GESTÃO DE	Item 1 - Licenciamento de Gestão de Vulnerabilidades - Scan de Ativo de Rede	R\$ 154.210,00	R\$ 154.210,00	R\$ 154.210,00	A metodologia utilizada para o cálculo do valor de referência foi o MENOR PREÇO dos preços pesquisados, conforme justificativas constantes no Mapa Comparativo de Preços (25062350) e Informação Conclusiva - Valor Estimado da Contratação (25068276).
	Item 2 - Licenciamento de DAST - Análise Dinâmica de Aplicações Web	R\$ 281.960,00	R\$ 281.960,00	R\$ 281.960,00	
	Item 3 - Licenciamento de Segurança de Contêineres	R\$ 210.000,00	R\$ 210.000,00	R\$ 210.000,00	VALOR UNITÁRIO = R\$22,03*7.000 (Quantitativo) = R\$ 154.210,00 * 3 anos = R\$ 462.630,00
	Item 4 - Licenciamento para Gestão de Postura de Identidade (ISPM)	R\$ 877.013,12	R\$ 877.013,12	R\$ 877.013,12	PARA O ITEM 2 - Licenciamento de DAST - Análise Dinâmica de Aplicações Web:
	Item 5 - Treinamento Técnico para Administração da Solução	R\$ 35.987,04	-	-	VALOR UNITÁRIO = R\$1.762,25*160 (Quantitativo) = R\$ 281.960,00 * 3 anos = R\$ 845.880,00
					PARA O ITEM 3 - Licenciamento para Gestão de Vulnerabilidades -

VULNERABILIDADES - SUBSCRIÇÃO COM PLATAFORMA EM NUVEM (SAAS)					Segurança de Contêineres: • VALOR UNITÁRIO = R\$ 1.500,00*140 (Quantitativo) = R\$ 210.000,00 * 3 anos = R\$ 630.000,00 PARA O ITEM 4 - Licenciamento para Gestão de Postura de Identidade (ISPM): • VALOR UNITÁRIO = R\$27.406,66*32 (Quantitativo) = R\$ 877.013,12* 3 anos = R\$ 2.631.039,36 PARA O ITEM 5 - Treinamento Técnico para Administração da Solução: • VALOR UNITÁRIO = R\$ 4.498,38*8 (Quantitativo) = R\$ 35.987,04 PARA O ITEM 6 - Serviço de Suporte Técnico: • VALOR UNITÁRIO = R\$ 27,60* 8.200 (Quantitativo) = R\$ 226.320,00*3 anos = R\$ 678.960,00 SOMA DOS ITENS: 1+2+3+4+5+6
	Item 6 - Serviço de Suporte Técnico	R\$ 226.320,00	R\$ 226.320,00	R\$ 226.320,00	
TOTAL					R\$ 5.284.496,40

9. ANÁLISE TÉCNICA E ECONÔMICA DAS SOLUÇÕES VIÁVEIS

9.1. O processo de gestão de vulnerabilidades, previsto como boa prática em frameworks de segurança como CIS Controls e NIST CSF, tem se consolidado no mercado com a vertente de sistemas que funcionam integralmente em nuvem, no modelo de Software como Serviço (SaaS). Esta abordagem moderna é a tendência adotada por organizações que buscam maior eficiência, escalabilidade e agilidade.

9.2. Para além da análise de cenários e da Consulta Pública nº 5/2024, a equipe de planejamento realizou aprofundada pesquisa de mercado, incluindo reuniões com diversos fabricantes e fornecedores de soluções de gestão de vulnerabilidades, com o objetivo de compreender os aspectos técnicos, modelos de licenciamento, estruturas de suporte e demais características das soluções disponíveis. A pesquisa identificou a existência de mais de um fabricante e fornecedor com capacidade de disponibilizar soluções compatíveis com as necessidades da contratação, destacando-se, entre as soluções avaliadas, as plataformas dos fabricantes Qualys e Tenable, que demonstraram capacidade de atender de forma integrada à totalidade dos requisitos essenciais estabelecidos. Dessa forma, não se caracteriza situação de fornecedor exclusivo, uma vez que há pluralidade de agentes aptos a fornecer soluções para atendimento ao objeto. As demais soluções analisadas, embora apresentem funcionalidades e recursos relevantes, não demonstraram, no conjunto da avaliação realizada, capacidade de atender integralmente e de forma unificada a todos os requisitos essenciais definidos. A documentação decorrente da pesquisa de mercado e das interações realizadas com fabricantes e fornecedores integra os autos, servindo de subsídio para demonstrar a existência de alternativas no mercado e afastar eventual restrição indevida à competitividade.

9.3. As reuniões, conduzidas por iniciativa da equipe de contratação, ocorreram diretamente com fabricantes e seus distribuidores oficiais. Essa abordagem proativa

permitiu discussões aprofundadas sobre arquitetura, funcionalidades (*features*), modelos de licenciamento e outros aspectos relevantes, garantindo um alinhamento preciso entre as necessidades do Tribunal e as capacidades das soluções de mercado.

9.4. A pesquisa revelou que as plataformas dos fabricantes Qualys e Tenable possuem portfólio para atender a todos os requisitos essenciais de forma integrada. As demais soluções analisadas, embora robustas em suas especialidades, não demonstraram, à primeira vista, capacidade de atender à totalidade dos requisitos em uma plataforma unificada. Com base nesse levantamento, os requisitos técnicos foram refinados para garantir a competitividade, permitindo a participação de, no mínimo, estas duas plataformas líderes de mercado, sem comprometer as necessidades do Tribunal.

9.5. A análise aprofundada dos cenários, corroborada pela pesquisa de mercado, demonstra que a contratação de uma solução de gerenciamento de vulnerabilidades na modalidade SaaS (Cenário 3) é a alternativa técnica e economicamente mais viável para atender às necessidades da Justiça Federal da 1ª Região.

9.6. **Do ponto de vista técnico**, o modelo SaaS atende plenamente à exigência de uma plataforma unificada, com visibilidade integrada de ameaças em rede, web, contêineres e identidade. Garante, por meio de SLAs contratuais, suporte contínuo e atualizações de segurança aplicadas de forma transparente pelo fabricante. Isso contrasta fortemente com os cenários Open Source e On-Premises, que impõem uma carga técnica insustentável sobre a equipe interna, seja pela necessidade de desenvolver uma plataforma customizada ou de gerenciar uma complexa infraestrutura de servidores.

9.7. **Do ponto de vista econômico**, o Cenário 3 apresenta a melhor relação custo-benefício. Ao eliminar o Custo de Aquisição (CAPEX) e consolidar os gastos em um Custo Operacional (OPEX) previsível, o modelo otimiza o uso dos recursos orçamentários. A análise revelou que o custo apenas com pessoal para sustentar uma solução *open source* seria proibitivo, enquanto o modelo *on-premises* exigiria um desembolso inicial massivo em hardware e licenças.

9.8. A abordagem SaaS transfere para a contratada a responsabilidade pela manutenção da plataforma, permitindo que a equipe da SECIN concentre seus esforços na gestão estratégica do risco cibernético e na coordenação das ações corretivas, em vez de se dedicar à sustentação de ferramentas e infraestrutura. Este modelo fortalece a atuação da área de segurança, proporcionando maior agilidade e eficiência.

9.9. Assim, fica evidente que a adoção do Cenário 3, escolhido pela equipe de planejamento, resultará no melhor aproveitamento dos recursos, na maior eficiência operacional e no mais robusto fortalecimento da postura de segurança cibernética da Administração.

10. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

10.1. Transição contratual

10.1.1. Ao final do contrato, a CONTRATADA deverá fornecer todos os dados pertencentes ao TRF1 em formato exportável (CSV, JSON ou similar) e apoiar a equipe do Tribunal em um plano de transição, caso uma nova solução seja contratada, garantindo a continuidade do processo de gestão de vulnerabilidades.

10.2. Adequações do ambiente do órgão impostas pela solução escolhida

10.2.1. Conforme **Anexo II** do ETP.

10.3. Demonstração de que o mercado atende aos requisitos mínimos

10.3.1. A demonstração de que o mercado possui soluções para atender aos requisitos da presente contratação, que tem por objeto a aquisição de solução de Gestão de Vulnerabilidades na modalidade Software como Serviço (SaaS), é realizada por meio da pesquisa de preços detalhada na Seção 6.3 e da Consulta Pública nº 5/2024 (20947125), que confirmou a existência de soluções e fornecedores aptos. O objeto desta contratação, por se tratar de solução de software como serviço (SaaS), possui um mercado consolidado e competitivo.

10.3.2. Inicialmente, o planejamento do TRF1 contemplava a contratação unificada

de serviços gerenciados de segurança cibernética, abrangendo diversos pilares como operação e atendimento a requisições, monitoramento e visibilidade de eventos, orquestração, automação e resposta a eventos, gestão de incidentes (blue team), e gestão de vulnerabilidades. No entanto, após aprofundada análise e identificação de riscos associados a um modelo de contratação tão abrangente, optou-se pela separação desses objetos em licitações apartadas, buscando maior eficiência e mitigação de riscos na gestão contratual.

10.3.2.1. Nesse contexto, a Consulta Pública nº 5/2024 (20947125), embora realizada com foco no escopo mais amplo inicialmente previsto, incluiu expressamente a "gestão de vulnerabilidades" como um de seus componentes. Sua realização demonstrou a ampla participação da sociedade e das empresas interessadas, que contribuíram com sugestões e críticas às especificações técnicas, confirmando a disponibilidade de soluções e a competitividade do mercado também para o segmento específico de gestão de vulnerabilidades, que é o objeto exclusivo deste Estudo Técnico Preliminar (ETP).

10.3.2.2. Link da consulta pública: <https://www.trf1.jus.br/trf1/contratos-arp-e-notas-de-empenho/consulta-publica>

10.3.3. Além dos primeiros subsídios coletados na consulta pública, a equipe de contratação fez diversas reuniões com revendedores e fabricantes, conforme explicitado anteriormente no item 9.

10.4. Aplicação de cotas a microempresas (ME) e empresas de pequeno porte (EPP)

10.4.1. Não se aplica, visto que a cota reservada se aplica somente a bens divisíveis, nos termos do artigo 48, inciso III da [Lei Complementar nº 123/2006](#) e do artigo 8º do [Decreto nº 8.538/2015](#), uma vez que a contratação trata-se de serviços na modalidade de Software como Serviço (SaaS):

Art. 48. Para o cumprimento do disposto no art. 47 desta Lei Complementar, a administração pública:

III - deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte.

(...)

Art. 8º Nas licitações para a aquisição de bens de natureza divisível, e desde que não haja prejuízo para o conjunto ou o complexo do objeto, os órgãos e as entidades contratantes deverão reservar cota de até vinte e cinco por cento do objeto para a contratação de microempresas e empresas de pequeno porte.

10.5. Parcelamento da solução

10.5.1. Recomenda-se **ADJUDICAÇÃO POR GRUPO**, a considerar:

10.5.1.1. A definição pela contratação dos serviços dos itens em grupo único levou em consideração o prejuízo de ordem técnica que poderiam ocorrer casos os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para sejam efetivos e alcancem os resultados pretendidos com a contratação.

10.5.1.2. Os itens devem ainda atender a segurança da rede do CONTRATANTE de maneira holística, monitorando-a de ponta a ponta e atuando na detecção e resposta a incidentes cibernéticos com visibilidade e automação.

10.5.1.3. O agrupamento de itens em um único grupo, na realização dos pregões eletrônicos, é orientação constante do Acórdão nº 861/2013 - Plenário, do Tribunal de Contas da União: "São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si".

10.5.1.4. A solução é considerada **indivisível** e, portanto, não deve ser parcelada. O principal requisito de negócio e técnico desta contratação é a

obtenção de uma **plataforma unificada e integrada**, capaz de correlacionar dados de diferentes vetores de ataque (rede, web, contêineres, identidades) para proporcionar uma visão holística e priorizada do risco. O parcelamento do objeto (e.g., contratar fornecedores distintos para DAST e análise de rede) anularia o benefício central da solução e comprometeria o atendimento a um requisito explícito do **ANEXO I**.

10.5.1.5. Ressaltamos que não há restrição de competitividade ao realizar o agrupamento, uma vez que os fornecedores de serviços técnicos de segurança da informação são habilitados a atender o serviço especificado.

10.5.1.6. Ademais, o agrupamento dos serviços, também, se justifica pelo aumento da eficiência administrativa por meio da otimização do gerenciamento do fornecedor. Deste modo, o não parcelamento do objeto no presente caso não é uma afronta a Súmula no 247 do TCU, conforme jurisprudências observadas nos Acórdãos no 5.260/2011 – TCU – 1ª Câmara e no 861/2013 – TCU – Plenário, que tratam de questões de economicidade e necessidade de padronização.

10.5.2. Embora o objeto da contratação apresente características que poderiam justificar a adjudicação global, optou-se pela **adjudicação por grupo**, considerando as particularidades da contratação por meio do Sistema de Registro de Preços, a participação de outros órgãos na futura Ata de Registro de Preços, e as barreiras existentes para o registro de empenho no caso de adjudicação global, com participação simultânea de diversos órgãos com quantidades diferentes.

10.5.2.1. A participação de outros órgãos na Ata de Registro de Preços também foi considerada na definição dessa sistemática, especialmente diante da incerteza quanto à forma de emissão das respectivas notas de empenho pelos órgãos participantes, Caso fosse adotada a adjudicação global, o objeto seria registrado como um único item no sistema, sem quantidades definitivas para cada subitem, o que poderia dificultar a emissão do empenho pelos diversos órgãos participantes da ata, além do acompanhamento e o controle dos quantitativos efetivamente utilizados por cada órgão.

10.5.2.2. Assim, considerando que os órgãos participantes poderão realizar contratações decorrentes da Ata de Registro de Preços de acordo com suas necessidades e quantitativos registrados, a estruturação do objeto em grupo único, composto por itens individualizados, mostra-se mais adequada para a operacionalização da futura Ata e emissão dos empenhos. Essa modelagem permite que os quantitativos registrados sejam controlados de forma individualizada, possibilitando ao órgão acompanhar com maior precisão os saldos disponíveis.

10.5.2.3. Portanto, considerando a realização de IRP e a participação de outros órgãos na futura Ata de Registro de Preços, bem como a necessidade de assegurar maior segurança e flexibilidade na operacionalização das contratações decorrentes da Ata, especialmente quanto à emissão das notas de empenho e ao controle dos quantitativos registrados, conclui-se que a adjudicação por grupo constitui a alternativa mais adequada para a gestão e

10.6. Descrição integral da solução

10.6.1. Contratação de **Solução de Gerenciamento de Vulnerabilidades, na modalidade Software como Serviço (SaaS)**, para análise de ativos de rede, análise dinâmica de aplicações web (DAST), análise de segurança de contêineres e monitoramento de identidades. A contratação abrange o licenciamento de uso da plataforma e sua implantação por 36 (trinta e seis) meses, serviços suporte técnico especializado e treinamento.

10.7. Benefícios diretos

10.7.1. **Visibilidade Unificada e Centralizada do Risco Cibernético:** Obtenção de uma visão completa e integrada da superfície de ataque, correlacionando vulnerabilidades em infraestrutura, aplicações, contêineres e

identidades em uma única plataforma.

10.7.2. Priorização Inteligente de Ameaças: Capacidade de focar os esforços de remediação nas vulnerabilidades que representam o maior risco real para a instituição, com base em inteligência de ameaças, explorabilidade e criticidade dos ativos.

10.7.3. Redução Efetiva da Superfície de Ataque: Implementação de um processo contínuo e proativo de identificação e gestão de falhas de segurança, diminuindo as oportunidades para agentes maliciosos.

10.7.4. Otimização da Eficiência Operacional: Automação de tarefas de varredura, análise e geração de relatórios, liberando a equipe de segurança para atividades estratégicas de análise e resposta a riscos.

10.8. Benefícios indiretos

10.8.1. Fortalecimento da Governança de Segurança e Conformidade Regulatória: Geração de evidências e relatórios que facilitam a auditoria e demonstram a conformidade com normativas como a LGPD e a ENSEC-PJ, além de boas práticas como o CIS Controls.

10.8.2. Melhora na Tomada de Decisão Estratégica: Fornecimento de dados e métricas de risco que subsidiam decisões de investimento em segurança e a alocação de recursos de forma mais eficaz.

10.8.3. Aumento da Resiliência Cibernética Institucional: Construção de uma base sólida para um programa de segurança maduro, aumentando a capacidade do Tribunal de prevenir, detectar e responder a incidentes de segurança.

10.8.4. Manutenção de Análise Histórica: Criação de um repositório centralizado de dados sobre vulnerabilidades, permitindo a análise de tendências e a avaliação da eficácia do processo de gestão ao longo do tempo.

10.9. Ciclo de vida

10.9.1. A avaliação do ciclo de vida do objeto visa assegurar a escolha da solução que melhor atenda às necessidades da Justiça Federal da 1ª Região (JF1), garantindo a execução eficaz e eficiente dos serviços contratados. Em conformidade com o art. 9º, inciso III, da Instrução Normativa SEGES/ME nº 81, de 2022, o ciclo de vida foi estruturado nas seguintes etapas:

10.9.1.1. Provisionamento e Ativação: O ciclo inicia-se com a disponibilização do acesso à assinatura da subscrição (criação do ambiente do contratante na plataforma SaaS e fornecimento de credenciais de acesso). Nesta fase, adquire-se o direito de uso da assinatura que contém um plano de suporte e garantia técnica.

10.9.1.2. Entrega: Será efetuada pela CONTRATADA, de forma eletrônica, mediante envio de credenciais de acesso ao ambiente SaaS e comprovação do licenciamento.

10.9.1.3. Parametrização e Configuração : A CONTRATADA realizará as parametrizações iniciais necessárias para a plena utilização dos módulos contratados, sem ônus adicional, estando os custos incluídos no valor do licenciamento. Esta etapa compreende a configuração de políticas de varredura, integração com diretórios ativos, definição de escopos de análise e demais ajustes necessários à utilização efetiva da solução.

10.9.1.4. Suporte Técnico: A assinatura da subscrição contempla os serviços de suporte e atualização durante o período vigência do contrato.

10.9.2. Essas são as principais fases do ciclo de vida do serviço de fornecimento das subscrições de uso de softwares.

10.10. Outras informações da solução a ser contratada

10.10.1. Da base legal e enquadramento do objeto

10.10.1.1. Modalidade e Tipo de licitação: Recomenda-se que esta

licitação seja efetuada nos moldes de **Pregão Eletrônico**, conforme disposto no inciso I, art. 28, da Lei n. 14.133/2021, visto se tratar de contratação de serviço comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos no edital, por meio de especificações usuais de mercado.

10.10.1.2. **Forma e critérios de seleção do fornecedor:** Para o objeto tratado neste ETP, não há ponderação de qualidade técnica das propostas que excedam os requisitos mínimos, de forma que o critério de julgamento será pelo **MENOR PREÇO**.

10.10.1.3. **Critério de aceitabilidade da proposta:** Recomenda-se **ADJUDICAÇÃO POR GRUPO**.

10.10.1.4. **Natureza da contratação:** O objeto da contratação é de natureza contínua.

10.10.1.4.1. Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.

10.10.1.4.2. Por sua vez, a doutrina entende que a caracterização de um serviço como contínuo requer a demonstração de sua essencialidade habitualidade para o Contratante. A essencialidade atrela-se à necessidade de existência e manutenção do contrato, pelo fato de eventual paralisação da atividade contratada implicar em prejuízo ao exercício das atividades da Administração contratante. Já a habitualidade é configurada pela necessidade de a atividade ser prestada mediante contratação de terceiros de modo permanente.

10.10.1.4.3. Este serviço é de provimento contínuo e ininterrupto (24 horas por dia, 7 dias por semana) e tem como objetivo proteger e garantir a segurança do ambiente tecnológico do TRF1. Sua natureza contínua é justificada pela importância da gestão de vulnerabilidades na segurança da informação, sendo um mecanismo crucial para prevenir ataques cibernéticos. A ferramenta detecta ameaças que poderiam interromper as atividades do TRF1 ou comprometer informações vitais. Além disso, escaneamentos de vulnerabilidades e manutenções específicas serão executados em horários alternativos para evitar indisponibilidade e impacto na produtividade. Assim, a solução deve estar acessível em tempo integral.

10.10.1.4.4. O prazo de vigência da contratação é de **36 (trinta e seis) meses**, contados a partir da assinatura do contrato, nos termos do art. 106 da Lei nº 14.133, de 2021. Para os subitens 1.1, 1.2, 1.3 e 1.4, o prazo de vigência das respectivas subscrições será de 36 (trinta e seis) meses, contados a partir do Recebimento Definitivo do licenciamento.

10.10.1.4.4.1. A adoção do prazo contratual de 36 (trinta e seis) meses fundamenta-se na natureza contínua da solução de Tecnologia da Informação e na necessidade de assegurar sua disponibilidade durante todo o período contratual, considerando os princípios da eficiência, do planejamento e da economicidade previstos no art. 5º da Lei nº 14.133, de 2021. A vigência plurianual mostra-se adequada à continuidade da solução e à obtenção de condições mais vantajosas para a Administração.

10.10.1.4.4.2. Nos termos do art. 106 da Lei nº 14.133, de 2021, os contratos de serviços e fornecimentos contínuos poderão ser celebrados por prazo de até 5 (cinco) anos, desde que atendidas as condições estabelecidas no referido dispositivo. O §2º do mesmo artigo estabelece a aplicação dessa disciplina à utilização de programas de informática. Nesse sentido, a adoção da vigência de

36 (trinta e seis) meses proporciona:

10.10.1.4.4.2.1. Diluição dos custos iniciais de implantação e configuração, resultando em um custo mensal otimizado;

10.10.1.4.4.2.2. Estímulo à competitividade, permitindo propostas comerciais mais vantajosas pela maior previsibilidade contratual;

10.10.1.4.4.2.3. Redução de custos transacionais, administrativos e operacionais, ao mitigar a necessidade de prorrogações sucessivas e aditivos;

10.10.1.4.4.2.4. Melhoria na fiscalização e controle, com histórico consolidado de execução, facilitando a gestão do contrato;

10.10.1.4.4.2.5. Aderência às práticas de mercado, em que soluções SaaS são tipicamente ofertadas com suporte e garantia em ciclos plurianuais;

10.10.1.4.4.2.6. Mitigação de riscos de inadimplemento, ao proporcionar maior estabilidade contratual e retorno sobre investimento ao contratado.

10.10.1.4.4.3. A adoção de prazo contratual de **36 (trinta e seis) meses** decorre da natureza contínua da solução e da necessidade de garantir sua disponibilidade durante o período contratado, observadas as disposições do art. 106 da Lei nº 14.133, de 2021. Eventuais prorrogações deverão observar o disposto no art. 107 da mesma Lei, desde que atendidos os requisitos legais e demonstrada a manutenção da vantajosidade para a Administração. A vigência plurianual não afasta a necessidade de observância da disponibilidade orçamentária correspondente a cada exercício financeiro.

10.10.1.4.4.4. Outrossim, para além dos aspectos relacionados à vantajosidade econômica acima apontados, mencione-se que a inaplicabilidade da regra de aplicação da fixação do prazo anual justifica-se pela contratação de serviços que satisfazem as necessidades permanentes deste Tribunal. Em outros termos, a autorização legal para fixar prazos mais longos nos contratos contínuos está vinculada ao objeto das contratações dessa natureza, sejam eles bens essenciais ou não, cujo serviço se torna permanente e o termo final da vigência do prazo contratual não induz necessariamente o fim do fornecimento do bem ou da prestação do serviço. Essas razões escapam à mera necessidade de apresentação da vantajosidade econômica, atraindo o vínculo contratual para a relevância do seu objeto e evidência que o prazo constitui importante elemento econômico do contrato.

10.10.1.4.5. A disponibilização das licenças na modalidade SaaS será realizada de forma integral e imediata, por ocasião da ativação, conforme o quantitativo necessário e demandado pela Contratante. O parcelamento refere-se exclusivamente ao pagamento da contratação, que será realizado em parcelas anuais, conforme as condições estabelecidas neste Termo de Referência, não caracterizando fornecimento parcelado do objeto.

10.10.1.5. Do Registro de Preço

10.10.1.5.1. Deverá ser adotado o Sistema de Registro de Preços, conforme estabelece o Decreto n. 11.462/2023, pelo seguinte aspecto: quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas (art. 3º, inciso III) e aquisição de bens com previsão de entregas parceladas (art. 3º, inciso II).

10.10.1.5.2. Prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, podendo ser prorrogado por igual período, nos termos do Art. 84 da Lei nº 14.133/2021. A vigência da Ata não implica obrigatoriedade de contratação, servindo apenas como instrumento de registro de preços para demandas futuras.

10.10.1.5.2.1. Justifica-se a possibilidade de prorrogação da vigência da Ata de Registro de Preços, conforme Art. 84 da Lei 14.133/2021, bem como a possibilidade de adesão por novos órgãos durante este período. A renovação dos quantitativos registrados dependerá de nova contratação, mediante celebração de instrumento próprio (contrato ou ordem de serviço), observadas as condições de mercado e a disponibilidade orçamentária.

10.10.2. Das condições de participação

10.10.2.1. Será assegurada a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei n. 14.133/2021.

10.10.2.2. Será admitida a participação de profissionais sob a forma de cooperativa, de acordo com o previsto no art. 16 da Lei n. 14.133/2021.

10.10.3. Subcontratação

10.10.3.1. Não é admitida a subcontratação do objeto contratual.

11. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de **R\$ 5.284.496,40 (cinco milhões, duzentos e oitenta e quatro mil quatrocentos e noventa e seis reais e quarenta centavos)**, conforme análise crítica e justificativas apresentadas na Tabela de Comparação de Custos (Seção 8.2), considerando o período de 36 meses.

GRUP	ITEM	DESCRIÇÃO	QUANT	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL 12 MESES	VALOR TOTAL 36 MESES
1	1	Licenciamento de Gestão de Vulnerabilidades - Ativos de Rede	7.000	Licenças para Ativos de Rede	R\$ 22,03	R\$ 154.210,00	R\$ 462.630,00
	2	Licenciamento de DAST - Análise Dinâmica de Aplicações Web	160	Licenças para Aplicações Web	R\$ 1.762,25	R\$ 281.960,00	R\$ 845.880,00
	3	Licenciamento de Segurança de Contêineres	140	Licenças para 1 Worker Node (kubernetes)	R\$ 2.091,20	R\$ 210.000,00	R\$ 630.000,00
	4	Licenciamento para Gestão de Postura de Identidade (ISPM)	32	Licença por Usuário (grupo de 1000 Usuários Monitorados)	R\$ 31.750,00	R\$ 877.013,12	R\$ 2.631.039,36
	5	Treinamento Técnico para Administração da Solução	8	Turma (grupo de 10 usuários por turma)	R\$ 7.149,14	R\$ 35.987,04	R\$ 35.987,04
	6	Serviço de Suporte Técnico	8.200	Unidade de Suporte por Ativo Equivalente (USAE)/mês	R\$ 27,60	R\$ 226.320,00	R\$ 678.960,00
VALOR TOTAL						R\$ 1.785.490,16	R\$ 5.284.496,40

12. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO 12.1. A equipe responsável pelo planejamento da contratação, ciente das regras e diretrizes da Resolução CNJ nº 468/2022 e com base nos elementos apresentados neste Estudo Técnico Preliminar, DECLARA a viabilidade da contratação. A análise demonstrou que a necessidade está alinhada aos objetivos estratégicos do TRF1, os requisitos são claros e factíveis, o mercado possui soluções maduras para atendê-los e o custo estimado é compatível com os benefícios esperados para o fortalecimento da segurança cibernética do Tribunal.
13. APROVAÇÃO E ASSINATURA 13.1. Conforme o § 2º do Art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC: 13.1.1. A Equipe de Planejamento da Contratação foi instituída pelo Despacho-DIGES (24584004).
Integrante técnico: (nome e matrícula do integrante técnico) O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação. Juarez de Oliveira - TR302241 Integrante Técnico
Integrante requisitante: (nome e matrícula do integrante demandante) O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação. Luiz Alberto Lima da Costa - TR136203 Integrante Requisitante
Autoridade máxima da área de TI: (nome e matrícula do diretor da Secin) O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que aprovo o artefato e encaminho para prosseguimento da contratação. Janderson Casado de Vasconcelos Santos - TR63903 Secretário de Tecnologia da Informação

1. REQUISITOS TRANSVERSAIS DA SOLUÇÃO (PLATAFORMA):

1.1. Arquitetura, Integração e Disponibilidade

1.1.1. Centralização e Interoperabilidade: A solução poderá ser composta por módulos de um ou mais fabricantes, desde que gerenciados de forma centralizada por interface única ou integração nativa que garanta a consolidação das informações em console unificado. A integração deve permitir correlação de dados e automação de fluxos de forma transparente, não sendo aceito o simples compartilhamento de credenciais (*Single Sign-On - SSO*) sem centralização de dados.

1.1.2. Hibridismo de Scanners: A solução deverá possuir scanners em nuvem para varreduras externas e scanners internos (on-premises) gerenciados centralizadamente pela plataforma.

1.1.3. Autonomia de Base: A solução deve possuir base de vulnerabilidades própria e funcionar independentemente da disponibilidade de serviços de terceiros (ex: NVD, CVE MITRE).

1.1.4. Integração via API: Deve possuir API (*Application Programming Interface*) para automação e integração com aplicações de terceiros (SIEM, EDR, DEX) para intercâmbio de dados de ativos e vulnerabilidades.

1.1.5. Maturidade do Produto: É vedado o uso de produtos que não sejam "de prateleira" em versão comercial (*General Availability - GA*), sendo proibidas versões experimentais ou beta no momento da publicação do edital.

1.2. Segurança, Auditoria e Relatórios

1.2.1. Autenticação Forte: Deve permitir autenticação com múltiplos fatores (MFA) para os usuários da plataforma.

1.2.2. Proteção de Dados em Trânsito: A solução deve fornecer criptografia de ponta a ponta em todas as comunicações entre agentes, *scanners* e a nuvem.

1.2.3. Auditoria Imutável: Deve permitir a auditoria de todas as atividades (ex: login, criação de scans, relatórios). Os registros de auditoria devem ser imutáveis, sem possibilidade de alteração ou deleção por usuários.

1.2.4. Exportação de Logs: Deve permitir o envio de logs de auditoria para SIEM ou servidor de logs externo.

1.2.5. Segregação de Funções (RBAC): Deve permitir a segregação administrativa por usuário ou grupos, baseada em ativo, tipo ou localidade.

1.2.6. Formatos de Saída: Os relatórios gerados devem suportar obrigatoriamente os formatos PDF, CSV e HTML.

1.3. Regras de Licenciamento

1.3.1. Titularidade: O licenciamento deve estar registrado junto ao fabricante em nome da CONTRATANTE, vedado o compartilhamento de licenças com outras entidades.

1.3.2. Abrangência: Devem estar inclusos no licenciamento base todos os componentes necessários (como software, *appliances* virtuais, sensores e agentes) para o pleno funcionamento.

2. ITEM 1 - LICENCIAMENTO DE GESTÃO DE VULNERABILIDADES - ATIVOS DE REDE - UNIDADE: LICENÇA POR ATIVO

2.1. Escopo e Inventário Automático

2.1.1. Automação de Verificação: A solução deve automatizar a verificação de vulnerabilidades, configurações seguras e conformidade de sistemas.

2.1.2. Inventário Dinâmico: A solução deve propiciar um inventário detalhado de hosts e aplicações, contendo: endereços IP, nome do ativo, Sistema Operacional, tipo do ativo, softwares instalados (versão/patch), correlação com vulnerabilidades, imagens de containers e URLs de aplicações web.

2.1.3. Modalidades de Scan: Deve realizar varreduras autenticadas e não-autenticadas.

2.1.4. Agentes e Redes: Deve permitir a instalação de agentes (Windows/Linux) para varreduras automáticas independentes de rede.

2.2. Deve permitir a instalação de agentes em sistemas operacionais (Windows e Linux) para varreduras automáticas, independente de escaneamento.

2.3. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance).

2.4. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) por meio da rede.

2.5. Deve suportar varreduras em dispositivos de IoT que possuam interfaces de comunicação TCP/IP.

2.6. Deve ser capaz de identificar no mínimo 100.000 CVEs (Common Vulnerabilities and Exposures).

2.7. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos.

2.8. Deve atribuir a todas as vulnerabilidades uma severidade baseada em scores de CVSS v3.1 ou superior.

2.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente.

2.10. Deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

2.10.1. Por sistema operacional.

2.10.2. Por determinado software instalado.

2.10.3. Por ativos impactados por determinada vulnerabilidade.

2.11. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.

2.12. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual.

2.13. A solução deve possuir um sistema de pontuação e priorização de riscos dos ativos próprio.

2.14. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

2.14.1. CVSS v3.1 ou 4.0 Score;

2.14.2. Idade da Vulnerabilidade;

2.14.3. Se existe ameaça ou exploit público;

2.14.4. Número de produtos afetados pela vulnerabilidade;

2.14.5. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo.

2.14.6. Classificação do ativo pelo cliente.

2.15. A solução deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo.

2.16. A solução deve ser licenciada para o uso de, no mínimo, 14 (quatorze) sensores passivos de rede, permitindo o monitoramento em tempo real.

2.17. Deve ser possível determinar, em tempo real, quais portas de serviços (UDP/TCP) estão abertas em determinado ativo.

2.18. A solução deve ser capaz de realizar, de forma contínua, a descoberta de novos ativos para, no mínimo:

2.18.1. Bancos de dados;

2.18.2. Hipervisores (no mínimo VMWare ESX/ESXi);

2.18.3. Dispositivos de rede;

2.18.4. Microcomputadores;

2.18.5. Aplicações web.

2.19. O resultado dos scans deve informar as possíveis mitigações e a existência de exploits públicos para a vulnerabilidade.

2.20. Deve ser capaz de realizar auditoria de conformidade nos ativos de forma ilimitada.

2.21. Deve realizar scans de conformidade para os padrões CIS e PCI.

2.22. Deve possuir modelos prontos de padrões de configuração, no mínimo para CIS Benchmarks.

2.23. Deve suportar a verificação de conformidade para, no mínimo:

2.23.1. Servidores Linux;

2.23.2. Servidores Windows;

2.23.3. Desktops Windows;

2.23.4. Desktops Linux.

2.24. Deve permitir a criação de políticas próprias para realização de verificação de conformidade.

2.25. A solução deve calcular os riscos relativos à exposição dos ativos da instituição na Internet.

3. ITEM 2 - LICENCIAMENTO DE DAST - ANÁLISE DINÂMICA DE APLICAÇÕES WEB - UNIDADE: LICENÇA POR APLICAÇÃO WEB

3.1. Escopo e Inventário de Aplicações

3.1.1. Identificação de Ativos: A solução deve propiciar um inventário das aplicações web contendo, no mínimo, a URL/URI de cada aplicação monitorada.

3.1.2. Abrangência Técnica: Deve realizar análise dinâmica (DAST) em aplicações web e APIs REST, executando varreduras por meio de endereços IP ou FQDN (DNS).

3.1.3. Referenciais de Vulnerabilidade: O escaneamento deve basear-se, no mínimo, nas listas OWASP Top 10 e OWASP Top 10 API Security Risks, sem se limitar a estas.

3.1.4. Proteção de Dados: A solução deve identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal (PII).

3.2. Arquitetura de Scan e Conectividade

3.2.1. Flexibilidade de DNS e Sensores: Deve suportar a substituição de entradas de DNS (override) para testes em ambientes internos ou disponibilizar sensor on-premises para a realização desses testes.

3.2.2. Simultaneidade de Processos: A solução deve ser capaz de realizar testes e varreduras em aplicações separadas de forma simultânea.

3.2.3. Integração com APIs: Deve possuir suporte nativo a Postman Collections para a realização de testes em APIs REST.

3.2.4. Protocolos Legados: A solução deverá ser compatível com a avaliação de web services tanto no padrão REST quanto no padrão SOAP.

3.3. Funcionalidades de Auditoria e Crawling

3.3.1. Navegação Automatizada (Crawling): Deve realizar a descoberta automática de URLs e da estrutura da aplicação, permitindo o uso de scripts customizados com parâmetros definidos pelo usuário.

3.3.2. Profundidade de Análise: Para varreduras extensas, deve auditar Cookies,

Headers, formulários, links, nomes e valores de parâmetros, elementos JSON, XML

3.3.3. Automação de Testes: A solução deve suportar a integração com o software Selenium para permitir sequências de autenticações complexas e a importação de scripts previamente configurados.

3.3.4. Exclusões Inteligentes: Deve ser capaz de excluir URLs específicas via expressões regulares e tipos de arquivos por meio de suas extensões.

3.4. Métodos de Autenticação Suportados

3.4.1. Diversidade de Esquemas: A solução deve suportar os seguintes esquemas de autenticação:

3.4.1.1. Autenticação Básica (Digest);

3.4.1.2. NTLM;

3.4.1.3. Autenticação de Cookies;

3.4.1.4. Autenticação via Selenium ou outra ferramenta de automação de testes.

3.5. Verificações de Segurança e Integridade

3.5.1. Reavaliação Focalizada (Reteste): Deve oferecer suporte à capacidade de testar novamente uma vulnerabilidade específica detectada anteriormente no aplicativo web, de forma isolada.

3.5.2. Infraestrutura de Conexão: A solução deve realizar a avaliação dos certificados de segurança e dos protocolos suportados (SSL/TLS) nas conexões HTTPS.

3.5.3. Detecção de Malware e Dia Zero: Deve identificar infecções por códigos maliciosos nas propriedades da aplicação e detectar vulnerabilidades de "dia zero", permitindo o acompanhamento de tendências de infecção.

3.6. Gestão de Resultados e Relatórios

3.6.1. Visão Histórica e Temporal: A solução deve exibir os resultados das varreduras de forma temporal, permitindo o acompanhamento da evolução das correções e o surgimento de novas vulnerabilidades.

3.6.2. Evidências Técnicas: Para vulnerabilidades de injeção (SQL, XSS, XSRF), deve evidenciar o payload injetado, a resposta da aplicação e os detalhes completos da requisição/resposta HTTP.

3.6.3. Suporte a Componentes Específicos: Deve possuir modelos prontos de varredura para componentes como Wordpress, AngularJS, Apache (Tomcat), ASP.NET, Bootstrap, jQuery, Nginx, PHP, Jboss/Wildfly e AJAX.

3.6.4. Planos de Remediação: Cada vulnerabilidade encontrada deve conter detalhes da falha, referências didáticas e soluções propostas para mitigação ou remediação.

4. ITEM 3 - LICENCIAMENTO DE SEGURANÇA DE CONTÊINERES - UNIDADE: LICENÇA POR WORKER NODE (KUBERNETS)

4.1. Escopo e Inventário de Ativos de Contêineres

4.1.1. Automação de Verificação: A solução deve automatizar a verificação de vulnerabilidades, configuração segura e conformidade de todo o ecossistema de contêineres.

4.1.2. Inventário Detalhado: Deve propiciar um inventário atualizado dos ativos, contemplando obrigatoriamente:

4.1.2.1. Tipo do ativo (imagem, registry, contêiner, etc.);

4.1.2.2. Imagens de contêineres e sua respectiva correlação com vulnerabilidades encontradas.

4.1.3. Localidade de Execução: A solução deve ser capaz de realizar análise de segurança em contêineres instalados tanto em ambiente on-premises quanto em nuvem pública.

4.2. Suporte a Infraestrutura e Orquestração

4.2.1. Integração com Provedores de Nuvem: Deve suportar integração nativa, no mínimo, com as nuvens AWS, Azure e GCP para o gerenciamento de contêineres.

4.2.2. Orquestração Local: Deve suportar clusters Kubernetes instalados em ambiente on-premises, independentemente do orquestrador utilizado.

4.2.3. Tecnologias de Runtime: A solução deve analisar a postura de segurança em ambientes que utilizem as tecnologias Docker e Containerd.

4.3. Análise de Vulnerabilidades e Ameaças

4.3.1. Escaneamento de *Registries*: Deve realizar a análise de imagens de contêineres diretamente nos repositórios (*registries*).

4.3.2. Detecção de Dados Sensíveis: A solução deve realizar buscas exaustivas em imagens para identificar a presença de segredos (*secrets*) expostos.

4.3.3. Identificação de Malwares: Deve ser capaz de analisar imagens em busca de códigos maliciosos conhecidos (malwares).

4.3.4. Hibridismo de Scanners: Deverá possuir scanners em nuvem para varreduras externas e sensores internos conectados e gerenciados pela plataforma.

4.4. Gestão de Postura e Resposta

4.4.1. Dashboard de Vulnerabilidades: A solução deve apresentar as vulnerabilidades detectadas em painel de controle (dashboard) imediatamente após a conclusão da avaliação da imagem.

4.4.2. Políticas de Bloqueio: Deve suportar a criação e aplicação de políticas de segurança para o bloqueio automático do uso de imagens, baseando-se no grau de vulnerabilidade encontrada.

4.4.3. Segregação Administrativa: Deve permitir a segregação na administração dos ativos de contêineres por usuário ou grupos, categorizada por tipo de ativo ou localidade.

5. ITEM 4 - LICENCIAMENTO PARA GESTÃO DE POSTURA DE IDENTIDADE (ISPM) - LICENÇA POR USUÁRIO (GRUPO DE 1000 USUÁRIOS MONITORADOS)

5.1. Escopo e Visibilidade Híbrida

5.1.1. Gestão de Postura (ISPM): A solução deve realizar a gestão da postura de segurança de identidades (Identity Security Posture Management), sendo capaz de analisar o Microsoft Active Directory (on-premises) e ambientes de identidade em nuvem (Microsoft Entra ID/Azure AD).

5.1.2. Identificação de Desvios: Deve visar a identificação proativa de desvios de configuração, vulnerabilidades de privilégios e caminhos de ataque.

5.1.3. Identidade Híbrida: A solução deve possuir capacidade nativa para correlacionar identidades entre o Active Directory local e o ambiente Microsoft Entra ID (Azure AD).

5.1.4. Suporte a Estruturas Complexas: Deve oferecer suporte nativo a múltiplos domínios e florestas complexas de diretório.

5.2. Análise de Caminhos de Ataque e Riscos

5.2.1. Mapeamento de Attack Path: A solução deve possuir capacidade de mapear visualmente rotas de escalada de privilégios.

5.2.2. Evolução de Privilégios: O mapeamento deve permitir identificar como um atacante pode evoluir de um usuário comum até o comprometimento total do domínio (Domain Admin).

5.2.3. Automação de Verificação: A solução deve automatizar a verificação de configurações seguras e a conformidade das identidades de forma contínua.

5.2.4. Centralização de Informações: Todos os módulos de identidade devem ser gerenciados de forma centralizada, permitindo a correlação de dados e a visualização consolidada em console unificado.

5.3. Requisitos de Análise de Exposição e Higiene (Inventário): A solução deve analisar e alertar sobre, no mínimo:

5.3.1. Inventário de Usuários: Manter registros atualizados de usuários ativos, inativos e desabilitados.

5.3.2. Grupos Privilegiados: Identificar contas com privilégios administrativos e usuários inseridos em grupos de alta criticidade.

5.3.3. Políticas de Senha: Verificar a conformidade e força das políticas de senha, identificando senhas fracas, em branco ou que nunca foram alteradas.

5.3.4. Atributos de Segurança: Monitorar contas cujas senhas nunca expiram, contas sem login por período prolongado e contas com delegação perigosa.

5.3.5. Infraestrutura de Diretório: Analisar o nível funcional do domínio, versões de protocolos (SMBv1/v2), configurações de LAPS e tempo de última alteração da conta KRBTGT.

5.3.6. Higiene de Dispositivos: Identificar computadores inativos, sem login recente e sistemas Windows legados ou descontinuados no diretório.

5.3.7. Identidades Não-Humanas (NHI): Identificar e monitorar riscos especificamente em contas de serviço, identidades de máquinas e chaves de API.

5.4. Monitoramento de Alterações e Indicadores de Ataque (IoA)

5.4.1. Monitoramento de Objetos Críticos: Realizar o acompanhamento contínuo de alterações em grupos privilegiados e objetos críticos do diretório.

5.4.2. Detecção em Tempo Real: Capacidade de detectar técnicas de quebras de Integridade de segurança.

5.4.3. Segregação Administrativa: Permitir a segregação na administração das identidades por usuário ou grupos, garantindo que a gestão seja feita por ativo ou localidade.

5.5. Arquitetura, Implementação e Licenciamento

5.5.1. Coleta de Dados: A integração com o MS Active Directory e EntraID deverá ser feita por meio de sensores ou agentes instalados no ambiente, garantindo a integridade dos dados.

5.5.2. Customização: A solução deve permitir que o usuário crie verificações customizadas ou novos indicadores de exposição.

5.5.3. Métrica de Licenciamento: O licenciamento deve ser isonômico, considerando a volumetria de 1.000 (mil) usuários ativos por unidade de contratação.

5.5.4. Relatórios de Remediação: Deve emitir relatórios executivos e técnicos que contenham planos de remediação guiados para as falhas encontradas.

6. ITEM 5 - TREINAMENTO TÉCNICO PARA ADMINISTRAÇÃO DA SOLUÇÃO - UNIDADE: TURMA (GRUPO DE 10 USUÁRIOS POR TURMA)

6.1. Organização, Idioma e Formato

6.1.1. Início dos Serviços: O treinamento deverá ser iniciado obrigatoriamente após a conclusão do serviço de provisionamento e configuração da solução.

6.1.2. Idioma e Escopo: O treinamento será ministrado em idioma português e deve possibilitar a instalação, configuração, operação, gerenciamento e solução de problemas da solução ofertada.

6.1.3. Modalidade Telepresencial: A capacitação deverá ser realizada de forma telepresencial, por meio de ferramenta a ser acordada com a CONTRATANTE, permitindo a interação dos alunos com o instrutor em tempo real.

6.1.4. Carga Horária e Escala: O treinamento terá carga horária mínima de 12 (doze) horas, divididas em 3 (três) dias. As aulas ocorrerão de segunda a sexta-feira (dias úteis), entre 08h e 18h.

6.1.5. Capacidade das Turmas: Cada turma será composta por, no máximo, 10 (dez) alunos.

6.2. Conteúdo Programático Obrigatório: O treinamento deve abordar, no mínimo, os seguintes tópicos técnicos:

6.2.1. Arquitetura e Acesso: Visão geral dos componentes, configuração de interface única/centralizada e parametrização de múltiplos fatores de autenticação (MFA).

6.2.2. Operação de Varredura: Criação de scans, instalação de agentes, sensores e proxies em diversos ambientes.

6.2.3. Gestão de Riscos e Ativos: Configuração de tags, grupos de ativos, parametrização para análise de riscos e uso de modelos de políticas de conformidade.

6.2.4. Módulos Especializados: Operação e integração com ambientes de contêineres e monitoramento de identidades (Active Directory e EntraID).

6.2.5. Governança e Integração: Geração de relatórios técnicos/executivos, uso da API para automação e gestão de logs de auditoria imutáveis.

6.2.6. Administração Avançada: Configuração de perfis de acesso segregados (RBAC) por localidade ou tipo de ativo.

6.2.7. Esclarecimento de dúvidas técnicas sobre qualquer tópico da solução;

6.2.8. Demais tópicos que a CONTRATADA, em acordo com a CONTRATANTE, julgar necessários para a completa utilização da solução.

6.3. Material Didático e Instrutor

6.3.1. Material de Apoio: A CONTRATADA deverá disponibilizar material didático como e-books, vídeos e conteúdos técnicos oficiais do fabricante.

6.3.2. Qualificação do Instrutor: O instrutor deverá possuir certificação na solução contratada, a qual deverá ser apresentada à CONTRATANTE antes do início do treinamento. Alternativamente, será aceita declaração formal do fabricante atestando a aptidão do instrutor para ministrar o treinamento.

6.4. Certificação: Ao final da capacitação, deverão ser fornecidos certificados de conclusão contendo:

6.4.1. Dados da Instituição: Nome da instituição de ensino e do curso.

6.4.2. Dados do Servidor: Nome do servidor capacitado e aproveitamento obtido.

6.4.3. Dados do Período: Data de início, término e carga horária total.

6.4.4. Escopo Técnico: Descritivo completo do conteúdo programático abordado.

7. ITEM 6 - SERVIÇO DE SUPORTE TÉCNICO - UNIDADE: UNIDADE DE SUPORTE POR ATIVO EQUIVALENTE (USAE)/MÊS

7.1. Natureza e Escopo do Serviço

7.1.1. Sustentação Operacional: O serviço consiste na prestação continuada de

suporte técnico especializado para a sustentação operacional de todos os módulos da solução (Ativos de Rede, DAST, Contêineres e Identidades).

7.1.2. Independência do Suporte Padrão: Este serviço de suporte especializado não se confunde com o suporte padrão do fabricante inerente às subscrições, tratando-se de serviço de apoio consultivo, operacional e técnico à equipe da CONTRATANTE.

7.1.3. Disponibilidade: O suporte deverá estar disponível nos dias úteis, de segunda-feira a sexta-feira, no horário das 08h às 18h, durante todo o período de vigência contratual, podendo ser prestado preferencialmente de forma remota ou, quando a intervenção remota não for tecnicamente viável, de forma presencial (on-site), sem ônus adicional para a CONTRATANTE.

7.1.4. Forma de Prestação: O suporte deverá ser prestado por profissionais especializados, instruídos e supervisionados pela CONTRATADA, compreendendo os ajustes, reparos, correções, orientações e demais intervenções necessárias à adequada utilização e ao perfeito funcionamento da solução contratada.

7.1.5. Operação da Solução: A operação da solução será realizada pela CONTRATANTE, podendo esta, a seu critério e quando necessário ao atendimento técnico, autorizar a criação de usuários específicos para os profissionais da CONTRATADA, observados os requisitos de segurança, autenticação, controle de acesso e rastreabilidade estabelecidos neste Anexo.

7.2. Metodologia de Remuneração (Métrica USAE)

7.2.1. Definição da Métrica: A remuneração será mensal, baseada na Unidade de Suporte por Ativo Equivalente (USAЕ).

7.2.2. Tabela de Pesos de Complexidade: Para o cálculo das USAEs, adotam-se os seguintes pesos por categoria de ativo monitorado:

7.2.2.1. Ativo de Rede: Peso 1;

7.2.2.2. Aplicação Web (URL): Peso 3;

7.2.2.3. Worker Node (Kubernetes): Peso 4;

7.2.2.4. Unidade de Monitoramento AD (Grupo de 1.000 usuários): Peso 5.

7.2.3. Cálculo do Montante Mensal: O total mensal de USAEs corresponderá à soma dos produtos entre a quantidade de ativos efetivamente suportados e seu respectivo peso de complexidade.

7.3. Atividades Incluídas no Suporte Técnico: O serviço compreende a execução das seguintes atividades técnicas, sem ônus adicional:

7.3.1. Diagnóstico e Troubleshooting: Realização de diagnósticos de falhas, identificação de erros de integração e resolução de problemas técnicos da plataforma.

7.3.2. Apoio à Parametrização: Auxílio técnico na configuração de novas políticas de varredura, criação de etiquetas (tags), ajustes de criticidade e definição de fluxos de automação.

7.3.3. Orientação Operacional: Fornecimento de diretrizes e melhores práticas para a utilização das ferramentas pelos analistas de segurança da CONTRATANTE.

7.3.4. Acompanhamento de Incidentes: Apoio direto à equipe de segurança no acompanhamento de vulnerabilidades críticas e incidentes detectados pela solução.

7.3.5. Apoio Técnico em Integrações: Suporte na manutenção de integrações via API com outras ferramentas (SIEM, EDR, ITSM).

7.3.6. Intermediação junto ao Fabricante: Quando necessário, especialmente em casos de falhas graves cuja resolução dependa de atuação do fabricante, a CONTRATADA deverá prestar o apoio necessário e intermediar o atendimento junto ao fabricante, acompanhando a tratativa até a apresentação de solução ou encaminhamento adequado.

7.4. Gestão e Atendimento dos Chamados

7.4.1. Canais de Atendimento: A CONTRATADA deverá disponibilizar meios eletrônicos e telefônicos para a abertura e o acompanhamento de chamados,

incluindo sistema de registro de chamados e atendimento telefônico por meio de número gratuito, preferencialmente 0800.

7.4.2. Registro do Chamado: Após a abertura do chamado, a CONTRATADA deverá disponibilizar à CONTRATANTE o respectivo número de identificação, permitindo o acompanhamento de sua tramitação.

7.4.3. Comunicação da Conclusão: Concluído o atendimento, a CONTRATADA deverá encaminhar relatório ou registro de conclusão aos endereços eletrônicos cadastrados pela CONTRATANTE, contendo, no mínimo, a descrição da demanda, as providências adotadas e a solução apresentada.

7.4.4. Encerramento do Chamado: Os chamados somente poderão ser encerrados após a apresentação da solução e a respectiva validação pela CONTRATANTE.

7.4.5. Vedação ao Encerramento Unilateral: É vedado o encerramento unilateral do chamado pela CONTRATADA sem a prévia autorização ou validação da CONTRATANTE, ressalvadas as hipóteses de impossibilidade de prosseguimento decorrentes exclusivamente de ação ou omissão da CONTRATANTE, devidamente registradas no atendimento.

7.5. Requisitos de Segurança e Gestão do Suporte

7.5.1. Autenticação e Acesso: Todo acesso de técnicos da CONTRATADA à plataforma deverá utilizar mecanismos de autenticação compatíveis com as políticas de segurança da CONTRATANTE, incluindo autenticação multifator (MFA), quando aplicável e disponibilizada pela solução.

7.5.2. Auditoria e Rastreabilidade: Todas as ações realizadas pela equipe de suporte na plataforma deverão ser passíveis de registro e rastreabilidade, permitindo, sempre que tecnicamente suportado pela solução, a identificação do responsável, da data e das alterações realizadas.

7.5.3. Segregação de Funções: O suporte deverá observar as políticas de segregação administrativa e os controles de acesso baseados em perfis (RBAC) definidos pela CONTRATANTE, limitando-se o acesso aos recursos estritamente necessários para a execução do atendimento.

7.5.4. Relatórios de Desempenho: A CONTRATADA deverá fornecer relatórios mensais contendo informações sobre o volume de ativos suportados, os atendimentos realizados e o cumprimento dos níveis de serviço (SLA), quando estabelecidos, para fins de acompanhamento, fiscalização, faturamento e eventual aplicação de glosas.

ANEXO II

PLANO DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL DE CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1. RECURSOS MATERIAIS E HUMANOS NECESSÁRIOS AO OBJETO CONTRATADO

1.1. Recursos Materiais

1.1.1. Recurso Material 1: A CONTRATANTE deverá provisionar em sua infraestrutura, máquinas virtuais (VMs) dedicadas para operar como *appliances* de *scanners* ou sensores da solução contratada, em conformidade com as especificações técnicas do fabricante. Estes recursos são essenciais para a realização de varreduras na rede interna do Tribunal e para a integração eficiente com a plataforma em nuvem da CONTRATADA.

1.2. Recursos Humanos (Equipe da CONTRATANTE)

1.2.1. Recurso humano 1:

1.2.1.1. Função: Integrante técnico

1.2.1.2. Responsável: Servidor(es) da Seção de Segurança da Informação Digital (SESEI)

1.2.1.3. Atribuições: Analisar e definir as especificações técnicas do

objeto/serviço a ser contratado; colaborar ativamente na elaboração dos artefatos de planejamento; avaliar as propostas das licitantes durante o processo licitatório; e viabilizar os acessos e meios necessários para a implantação e configuração dos serviços.

1.2.1.4. Quantidades/competências: 2 (dois) profissionais com expertise em segurança da informação e gestão de projetos de TI.

1.2.2. Recurso humano 2:

1.2.2.1. Função: Integrante demandante

1.2.2.2. Responsável: Servidor da Divisão de Tecnologia - DITEC.

1.2.2.3. Atribuições: Especificar detalhadamente os requisitos técnicos da solução; colaborar na elaboração dos artefatos do planejamento da contratação; acompanhar todas as fases do processo de contratação; avaliar as propostas das licitantes; e viabilizar os acessos e meios necessários para a implantação dos serviços.

1.2.2.4. Quantidades/competências: 1 (um) profissional com conhecimento aprofundado das necessidades de negócio e tecnológicas do Tribunal.

1.2.3. Recurso humano 3:

1.2.3.1. Função: Profissionais para Gerenciamento e Operação da Solução

1.2.3.2. Formação: Profissionais de Tecnologia da Informação com experiência comprovada em gestão de ferramentas de segurança cibernética.

1.2.3.3. Atribuições: Realizar o gerenciamento técnico e a operação diária da solução contratada, incluindo a configuração de políticas, execução de varreduras, análise preliminar de resultados e interação com a equipe de gestão de vulnerabilidades.

1.2.3.4. Quantidades/competências: 1 (um) profissional, com expectativa de ampliação conforme a complexidade e volume de atividades da solução.

1.2.4. Recurso humano 4:

1.2.4.1. Função: Equipe de Gestão do Processo de Vulnerabilidades

1.2.4.2. Formação: Servidores da Seção de Segurança da Informação Digital - SESEI e de outras áreas correlatas com conhecimentos em cibersegurança e análise de riscos.

1.2.4.3. Atribuições: Operar a plataforma SaaS para agendar e executar varreduras; analisar e interpretar os relatórios e *dashboards* gerados pela ferramenta, identificando e compreendendo os riscos; priorizar vulnerabilidades com base nos *scores* de risco da ferramenta e no contexto de negócio do Tribunal; coordenar o processo de remediação, interagindo com as equipes responsáveis pela correção (infraestrutura, desenvolvimento, etc.); acompanhar os Acordos de Nível de Serviço (SLAs) de correção e validar as mitigações aplicadas; e gerar relatórios gerenciais sobre a postura de segurança e a evolução do programa de gestão de vulnerabilidades.

1.2.4.4. Quantidades/competências: 2 (dois) profissionais com capacidade analítica e de coordenação, com foco em gestão de riscos cibernéticos.

2. CONTINUIDADE DO FORNECIMENTO DA SOLUÇÃO DE TI

2.1. Situação 1: Contratação de solução inadequada ou fornecedor que não atenda aos níveis mínimos de serviço.

2.1.1. Ação preventiva: Realizar levantamento exaustivo e detalhado dos requisitos de negócio e técnicos, assegurando sua clareza, objetividade e compatibilidade com as práticas de mercado e as necessidades do Tribunal.

2.1.1.1. Responsável: Equipe de Planejamento da Contratação, Gestor do Contrato e Fiscal do Contrato.

2.1.2. Ação de contingência: Formalizar a comprovação do não atendimento, por parte do fornecedor ou da solução, aos requisitos de habilitação ou às especificações técnicas, procedendo à aplicação das sanções contratuais cabíveis, conforme

legislação vigente.

2.1.2.1. Responsável: Equipe de Planejamento da Contratação, Gestor do Contrato e Fiscal do Contrato.

2.2. Situação 2: Insuficiência de experiência do fornecedor para a execução dos serviços contratados.

2.2.1. Ação preventiva: Exigir no edital atestado(s) de capacidade técnica que comprove(m) o bom desempenho da licitante em contratos anteriores de natureza e complexidade similares ao objeto.

2.2.1.1. Responsável: Equipe de Fiscalização do Contrato

2.2.2. Ação de contingência: Proceder à aplicação das penalidades contratuais previstas, observando os prazos e procedimentos legais.

2.2.2.1. Responsável: Gestor do Contrato e Unidade de Apoio à Contratação (DIACO).

3. ATIVIDADES DE TRANSIÇÃO CONTRATUAL E DE ENCERRAMENTO DO CONTRATO

3.1. **Ação de Encerramento:** Ao final do contrato, a CONTRATADA deverá fornecer todos os dados históricos de varreduras, ativos e vulnerabilidades pertencentes ao TRF1 em formato padrão e exportável (CSV, JSON ou similar).

3.2. **Ação de Transição:** A CONTRATADA deverá apoiar a equipe do Tribunal em um plano de transição para garantir a migração dos dados e a continuidade do processo de gestão de vulnerabilidades, caso uma nova solução seja contratada.

4. ESTRATÉGIA DE INDEPENDÊNCIA

4.1. **Transferência de conhecimento:** O conhecimento será transferido à equipe do TRF1 por meio do treinamento formal previsto no Anexo I e pelo suporte contínuo durante a vigência do contrato. O objetivo é capacitar a equipe interna a operar a ferramenta de forma autônoma, analisar os resultados e gerenciar todo o ciclo de vida das vulnerabilidades, garantindo a independência em relação à execução do processo.

4.2. Direitos de propriedade intelectual

4.2.1. Cláusulas (nos termos do artigo 93, da Lei n. 14.133/2021, concomitante com o art. 4º, da Lei n. 9.609/1998):

4.2.1.1. Toda documentação gerada na base de conhecimento será de uso exclusivo do CONTRATANTE, devendo ser mantida quando do encerramento do contrato. A transferência ou repasse para a própria contratada não alocada ou terceiros só será admitida após autorização do gestor do contrato.

4.2.1.2. Como documentação gerada, entende-se por quaisquer resultados de estudos, análises, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e qualquer outra documentação produzida no escopo da presente contratação, em papel ou em mídia eletrônica.

4.2.1.3. A CONTRATADA deverá ceder os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração.



Documento assinado eletronicamente por **Juarez de Oliveira, Analista Judiciário**, em 28/08/2026, às 16:45 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.trf1.jus.br/autenticidade> informando o código verificador **25792271** e o código CRC **4F5F8CAC**.

