



TRIBUNAL REGIONAL ELEITORAL DO PARA
Rua João Diogo 288 - Bairro Campina - CEP 66015-902 - Belém - PA
ESTUDOS TÉCNICOS PRELIMINARES
(ETP SERVIÇOS - TIC)

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (obrigatório)

Fundamentação: Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público (inciso I do § 1º do art. 18 da Lei 14.133/2021 e art. 11, inciso I da IN SGD/ME 94/2022).

1.1. Descrição da necessidade

O Plano Diretor de Tecnologia da Informação do TRE-PA possui como uma de suas principais iniciativas o PDTI 2025. A segurança cibernética é fundamental para garantir a integridade, confidencialidade e disponibilidade dos ativos de tecnologia da informação em qualquer organização. Com o aumento da conectividade e da digitalização dos serviços, a superfície de ataque se expande, elevando significativamente os riscos associados à segurança cibernética. Nesse contexto, a capacidade de gerenciar de forma contínua e centralizada as vulnerabilidades e os riscos associados é essencial para proteger os dados críticos e os ativos do Tribunal.

Nestes termos, tratam os autos da necessidade de avaliar a viabilidade técnica e econômica da contratação de empresa especializada para fornecimento de solução de cibersegurança.

Para tanto, este Estudo Técnico Preliminar (ETP) tem por objetivo fornecer o embasamento técnico para a seleção da solução mais adequada visando a contratação de solução para a gestão de vulnerabilidades e ativos. Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

- Padronização tecnológica na Administração Pública;
- Melhorar a continuidade na prestação dos serviços de TI do TRE-PA;
- Tornar os ambientes tecnológicos mais seguros e resiliente;
- Reduzir riscos de invasão, sequestro de dados, engenharias reversas, acessos não autorizados, exposição de dados;
- Fortalecimento da segurança da informação com análises contínuas de vulnerabilidades;
- Conformidade com regulamentações de segurança da informação;
- Redução de riscos operacionais com monitoramento e gerenciamento contínuo;
- Eficiência e otimização dos recursos de TIC atuais;
- Confiança e transparência institucional.

Neste contexto, listamos a seguir as principais demandas identificadas para a contratação atingir os objetivos propostos, que abrangem características do objeto:

DEMANDA 01: Consolidação e integração das soluções de segurança cibernética existentes: Integrar as ferramentas Tenable.sc+ e Tenable AD/Identity Exposure em uma plataforma unificada, proporcionando uma visão completa da superfície de ataque e uma gestão centralizada.

DEMANDA 02: Expansão da visibilidade e do gerenciamento de toda a superfície de ataque: Monitorar e gerenciar vulnerabilidades de forma contínua em ativos físicos, virtuais, identidades e ambientes em nuvem, identificando e priorizando riscos com base em seu impacto e probabilidade

DEMANDA 03: Redução de complexidade operacional e custos: Centralizar as operações de segurança em uma única plataforma SaaS, reduzindo custos operacionais e facilitando a automação de processos.

DEMANDA 04: Ampliação das capacidades de inteligência artificial: Utilizar recursos avançados de inteligência artificial e aprendizado de máquina para análise preditiva de ameaças, permitindo antecipar e mitigar riscos potenciais antes que se tornem incidentes de segurança.

DEMANDA 05: Conformidade com legislações e regulamentações vigentes: Garantir que a solução atenda aos requisitos da LGPD e da Instrução Normativa nº 5/2021, assegurando a proteção dos dados pessoais e o cumprimento das normas de segurança da informação.

DEMANDA 06: Melhoria na resposta a incidentes cibernéticos: Otimizar os processos de detecção, análise e resposta a incidentes, reduzindo o tempo de reação e minimizando impactos negativos nas operações do Tribunal.

Além da solução tecnológica, a contratação deverá incluir:

Suporte técnico: Assistência especializada para garantir o funcionamento adequado da plataforma.

Treinamento da equipe: Capacitação dos profissionais para a utilização eficiente da nova plataforma.

Consultoria especializada: Serviços para garantir a plena integração e utilização dos recursos da solução.

Com a implementação de uma plataforma integrada que atenda às demandas identificadas, o Tribunal espera alcançar um novo patamar de segurança cibernética, fortalecendo a proteção de seus ativos, otimizando processos e assegurando conformidade com as legislações vigentes. A integração e a centralização das ferramentas de segurança permitirão uma resposta mais ágil e eficaz às ameaças, contribuindo para a continuidade das operações e a confiança nos serviços prestados.

1.2. Motivação/justificativa

A Secretaria de Tecnologia da Informação do TRE-PA reconhece que a adoção de uma solução robusta para gerenciamento de exposição cibernética e ativos de segurança é uma medida essencial para proteger sua infraestrutura tecnológica, que lida com dados sensíveis e críticos. A estratégia envolve a implementação de sistemas de detecção, monitoramento e gestão contínua de vulnerabilidades em TIC, com o intuito de fortalecer a resiliência contra ameaças e otimizar o controle dos ativos em circulação.

Esse tipo de solução de segurança possibilita que o TRE-PA tenha um mapeamento detalhado dos dispositivos e sistemas conectados à rede, assim como um panorama atualizado sobre as vulnerabilidades que podem ameaçar a integridade das operações. Atualmente, o Tribunal opera com infraestrutura distribuída em diversas unidades, e a implantação dessa solução de segurança permitirá consolidar dados de ativos de TIC em uma plataforma unificada, otimizando a gestão e a resposta a incidentes. Dessa forma, a contratação do gerenciamento de vulnerabilidades e ativos vem para garantir que o TRE-PA tenha uma visão clara e abrangente do estado de segurança de sua rede, permitindo um monitoramento proativo.

O investimento em ferramentas de gerenciamento de vulnerabilidades e ativos atende ao modelo de compliance com normas de segurança e boas práticas recomendadas. Esta abordagem se alinha aos requisitos estabelecidos na Lei Geral de Proteção de Dados (LGPD) e normas específicas do setor público, que exigem controle rigoroso sobre o ciclo de vida dos ativos e a mitigação de riscos operacionais. A manutenção de uma infraestrutura segura, em conformidade com padrões legais, assegura que as atividades do Tribunal possam ser realizadas com confiança e transparência.

Ao adotar uma solução completa de gestão de vulnerabilidades e ativos, o TRE-PA busca otimizar sua eficiência operacional, priorizando vulnerabilidades com base em criticidade e reduzindo o tempo de resposta a incidentes. A priorização automatizada, fornecida pela solução, garante que a equipe de TI se concentre nos riscos mais significativos, gerando um ambiente de segurança mais dinâmico e alinhado aos objetivos estratégicos da instituição.

Essencialmente, essas ferramentas operam por meio de uma varredura de vulnerabilidades em sistemas, redes e dispositivos conectados. Esse processo permite que as

equipes de segurança detectem possíveis falhas que possam ser exploradas por agentes mal-intencionados.

A detecção ocorre em tempo real, oferecendo informações detalhadas e precisas sobre cada vulnerabilidade identificada. Ao fornecer relatórios abrangentes, essas ferramentas tornam-se um recurso indispensável para a análise e a mitigação proativa de riscos, ajudando a proteger a integridade dos sistemas.

Outro ponto central nas soluções de gerenciamento de vulnerabilidades é a gestão de ativos. Essas ferramentas mapeiam continuamente os ativos conectados a uma rede, criando uma lista precisa e em tempo real de todos os dispositivos presentes. Essa capacidade de monitorar e identificar todos os componentes de uma infraestrutura permite às equipes de segurança identificar dispositivos não autorizados ou que estejam configurados incorretamente, oferecendo uma visão completa da rede e eliminando potenciais pontos de fraqueza.

As soluções para gerenciamento de vulnerabilidades também são essenciais para garantir conformidade com regulamentações e padrões de segurança. Além de detectar vulnerabilidades, essas ferramentas oferecem análises que ajudam as organizações a manterem-se alinhadas a normas como PCI-DSS, HIPAA e outras diretrizes de segurança. Isso é particularmente relevante para setores que lidam com dados sensíveis, pois o descumprimento dessas normas pode gerar sérias consequências legais e financeiras.

Esse tipo de solução deve atender aos requisitos estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e pela Instrução Normativa nº 5/2021, que regulamenta o uso de computação em nuvem na administração pública federal. Conforme essa normativa, os dados, metadados e informações transferidos para o provedor de nuvem devem estar hospedados em território brasileiro, com a exigência de que pelo menos uma cópia de segurança seja mantida no Brasil. Além disso, o provedor de serviço de nuvem deve garantir confidencialidade, exclusividade sobre as informações tratadas e conformidade com a legislação brasileira de segurança da informação, assegurando que o Ponto de Presença (PoP) e o datacenter da solução estejam no país. Esses requisitos asseguram a proteção dos dados pessoais e a observância ao direito ao esquecimento, conforme o art. 16 da LGPD.

Uma característica importante dessas soluções é o monitoramento contínuo. Em vez de realizar apenas varreduras periódicas, as ferramentas de monitoramento contínuo permitem que a segurança da rede seja avaliada em tempo real. Esse tipo de monitoramento possibilita uma resposta rápida e eficaz a novas ameaças e reduz significativamente o tempo necessário para identificar e corrigir vulnerabilidades críticas, o que fortalece a segurança da infraestrutura digital.

Outra funcionalidade valiosa oferecida por essas ferramentas é a priorização e geração de relatórios. As soluções de gerenciamento de vulnerabilidades fornecem relatórios detalhados, com insights sobre as vulnerabilidades mais críticas e as áreas que exigem atenção imediata. Com a capacidade de priorizar as vulnerabilidades mais impactantes, a equipe de segurança pode direcionar os recursos para as questões mais urgentes, otimizando o processo de mitigação e fortalecendo a proteção da rede.

As soluções de gerenciamento de vulnerabilidades desempenham um papel fundamental na proteção das redes e sistemas corporativos. Elas garantem que as organizações possam monitorar e gerenciar continuamente seus ativos, identificar vulnerabilidades em tempo real, manter-se em conformidade com regulamentações de segurança e priorizar ações corretivas. Essas funcionalidades tornam essas ferramentas indispensáveis para empresas que buscam proteger seus dados e garantir a continuidade e a integridade de suas operações digitais.

O aumento significativo de ataques cibernéticos, aliado à expansão das superfícies de ataque decorrente da digitalização dos serviços, exige uma gestão contínua e proativa das vulnerabilidades e ameaças que impactam diretamente as infraestruturas críticas de Tecnologia da Informação e Comunicação (TIC). Dados recentes do CTIR Gov indicam que o número de incidentes cibernéticos notificados ultrapassou 15.000 em 2023.

Conforme o Manual de Referência – Proteção de Infraestruturas Críticas de TIC da Estratégia Nacional de Segurança Cibernética (ENSEC-PJ), estabelecido pela Resolução nº 396 de 07/06/2021, é essencial adotar medidas que garantam a resiliência e proteção das infraestruturas tecnológicas do Poder Judiciário. Isso inclui o uso de ferramentas automatizadas para a detecção e priorização de vulnerabilidades, a aplicação ágil de atualizações de segurança e a correlação contínua de informações para mitigar riscos de forma eficiente.

Neste contexto, a referida contratação está alinhada ao:

- 1) Planejamento Estratégico 2021-2026 do TRE-PA (PEJEP), com relação ao Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados - Índice de cumprimento de requisitos de Proteção de Dados (Mede o percentual de cumprimento da implantação dos requisitos relacionados à Proteção e Segurança de Dados).
- 2) Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD), com relação ao Objetivo 7 - Aprimorar a Segurança da Informação e a Gestão de Dados, da [Resolução Nº 370 de 28/01/2021](#).
- 3) Plano Diretor de Tecnologia da Informação (PDTIC) 2025-2026 TRE-A: SOC 24/7

Em consonância com essas diretrizes, a Gartner, em seu relatório de tendências de cibersegurança para 2024, identifica o Gerenciamento Contínuo da Exposição Cibernética (CTEM) como uma estratégia fundamental para enfrentar o crescimento exponencial das superfícies de ataque. O CTEM, ao utilizar frameworks como o MITRE ATT&CK, permite uma correlação inteligente e proativa das ameaças, possibilitando a antecipação de riscos e a mitigação eficaz de ataques.

Atualmente, o Tribunal utiliza duas soluções independentes do mesmo fabricante: Tenable.sc+ / Tenable.IO WAS (CONTRATO Nº 49 / 2021) e Tenable AD/Identity Exposure (CONTRATO Nº 207 / 2022), ambas provenientes de processos de ATA/SRP nº 101/2020 TRE-PB e nº 68/2022 TRE-PB. Essas ferramentas são voltadas para a gestão de vulnerabilidades de rede e proteção de identidades, respectivamente. Contudo, elas não possuem integração nativa nem via terceiros, resultando em uma gestão de segurança fragmentada que dificulta a obtenção de uma visão unificada e centralizada da superfície de ataque. Essa fragmentação impacta negativamente a eficiência operacional e a capacidade de resposta a ameaças cibernéticas.

A necessidade de centralizar e integrar as operações de segurança cibernética é premente, visando eliminar a fragmentação atual e proporcionar uma visão unificada da superfície de ataque. A plataforma integrada oferecida pela Tenable, que inclui os módulos já adquiridos e outros que contemplam o gerenciamento contínuo da exposição cibernética, apresenta-se como uma solução alinhada a essa necessidade.

A adoção de uma plataforma integrada permitirá:

- Centralização e integração das operações de segurança cibernética: Eliminando a fragmentação entre as soluções atuais, proporcionando uma visão unificada e abrangente da superfície de ataque.
- Automatização da detecção e correção de vulnerabilidades: Em conformidade com o manual da ENSEC-PJ, possibilitando uma gestão contínua e baseada em risco, com aplicação ágil de atualizações de segurança.
- Ampliação da visibilidade e capacidade de resposta: Utilizando tecnologias de inteligência artificial para correlacionar vulnerabilidades e ameaças de forma contextualizada e precisa.
- Conformidade regulatória: Atendendo às exigências da LGPD e da Instrução Normativa nº 5/2021, com a hospedagem de dados e cópias de segurança em datacenters localizados no Brasil.

A plataforma integrada não apenas oferece uma abordagem robusta e unificada de Gerenciamento Contínuo da Exposição Cibernética (CTEM), mas também está alinhada aos princípios estabelecidos pelo ANEXO IV do Manual de Proteção de Infraestruturas Críticas de TIC, promovendo a resiliência cibernética e a proteção contínua das infraestruturas essenciais do Tribunal.

Necessidade Primária e Alinhamento com Soluções Disponíveis

A necessidade primária é, portanto, ampliar o nível de gerenciamento da exposição cibernética e integrar as soluções existentes para garantir um monitoramento contínuo e eficiente. Essa necessidade está alinhada com as soluções oferecidas pela Tenable, que dispõe de uma plataforma integrada capaz de unificar os módulos já adquiridos e em operação (Tenable.sc+ e Tenable AD/Identity Exposure) e adicionar outros componentes que contemplam o gerenciamento de exposição cibernética. A plataforma Tenable One, por exemplo, permitiria a consolidação das ferramentas atuais em uma única solução integrada, proporcionando maior visibilidade, gestão centralizada e redução de custos operacionais, além de ampliar as capacidades de inteligência artificial para análise avançada de ameaças e otimização da resposta a incidentes cibernéticos.

Benefícios da Integração e do Correlacionamento de Informações

A adoção de uma plataforma integrada como a Tenable One traria diversos benefícios ao Tribunal:

- Consolidação e integração das soluções de segurança cibernética existentes: A plataforma permitiria a integração das funcionalidades de monitoramento e mitigação em uma única solução, eliminando a necessidade de gerenciar múltiplas ferramentas isoladas. Isso resultaria em redução de complexidade e

melhoria da eficiência da equipe de segurança.

- Expansão da visibilidade e do gerenciamento de toda a superfície de ataque: Com cobertura ampliada, a plataforma abrange ativos físicos, virtuais, identidades e ambientes em nuvem. Isso possibilita o monitoramento e gerenciamento contínuo de vulnerabilidades, identificando e priorizando riscos com base em seu impacto real.
- Correlacionamento nativo de informações: A integração das informações entre vulnerabilidades de rede e identidades permite uma análise mais precisa dos riscos, facilitando a detecção e mitigação de ameaças de maneira mais rápida e eficaz.
- Integração com frameworks reconhecidos: A plataforma integra-se com frameworks amplamente aceitos, como o MITRE ATT&CK, proporcionando uma análise detalhada das ameaças baseada em evidências e comportamentos conhecidos de agentes maliciosos.
- Redução de complexidade operacional e custos: A migração para um modelo SaaS evita custos adicionais com aquisição e manutenção de múltiplas soluções on-premise. A centralização das operações de segurança em uma única plataforma facilita a automação de processos, como a análise e a correção de vulnerabilidades, otimizando o uso dos recursos de TI.

Riscos da não contratação

- Aumento da exposição a ameaças cibernéticas decorrente de recursos desatualizados;
- Incapacidade de detecção de novas vulnerabilidades devido à falta de escopo abrangente nas ferramentas;
- Risco de não conformidade com regulamentações de segurança e proteção de dados, como a LGPD;
- Perda de visibilidade e controle sobre ativos de TIC em uso na rede;
- Elevação do tempo de resposta a incidentes de segurança pela falta de ferramentas eficazes;
- Maior suscetibilidade a ataques de phishing e ransomware sem análise constante de vulnerabilidades;
- Risco de vazamento de dados sensíveis por brechas não monitoradas adequadamente;
- Possibilidade de interrupções nos serviços críticos devido à falta de gestão de riscos de segurança;
- Aumento de custos futuros com reparações e contenção de incidentes cibernéticos;
- Impacto na confiança e credibilidade institucional devido à falta de segurança nas operações de TIC.

Objetivos e Resultados Esperados

O principal objetivo é aprimorar o gerenciamento contínuo da exposição cibernética, integrando as soluções existentes em uma plataforma unificada que possibilite uma visão ampliada da superfície de ataque e o correlacionamento das informações em tempo real. Com isso, o Tribunal terá uma capacidade significativamente aumentada de:

- Detectar e mitigar ameaças de maneira mais rápida e eficaz, com base em dados correlacionados e análise preditiva.
- Reduzir a complexidade operacional, com uma plataforma centralizada que permite o gerenciamento automatizado e a análise contínua de vulnerabilidades.
- Aumentar a visibilidade e priorizar ameaças com base em frameworks como o MITRE ATT&CK, que fornecem evidências detalhadas e práticas recomendadas para mitigação de ataques
- Fortalecer a postura de segurança por meio da atualização tecnológica das ferramentas de gestão de vulnerabilidades, permitindo acompanhar as tendências em cibersegurança e reduzir a exposição a ameaças emergentes;
- Garantir conformidade contínua com normas e regulamentações de segurança, como a LGPD, identificando e tratando vulnerabilidades que possam comprometer dados pessoais e assegurando requisitos de conformidade;
- Implementar um monitoramento mais abrangente e em tempo real dos ativos de TIC, obtendo visibilidade constante sobre todos os ativos e evitando pontos de entrada para ameaças;
- Reduzir os riscos de interrupções nos serviços essenciais do Tribunal, promovendo a continuidade das operações e minimizando o impacto de incidentes de segurança em serviços críticos;
- Otimizar os recursos da equipe de segurança de TI, automatizando atividades manuais e permitindo que a equipe foque em atividades de maior impacto estratégico;
- Desenvolver capacidades preditivas para antecipar e neutralizar possíveis ameaças, identificando padrões e agindo preventivamente para proteger a infraestrutura;
- Aumentar a confiabilidade dos serviços de TIC oferecidos aos usuários internos e externos, elevando o nível de segurança das operações e assegurando um ambiente digital confiável para todos os usuários.

O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

- [PORTARIA Nº 23423/2024](#) (evento SEI 0002542876)
- Processo SEI Nº 0002591-55.2024.6.14.8000, Anexo V evento 0002538480
- ITEM 5 do ANEXO V: *Contratação de solução de gestão contínua de vulnerabilidades e auditoria de configurações de ativos de rede.*

1.3. Identificação das necessidades não tecnológicas ou de negócio

NECESSIDADES DE NEGÓCIO			
ID		Requisitos	Justificativa
1	Continuidade Operacional e Modernização Como ocorrerem grandes mudanças na solução Tenable tanto em funcionalidades como nos tipos de licenciamentos, a contratação deve prever, para os Tribunais que tem ainda licenças válidas, a opção de fazer o upgrade para as novas licenças e funcionalidades.	• Renovação das licenças Tenable.SC e opção de migração para o Tenable.IO e Tenable One.	Permitir a continuidade das operações para os Tribunais que dependem das soluções atuais, ao mesmo tempo que se oferece a possibilidade de migração para soluções mais completas e flexíveis.
2	Apoio Operacional Especializado Considerar a inclusão de item de serviço continuado de Operação Assistida	• Inclusão de item de serviço continuado para Operação Assistida.	A operação assistida assegura o uso correto das ferramentas adquiridas, bem como a capacitação contínua das equipes de TI, maximizando os benefícios da solução contratada.

3	Melhoria na Governança de Segurança Cibernética Necessidade de fortalecer a governança com uma visão unificada da segurança.	- Integração de todas as funcionalidades de segurança em uma única plataforma. - Ferramentas para acompanhamento centralizado das políticas de segurança.	Uma governança robusta exige controle e visibilidade centralizados para facilitar a tomada de decisões estratégicas. Uma plataforma integrada permite uma visão consolidada, essencial para gerenciar ameaças com precisão e cooperação.
4	Aprimoramento do Gerenciamento de Riscos Necessidade de identificar e priorizar vulnerabilidades com precisão para uma resposta alinhada aos objetivos do órgão.	- Expansão da cobertura para monitorar redes, dispositivos e identidades. - Ferramentas de priorização de riscos com base em impacto real.	Uma cobertura abrangente facilita o monitoramento contínuo de ativos críticos, alinhando o gerenciamento de riscos aos interesses institucionais e garantindo proteção eficaz.
5	Otimização de Recursos Necessidade de redução de custos com soluções locais e otimização dos recursos de TI disponíveis.	- Migração para um modelo SaaS para segurança. - Redução de custos com manutenção e aquisição de múltiplas soluções.	A centralização e o modelo SaaS reduzem custos e aumentam a eficiência dos recursos, maximizando o retorno do investimento em segurança e garantindo proteção proativa.
6	Conformidade com Normas e Regulamentações Necessidade de atender a padrões e regulamentos de segurança cibernética com agilidade e precisão.	- Integração com estruturas de segurança reconhecidas. - Monitoramento contínuo da conformidade regulatória.	O uso de frameworks padronizados, como o MITRE ATT&CK, garante o cumprimento das normas e facilita auditorias, promovendo uma segurança que atende aos requisitos legais e regulatórios.
7	Facilidade de Auditoria e Transparência Necessidade de manter registros claros e rastreáveis para facilitar auditorias de segurança.	- Centralização de logs e relatórios de segurança. - Funcionalidades de auditoria acessíveis e planejadas.	Uma plataforma única com transparência nos processos de segurança fornece auditorias facilitadas e documentadas, essenciais para o controle e a confiabilidade institucional.
8	Escalabilidade e Flexibilidade Necessidade de aumentar ou diminuir recursos de segurança de TI conforme a demanda e o risco.	- Capacidade de ajustar o monitoramento de ameaças em tempo real. - Suporte para diferentes superfícies de ataque (redes, dispositivos, identidades).	O ambiente de TI do Tribunal precisa de flexibilidade para escalar o monitoramento da segurança conforme novos riscos surgem. A solução de gerenciamento de vulnerabilidades deve oferecer escalabilidade dinâmica, otimizando o uso dos recursos e garantindo uma gestão proativa da superfície de ataque.
9	Redução de Custos Operacionais Necessidade de diminuir os gastos com a gestão de múltiplas soluções de segurança.	- Modelo de pagamento conforme o uso (SaaS). - Redução de custos com infraestrutura on-premise e atualizações manuais.	A solução de gerenciamento de vulnerabilidades deve permitir centralizar várias funcionalidades de segurança cibernética em uma única plataforma, reduzindo a necessidade de manter várias soluções independentes e os custos associados à sua manutenção. Isso otimiza os recursos e aumenta a eficiência operacional.
10	Melhoria na Segurança e Conformidade Necessidade de garantir a conformidade com regulamentos, como LGPD, e aumentar a segurança cibernética.	- Implementação de medidas robustas de segurança, como correlação de dados de ameaças e detecção baseada em risco. - Conformidade com regulamentos de proteção de dados.	A solução de gerenciamento de vulnerabilidades deve fortalecer as práticas de segurança do Tribunal, ao fornecer um Gerenciamento Contínuo da Exposição Cibernética (CTEM). Além disso, a conformidade com normas como a LGPD é garantida por meio da localização de dados no Brasil e o cumprimento de exigências legais.
11	Eficiência Operacional e Automação Necessidade de automatizar processos de detecção e mitigação de vulnerabilidades, reduzindo o tempo de resposta a incidentes.	- Ferramentas de automação para varredura contínua e correção de vulnerabilidades. - Capacidade de resposta rápida e automatizada a incidentes.	A solução de gerenciamento de vulnerabilidades deve fornecer automação das operações de segurança cibernética, permitindo uma resposta imediata a ameaças, reduzindo o tempo de exposição e a carga manual da equipe de TI.
12	Mitigação de Riscos e Gestão Proativa Necessidade de reduzir o risco de ataques cibernéticos de forma contínua, antecipando ameaças e priorizando vulnerabilidades.	- Implementação de inteligência artificial e análise baseada em riscos. - Priorização das correções de vulnerabilidades mais críticas.	A solução de gerenciamento de vulnerabilidades deve utilizar inteligência artificial e frameworks como o MITRE ATT&CK para priorizar as vulnerabilidades com maior risco de exploração, promovendo uma gestão proativa de ameaças.
13	Transparência e Relatórios de Compliance Necessidade de garantir relatórios claros e auditáveis para atender às auditorias internas e externas de conformidade e segurança.	- Ferramentas de relatórios automatizados e personalizáveis. - Geração de evidências para auditorias em conformidade com normas como a LGPD.	A solução de gerenciamento de vulnerabilidades deve permitir a geração de relatórios detalhados e transparência no gerenciamento de vulnerabilidades, facilitando auditorias de conformidade e garantindo que a segurança esteja sempre documentada.

1.4. Identificação das necessidades tecnológicas

NECESSIDADES TECNOLÓGICAS		
ID	Requisitos	Justificativa

1	Monitoramento Contínuo de Vulnerabilidades. Necessidade de monitorar continuamente a superfície de ataque.	- Ferramentas de monitoramento contínuo para detecção de vulnerabilidades em tempo real. - Automação de varreduras de segurança.	O monitoramento contínuo é essencial para identificar e corrigir vulnerabilidades à medida que surgem, minimizando o impacto de ameaças cibernéticas.
2	Automação de Mitigação de Ameaças Necessidade de automatizar a correção de vulnerabilidades e resposta a incidentes.	- Ferramentas de automação para correção imediata de vulnerabilidades. - Implementação de inteligência artificial para análise automatizada.	A automação da mitigação de ameaças reduz o tempo de resposta e libera a equipe de TI para se concentrar em tarefas mais estratégicas.
3	Integração e Orquestração de Dados de Segurança Necessidade de consolidar e correlacionar dados de segurança para uma visão unificada.	- Suporte a integração de dados com frameworks como MITRE ATT&CK. - Orquestração de informações de múltiplas ferramentas de segurança.	A integração de dados de segurança oferece uma visão unificada e holística dos riscos, permitindo uma resposta proativa a ameaças.
4	Visualização Centralizada de Riscos Necessidade de uma interface unificada para visualizar e gerenciar todos os riscos cibernéticos.	- Painel centralizado de riscos cibernéticos. - Ferramentas de análise de risco baseadas em inteligência artificial.	A visualização centralizada de riscos permite que as equipes de segurança tomem decisões mais rápidas e precisas com base em uma visão unificada de todos os ativos e vulnerabilidades. Isso facilita a priorização de ações corretivas e o acompanhamento em tempo real dos riscos emergentes.
5	Conformidade e Auditoria Contínua Necessidade de monitorar continuamente a conformidade com normas como LGPD, PCI-DSS, entre outras.	- Ferramentas automatizadas para monitoramento de conformidade. - Relatórios automáticos de auditoria e conformidade.	A conformidade contínua garante que o Tribunal esteja sempre em conformidade com regulamentos, evitando multas e garantindo a segurança e privacidade de dados sensíveis. A plataforma permite monitoramento automatizado de conformidade e a geração de relatórios para auditorias de forma contínua e sem esforço manual.
6	Análise de Caminhos de Ataque Necessidade de identificar e correlacionar técnicas adversárias para antecipar e mitigar possíveis vetores de ataque.	- Integração com o MITRE ATT&CK Framework para análise de caminhos de ataque. - Ferramentas de visualização de caminhos de ataque e interação com dados de ameaças para explorar origens e destinos. - Automação da detecção de vetores de ataque e recomendações para mitigação com base em análises gráficas avançadas. - Capacidade de ingestão de dados de vulnerabilidades e identidades, incluindo auditoria de credenciais e análise de senhas.	A Análise de Caminhos de Ataque permite que o Tribunal visualize e interaja diretamente com as técnicas utilizadas por adversários, utilizando o MITRE ATT&CK Framework para mapear possíveis vetores de ataque. Ao correlacionar dados de vulnerabilidades com as técnicas usadas em ataques reais, o Tribunal pode identificar fraquezas críticas e mitigar ameaças antes que elas sejam exploradas. A capacidade de automatizar essa análise em tempo real oferece uma vantagem significativa na defesa contra ameaças avançadas e persistentes.
7	Gestão de Exposição e Comunicação de Riscos Cibernéticos Necessidade de visualizar e comunicar claramente os riscos de exposição cibernética para otimizar a segurança e alinhar a estratégia de negócios.	- Ferramentas de visualização abrangente de ativos e vulnerabilidades, tanto on-premises quanto na nuvem. - Priorização de esforços de mitigação de ameaças com base em inteligência artificial e dados de vulnerabilidade contextualizados. - Relatórios e KPIs para comunicação clara de riscos cibernéticos para executivos, gestores e equipes de segurança. - Integração com fontes de dados externas para aprimorar a análise e a remediação de vulnerabilidades.	A Gestão de Exposição e Comunicação de Riscos Cibernéticos permite que o Tribunal tenha uma visão completa de seus ativos e vulnerabilidades, tanto em ambientes locais quanto na nuvem, e priorize os esforços de mitigação de acordo com as ameaças mais prováveis. Além disso, a capacidade de comunicar riscos de forma clara e objetiva, utilizando KPIs e benchmarks, garante que os líderes executivos possam tomar decisões informadas e estratégicas. A solução também oferece uma visão holística da maturidade da remediação e dos riscos, alinhando a segurança cibernética às metas de negócios.
8	Resiliência Cibernética Necessidade de fortalecer a capacidade do Tribunal de resistir, adaptar-se e recuperar-se de incidentes cibernéticos com o mínimo de interrupção nas operações.	- Ferramentas de monitoramento contínuo e detecção precoce de ameaças. - Soluções para resposta rápida e mitigação de impactos.	A resiliência cibernética é fundamental para garantir a continuidade dos serviços institucionais e proteger as infraestruturas críticas contra interrupções. Uma plataforma robusta e integrada fortalece a defesa proativa, permitindo ao Tribunal manter operações seguras e minimizar os danos em caso de incidentes.

1.5. Análise da contratação anterior ou a série histórica, se houver.

1.5.1. Com relação à contratação anterior, destaca-se o CONTRATO Nº 49 / 2021 (evento 1373848 - Processo SEI 0001993-09.2021.6.14.8000), com a fornecedora ADISTEC BRASIL INFORMÁTICA LTDA, proveniente da Ata de Registro de Preços nº 101/2020 – TRE-PB, que teve como objeto a aquisição de licenciamento de softwares relacionados à solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web. Essa solução engloba a aquisição de softwares e suporte técnico. Os seguintes softwares foram fornecidos na contratação, são baseados em licenças perpétuas (*on premise*):

- Tenable.io Web Application Scanning
- Standard Tenable.sc Continuous View - Perpetual

Cumprido salientar que a Ata de Registro de Preços nº 101/2020 – TRE-PB foi resultante do Pregão Eletrônico nº 37/2020 do Tribunal Regional Eleitoral da Paraíba (TRE-PB). A licitação foi dividida em dois lotes, cada um com especificações técnicas específicas, conforme os grupos a seguir:

- Lote 01 (G1): Solução com armazenamento e gerenciamento em Nuvem (*On Cloud*), fabricante vencedor QUALIS
- Lote 02 (G2): Solução com armazenamento e gerenciamento local (*On Premise*), fabricante vencedor TENABLE.

Além do TRE-PB, os seguintes Tribunais Regionais Eleitorais figuraram como participantes do SRP: Amazonas, Piauí, Ceará, Rio Grande do Norte, Alagoas, Minas Gerais, Espírito Santo, Mato Grosso do Sul e Rio Grande do Sul. O TRE-PB atuou como órgão gerenciador da Ata de Registro de Preços. O edital também previu a possibilidade de adesão de outros órgãos da administração pública federal que não tenham participado inicialmente do processo licitatório. Deste modo o CONTRATO Nº 49 / 2021 resultou da adesão à Ata de Registro de Preços nº 101/2020 – TRE-PB.

Da mesma forma, este ETP deve tratar da contratação com indicação de marca para o fabricante Tenable, uma vez que trata-se de contratação complementar para solução de segurança da informação existente nos TRES.

- Lote 01 (G1): Solução com armazenamento e gerenciamento local (On Premise), renovação de licenciamento.
- Lote 02 (G2): Solução com armazenamento e gerenciamento em Nuvem (SaaS), renovação de licenciamento e contratação de novas licenças.

2. REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

Fundamentação: descrição dos requisitos da contratação contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição (inciso III do § 1º do art. 18 da Lei 14.133/2021 e art. 11, inciso I da IN 94/2022).

2.1. Natureza do objeto

- 2.1.1. O objeto da contratação é caracterizado como comum, nos termos do art. 6º, inciso XIII, da Lei 14.133/2021, por possuir especificações usuais do mercado, que permitem a fixação de padrões de qualidade e de desempenho para o referido serviço. Nesse sentido, dispõe o art. 5º da Portaria SGD/MGI nº 5.950/2023.
- 2.1.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507/2018, da Resolução TSE nº 23.702/2022 e da IN SEGES nº 5/2017, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.
- 2.1.3. Dessa forma, a classificação apresentada se adequa perfeitamente ao objeto em questão, levando em consideração sua natureza explicitamente definida neste ETP, bem como os padrões de desempenho estabelecidos nos Níveis Mínimos de Serviços.
- 2.1.4. Neste sentido, a solução apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.2. Necessidade continuada da solução

- 2.2.1. O objeto é de natureza continuada.
- 2.2.2. O presente Estudo Técnico Preliminar (ETP) visa a contratação de serviços contínuos e especializados para gestão da exposição cibernética, por meio de uma plataforma integrada de segurança cibernética. Tais serviços caracterizam-se pela natureza continuada, sendo imprescindíveis para garantir uma proteção consistente e abrangente à infraestrutura digital do Tribunal. A proposta de solução permite visibilidade extensiva e centralizada sobre as vulnerabilidades de segurança, abrangendo todas as superfícies de ataque, o que contribui para uma resposta ágil e eficaz na mitigação de riscos cibernéticos.
- 2.2.3. A adoção de uma plataforma integrada não apenas facilita a detecção e correção contínua de ameaças, mas também é essencial para preservar a integridade e a disponibilidade de dados e sistemas institucionais, promovendo a continuidade operacional e o alinhamento com os requisitos de conformidade e governança de TI. Em virtude da criticidade da segurança cibernética e da complexidade do cenário digital contemporâneo, a necessidade continuada dessa solução se revela estratégica, garantindo a permanência e a estabilidade das ações preventivas e corretivas indispensáveis à defesa dos ativos digitais do Tribunal.

2.2.1. Vigência plurianual

(X) SIM, conforme justificativa abaixo. () NÃO

I - Vantagens de Ordem Econômica e Orçamentária:

- Economia de Escala e Redução de Custos: Contratos de longa duração para soluções de tecnologia (especialmente no modelo SaaS - *Software as a Service*) costumam ter um custo anualizado inferior ao de renovações anuais. Fornecedores oferecem descontos substanciais para garantir a fidelidade contratual, resultando em economia direta de recursos públicos ao longo do período.
- Previsibilidade Orçamentária e Proteção Cambial: A fixação de um valor por 60 (sessenta) meses assegura a previsibilidade orçamentária para a Secretaria de Tecnologia da Informação, blindando o Tribunal contra a volatilidade cambial (dado que muitas licenças de software são cotadas em dólar) e reajustes anuais acima da inflação, garantindo a estabilidade para o planejamento financeiro do órgão.
- Racionalidade Administrativa: A celebração de um único processo licitatório para um período de 5 anos mitiga os custos e o esforço administrativo (mobilização da equipe de planejamento, setor de licitações, assessoria jurídica) inerentes à condução de certames anuais ou bienais para o mesmo objeto. Isso otimiza a força de trabalho para se dedicar a outras contratações estratégicas.

II - Vantagens de Ordem Técnico-Operacional:

- Continuidade e Estabilidade do Serviço: A segurança cibernética é uma atividade de natureza eminentemente contínua. A interrupção do serviço de monitoramento de vulnerabilidades, mesmo que por curtos períodos durante processos de transição contratual, representaria uma exposição inaceitável dos ativos digitais do TRE-PA. Uma vigência de 60 meses garante a continuidade e a estabilidade da proteção.
- Amortização do Investimento em Implantação e Curva de Aprendizagem: A contratação envolve custos iniciais não apenas financeiros, mas também de tempo e esforço para implantação, configuração e treinamento da equipe técnica. Um prazo de vigência estendido permite que este investimento inicial seja plenamente amortizado e que a equipe atinja a maturidade operacional na ferramenta, extraindo seu máximo potencial e otimizando os processos de gestão de segurança.
- Natureza do Objeto: O objeto contratado, uma plataforma de gerenciamento de exposição cibernética, é um serviço contínuo que evolui com o cenário de ameaças. A relação de longo prazo com o fornecedor facilita o planejamento de atualizações e a adaptação da solução às novas necessidades do Tribunal, fomentando uma parceria estratégica para a segurança da informação.

2.2.1.1. Desta forma, a vigência plurianual de 60 meses se demonstra a opção mais vantajosa para a Administração Pública, conciliando a necessidade de uma proteção cibernética ininterrupta e eficaz com os princípios da economicidade e da eficiência.

2.3. Adoção do Sistema de Registro de Preços – SRP ?

(X) Sim () Não

Vide tópico 10 deste ETP.

2.3.1. Foi realizada consulta às IRPs em andamento.

(X) Sim () Não

Destaca-se que, nas consultas realizadas ao SIASGnet e ao PNCP, não foram encontradas IRPs abertas de objeto semelhante (gestão de vulnerabilidades) para participação, provavelmente em razão das especificidades do objeto.

SIASGnet IRP - Google Chrome

Não seguro <https://www2.comprasnet.gov.br/siasgnet-irp/consultarServicoInteresseSubmit.do?method=consultarLista>

Ambiente: **PRODUÇÃO** Consultar Serviço Interesse 11/08/2025 11:57:28

Critério de Consulta

☒ do Serviço ☐ do Grupo

Consulta por Descrição

Busca por Radicais

☒ Contendo a(s) Palavra(s) ☐ Iniciando com a Palavra

Pesquisar Fechar

Não foi encontrado serviço de interesse com o parâmetro informado

Seleção SESP

2.3.2. Haverá órgãos participantes deste Registro de Preços? Justificar.

(X) Sim () Não

Justificativa:

2.3.2.1. A contratação conjunta, por meio de Instrumento de Registro de Preços (IRP), visa atender às exigências da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Tal estratégia enfatiza a necessidade de soluções robustas e integradas de gestão de vulnerabilidades para garantir um nível uniforme de proteção em todas as unidades participantes através de soluções padronizadas.

2.3.2.2. Além disso, a aquisição conjunta possibilita economia de escala, padronização de processos e otimização de recursos tecnológicos e financeiros, alinhando-se aos princípios da eficiência e da economicidade previstos na legislação vigente. A solução Tenable, objeto da contratação, é essencial para o monitoramento contínuo, identificação e mitigação de vulnerabilidades em ativos críticos, contribuindo diretamente para o fortalecimento da segurança cibernética no âmbito do Poder Judiciário.

2.3.2.3. A adoção do Instrumento de Registro de Preços também se fundamenta no disposto no art. 12, § 1º, da Resolução CNJ nº 468/2022, que incentiva a adoção de contratações centralizadas e compartilhadas entre os órgãos do Poder Judiciário. Essa diretriz visa promover maior eficiência administrativa, garantir a uniformização das soluções de segurança cibernética e assegurar a mitigação de riscos em toda a infraestrutura tecnológica dos órgãos participantes.

2.3.2.4. O quadro a seguir sintetiza as principais vantagens relacionadas:

Vantagem	Justificativa
Economia de Escala	O IRP possibilita a ampliação do volume total contratado ao consolidar a demanda de diferentes órgãos, gerando economia de escala. Com isso, há potencial para negociar preços mais vantajosos e condições mais detalhadas, convenientes os custos unitários dos bens ou serviços adquiridos.
Racionalização dos Recursos Públicos	O registro de preços permite otimizar a utilização dos recursos públicos, uma vez que a Administração adquira apenas o necessário e no momento certo, evitando o desperdício e a obsolescência de itens estocados. O IRP é uma ferramenta eficaz para planejar e distribuir as demandas de acordo com as necessidades reais dos participantes.
Flexibilidade e Adequação às Necessidades dos Entes	A utilização do IRP oferece gratuitamente para que os entes manifestem interesse em aderir ao processo, de acordo com suas necessidades específicas e capacidade orçamentária. Isso facilita a aquisição das aquisições à realidade de cada participante, sem obrigação de aquisição imediata.
Simplificação e Redução de Esforços na Gestão de Contratações	Ao centralizar o processo de licitação em um único registro de preços, o IRP reduz a necessidade de múltiplas licitações para itens da mesma natureza, dificultando o volume de processos licitatórios e, consequentemente, o tempo e o esforço despendidos pela Administração.
Possibilidade de Inclusão de Entes Interessados em Etapas Finais	A abertura do IRP permite que, até a fase externa, outros entes manifestem interesse em participar do edital. Isso amplia a base de contratação e aumenta a eficiência da aquisição, permitindo que todos se beneficiem do conjunto do processo.

2.3.3. Será realizado procedimento público de intenção de registro de preços - IRP?

(X) Sim () Não (Justificar)

Justificativa:

2.3.3.1. A publicação do Procedimento Público de Intenção de Registro de Preços (IRP) será realizada entre os Tribunais Regionais Eleitorais que atendam aos requisitos da contratação, especificamente relacionados à renovação/upgrade, bem como nova contratação de licenciamento da solução de gestão de vulnerabilidades Tenable.

2.3.3.2. Essa abordagem permite o atendimento coordenado às demandas de segurança cibernética no âmbito da Justiça Eleitoral, promovendo a uniformização das ferramentas utilizadas e a conformidade com as diretrizes estabelecidas pela Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

2.3.3.3. Além disso, a adoção do IRP favorece a economia de escala, a otimização de recursos financeiros e administrativos e a maior celeridade nos processos de aquisição. Também contribui para a transparência e a competitividade, alinhando-se aos princípios da eficiência e da economicidade previstos na legislação.

2.3.4. Será estabelecido (se for o caso) o número máximo de participantes, em conformidade com a capacidade de gerenciamento do órgão? Justificar.

(X) Sim () Não (Justificar)

2.3.4.1. Conforme mencionado no tópico anterior, a publicação do Procedimento Público de Intenção de Registro de Preços (IRP) será limitado aos Tribunais Regionais Eleitorais que atendam aos requisitos da contratação. A quantidade relacionada à contratação será obtida mediante consulta prévia aos Tribunais.

2.3.5. Será admitida a adesão à ata de registro de preços por órgão não participante? Justificar.

(X) Sim () Não

2.3.5.1. Será admitida adesão à Ata de Registro de Preços apenas aos Tribunais Regionais Eleitorais não participantes, obedecido o regramento do item anterior.

2.3.6. Havendo possibilidade de adesão, há previsão de quantitativos máximos para adesão e dos respectivos quantitativos? (art. 32 do Decreto nº 11.462/23)

(☒) Sim (☐) Não (☐) Não se aplica

2.3.6.1. As adesões autorizadas apenas para os Regionais Eleitorais não participantes deverão observar ainda os limites de quantitativo por órgão (50%) e total (200%) previstos no art. 32 do Decreto nº 11.462/23.

2.4. Admissão ou não de subcontratação do objeto contratual

(☐) SIM (☒) NÃO

2.4.1. Não será admitida a subcontratação para a contratação.

2.5. Exigência de amostra/prova de conceito

(☐) SIM (☒) NÃO

2.5.1. Não haverá necessidade de apresentação de amostra/prova de conceito.

2.6. Garantia, manutenção e assistência técnica

2.6.1. O prazo de garantia deverá ter, no mínimo, a mesma duração do contrato a ser implementado pela CONTRATANTE, contados da data do aceite definitivo emitido pela CONTRATANTE.

2.6.2. Durante o período de garantia, a CONTRATADA será obrigada a reparar, corrigir ou substituir, às suas expensas, no total ou em parte, o objeto da contratação em que se verificarem vícios, defeitos ou incorreções, salvo se por culpa da CONTRATANTE o objeto venha a perecer ou por fatores alheios a vontade da CONTRATADA.

2.6.2.1. A CONTRATADA deverá fornecer suporte oficial e direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante, se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto.

2.6.2.2. Deverá ser garantido ao CONTRATANTE pleno acesso ao site do FABRICANTE, além de acesso irrestrito a console de gerenciamento da solução em nuvem, devendo ser possível delegar a função de abertura de chamados com o FABRICANTE para a CONTRATADA, assim como delegar os acessos necessários para a execução dos serviços de suporte diretamente pela equipe da CONTRATADA.

2.6.3. A CONTRATADA deverá proceder à substituição ou correção no prazo máximo de **10 (dez) dias** corridos, contados do recebimento da notificação respectiva, que poderá ser enviada por e-mail.

2.6.4. Todas as despesas necessárias para efetivar a substituição ou correção das soluções durante a garantia ficarão a cargo da CONTRATADA.

2.6.5. A prestação dos serviços de garantia, assistência técnica e suporte, excetuadas as manutenções programadas, será por solicitação, ou seja, a CONTRATADA receberá da CONTRATANTE solicitação para o fornecimento de suporte técnico, conforme SLA e severidades especificadas.

2.6.6. A CONTRATADA deverá disponibilizar o acesso à Central de Atendimento através de plataforma online, e-mail, número de telefone local ou DDG (número 0800), para abertura de chamados de suporte técnico, conforme períodos, horários e condições estabelecidas no Termo de Referência.

2.6.7. A abertura de chamados através do “Help Desk” deverá gerar um número de protocolo para que a CONTRATANTE possa ter registro documental de abertura da ocorrência e realizar o acompanhamento e controle dos prazos para atendimento.

2.6.8. Para os Serviço de Suporte Técnico, a CONTRATANTE poderá abrir número ilimitado de chamados durante a vigência do contrato, sem qualquer ônus adicional.

2.6.9. O horário de atendimento do Serviço de Suporte Técnico deverá ser de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias ao ano e prestados em Português do Brasil.

2.6.10. O prazo de resposta aos chamados abertos será de, no máximo, 02 (duas) horas, independente da criticidade.

2.7. Garantia de execução contratual

(☒) SIM (☐) NÃO

2.7.1. Será exigida a garantia contratual da execução, nos termos do art. 96 da Lei 14.133/2021, no percentual de 5% do valor contratado e de acordo com a condições devidamente especificada no Termo de Referência, tendo em vista o valor estimado da contratação ser de monta considerável, bem como aos riscos inerentes à solução contratada para o Tribunal, conforme estabelecido no mapa de gerenciamento de risco.

2.8. Requisitos de capacitação

(☒) SIM (☐) NÃO (☐) NÃO SE APLICA

2.8.1. Haverá a necessidade de treinamento definida em cada Lote ou Grupo do objeto.

2.8.2. O serviço de treinamento é considerado necessário à plena execução do objeto a ser contratado, promovendo o desenvolvimento dos servidores do Tribunal diretamente envolvidos no processo de gestão de vulnerabilidades, objetivando ainda a utilização plena de todos os recursos da solução, sem que ocorra lacunas de conhecimento. O treinamento deverá ofertar vagas para **até 10 participantes**, podendo ser realizado de forma oficial pelo fabricante, com carga horária mínima de 20 (vinte) horas, com fornecimento de materiais didáticos oficiais, podendo ocorrer na modalidade EAD.

2.8.3. Caso o treinamento não seja possível no modo EAD, todos os custos para a realização do treinamento, a ser realizado na sede da contratante, ficará a cargo da CONTRATADA.

2.8.4. O Termo de referência especificará com maiores detalhes os requisitos de capacitação.

2.9. Requisitos legais

O processo de contratação deve estar aderente à seguinte legislação, sem prejuízo de outras normas aplicáveis:

- Lei nº 14.133, de 1º de abril de 2021, Nova Lei de Licitações e Contratos, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, Estados, Distrito Federal e Municípios.
- Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
- LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018).
- Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor)
- Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Portaria SGD/MGI nº 852, de 28 de maio de 2023, que dispõe o Programa de Privacidade e Segurança da Informação.
- Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
- Norma Complementar nº 14/IN01/DSIC/SCS/GSIPR, Estabelece os princípios, diretrizes e responsabilidades relacionados à segurança da informação para o

tratamento da informação em ambiente de computação na nuvem.

- Resolução CNJ nº 468 de 15/07/2022, 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 (CNJ).
- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Decreto 11.462, de 31 de março de 2023, Dispõe sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.
- Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
- Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Resolução TSE nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
- Resolução TSE nº 23.702, de 9 de junho de 2022, Dispõe sobre a Política de Governança das contratações na Justiça Eleitoral e dá outras providências.
- Resolução CNJ nº 400, de 16 de junho de 2021, que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.
- ABNT NBR ISO/IEC 27017 de 07/2016. Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem.
- PORTARIA CNJ Nº 140 DE 22 DE ABRIL DE 2024. Determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.
- DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018 - Institui a Política Nacional de Segurança da Informação - PNSI, dispõe sobre a governança da segurança da informação, no âmbito da administração pública federal.

Normas específicas do Tribunal:

- PORTARIA Nº 22808, de 25 de janeiro de 2024. Institui norma de gerenciamento contínuo de vulnerabilidades no âmbito do TRE-PA.
- PORTARIA Nº 22811, de 25 de janeiro de 2024. Dispõe sobre as regras e os procedimentos para gestão de riscos de segurança da informação do Tribunal Regional Eleitoral do Pará.
- Portaria Nº 23242/2024, dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito do Tribunal Regional Eleitoral do Pará.
- Resolução TRE-PA Nº 5.734 - Implementou, no âmbito do Tribunal Regional Eleitoral do Pará, a Resolução TSE nº 23.644/2021, que estabelece a Política de Segurança da Informação da Justiça Eleitoral.
- Resolução Nº 5699, de 11 de novembro de 2021. Institui a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPD) no âmbito do TRE-PA.

2.10. Requisitos temporais

- 2.10.1. A contratada deverá fornecer o objeto contratado em até 10 (dez) dias úteis, contados a partir da confirmação do recebimento da Ordem de Serviços ou outro instrumento hábil, prorrogável por mais 10 dias mediante formalização de justificativa plausível e aprovação da Diretoria Geral, após análise e parecer jurídico.
- 2.10.2. O cronograma de implementação, instalação e capacitação da solução será apresentado, conforme o estipulado no Termo de Referência e deverá obedecer ao prazo máximo de 60 (sessenta) dias para a instalação e configuração completa da solução de TIC contratada, de modo a conferir o seu pleno funcionamento.
- 2.10.3. O período de garantia e suporte técnico será contado a partir do início da implementação e/ou instalação, e deverá permanecer durante toda a vigência do futuro contrato.
- 2.10.4. Quando da ocorrência de quaisquer falhas de funcionamento, será aberto um chamado técnico para solução do incidente. O atendimento a este chamado poderá ocorrer inicialmente por telefone ou acesso remoto e deverá estar disponível durante toda a vigência contratual. Os prazos de cada tipo de chamado serão definidos no termo de referência.
- 2.10.5. A contagem dos prazos referente a entrega de produtos e início dos serviços será em dias úteis, conforme período consignado em cada etapa.
- 2.10.6. Os serviços contratados deverão ser executados pela CONTRATADA em regime 24x7, 365 dias por ano.
- 2.10.7. O prazo de vigência da contratação será de **60 (sessenta) meses** para os itens relacionados à Contratação da Plataforma de Gerenciamento de Exposição, contados da assinatura do termo de contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.11 Requisitos de Segurança da informação e Privacidade

- 2.11.1. O Termo de Referência deve conter, no que couber ao objeto contratado, requisitos e obrigações de privacidade e segurança da informação, devendo o órgão ou entidade empregar, conforme critérios próprios, aqueles requisitos que forem imprescindíveis, considerando a legislação vigente e os riscos de privacidade e segurança da informação.
- 2.11.2. A solução deverá estar alinhada, na medida do possível, com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), em especial, aos princípios de segurança (Art. 6º, inciso VII) e prevenção (Art. 6º, inciso VIII).
- 2.11.3. A CONTRATADA deverá assegurar que possui total conhecimento da Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) e que em toda sua prestação de serviço respeitará o regramento nela preconizado, especialmente quando algum preposto eventualmente tiver acesso a informações que contenham dados pessoais.
- 2.11.4. A solução deverá estar alinhada à Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- 2.11.5. Conforme definido na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, para as contratações de serviços em nuvem (IaaS, PaaS e SaaS) devem ser observados, no mínimo, os requisitos de privacidade e segurança da informação, além daqueles constantes nos templates de artefatos da contratação disponibilizados pela SGD em parceria com a AGU:
 - a contratação deve estar alinhada às normas correlatas publicadas pelo Gabinete de Segurança Institucional da Presidência da República- GSI/PR, a exemplo da IN GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
 - a solução deve estar em conformidade com a Política de Segurança da Informação da Justiça Eleitoral.
 - todas as informações consideradas sensíveis pelo TRE-PA deverão ser resguardadas por parte da CONTRATANTE não sendo permitido, em hipótese alguma, o compartilhamento, cópia, retirada, reprodução, carga, levantamento, entre outros, de informações oriundas dos usuários da solução ou de sistemas informatizados institucionais sem a devida autorização prévia e expressa por parte da autoridade competente do TRE-PA.
 - a CONTRATADA deverá assinar Termo de Compromisso de Manutenção de Sigilo e os respectivos funcionários alocados ao contrato deverão assinar Termo de Ciência, cujo prazo de entrega ao CONTRATANTE será de 5 (cinco) dias úteis após a assinatura do CONTRATO.
 - a CONTRATADA deverá apresentar, na reunião inicial, relação nominal dos profissionais envolvidos na execução do contrato que terão acesso às informações do CONTRATANTE, se for o caso, bem como os referidos Termos de Ciência assinados. Caberá ao preposto alocado ao contrato manter esta lista atualizada sempre que um novo profissional necessitar de acesso às informações tratadas.

- cumprir a Política de Segurança da Informação da CONTRATANTE (Política de Segurança da Informação da Justiça Eleitoral - Resolução N° 23.644), assim como a Resolução TRE -PA n.º 5.699/2021 que institui a Política de Privacidade e Proteção de Dados.
- não veicular publicidade acerca dos serviços contratados, sem prévia e formal autorização por parte da CONTRATANTE.
- comunicar formal e imediatamente à CONTRATANTE qualquer ponto de fragilidade percebido que exponha a confidencialidade, integridade ou disponibilidade das informações e do serviço CONTRATADO.
- cada provedor de nuvem deve possuir, no mínimo, dois data centers em território brasileiro, capaz de ofertar serviços padronizados e altamente automatizados, nos quais os recursos de infraestrutura (por exemplo, computação, rede e armazenamento) são complementados por serviços de plataforma integrados, e deve cumprir os requisitos de segurança da informação estabelecidos nos artigos 20 e 25 da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;
- os dados tratados em ambiente de nuvem devem ser armazenados em data centers localizados em território brasileiro, admitindo-se o tratamento de dados em data centers fora do território brasileiro somente nos casos em que haja cópia de segurança atualizada armazenada em data centers localizados em território brasileiro.
- deve-se exigir, mediante justificativa prévia, que os provedores de serviços em nuvem possuam, no momento da assinatura do contrato, as seguintes certificações de normas de segurança da informação aplicáveis ao objeto da contratação:
 - ISO 27001;
 - ISO 27017;
 - ISO 27018;
 - ISO 27701;
 - AICPA SOC1;
 - AICPA SOC2;
 - HIPAA COMPLIANT;
- devem ser predefinidos canais para comunicação - de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais - de eventos de segurança da informação;
- deve-se prever cópia dos logs fornecidos, de acordo com a política de retenção do cliente;
- a CONTRATADA deve garantir controles eficazes e compatíveis com as políticas e procedimentos do CONTRATANTE para gerenciamento de identidades de usuários e controle de acessos;
- devem ser estabelecidas políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pelo cliente e pelo provedor;
- os dados armazenados no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado ao nível de sigilo das informações e as chaves criptográficas não devem ser armazenadas na nuvem;
- devem ser estabelecidos os limites do acesso do provedor aos dados do cliente e a responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes;
- devem ser definidos os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, e o provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato;
- a utilização de termo de confidencialidade, que deverá conter cláusula que impeça o integrador ou provedor de serviço de nuvem de usar, transferir, e liberar dados, sistemas, processos e informações do órgão ou da entidade para terceiros, como empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros, além de incluir a proibição do uso de informações do órgão ou da entidade para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado;
- o ambiente de nuvem deverá possuir padrão de controle que protege a confidencialidade e privacidade de informações armazenadas e processadas na nuvem através do SOC – Service Organization Controls.
- Tanto a futura CONTRATADA quanto seus funcionários e colaboradores, deverão se submeter às diretrizes, padrões e requisitos de segurança da informação em uso ou futuramente adotados pelo Tribunal;

2.12. Requisitos sociais, ambientais e culturais

- 2.12.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PTBR e fornecidos em meio digital.
- 2.12.2. O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.
- 2.12.3. Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.
- 2.12.4. Os funcionários e colaboradores deverão se comportar de forma educada e respeitosa, quando estiver no ambiente do Tribunal ou em qualquer tipo de contato a ser realizado;
- 2.12.5. No que se refere aos aspectos culturais e sociais, os funcionários e colaboradores deverão atender somente demandas relacionadas com o objeto a ser contratado;
- 2.12.6. Toda e qualquer comunicação deverá ser realizada ou redigida em língua portuguesa, escrita e falada no Brasil, em conformidade com as normas técnicas e jurídicas aplicáveis;
- 2.12.7. Os profissionais designados para prestar serviços no ambiente do Tribunal deverão apresentar-se devidamente identificados e trajados de forma condizente com o ambiente de trabalho, de modo a resguardar a imagem institucional e evitar o uso de vestuário que possa comprometer a seriedade e a formalidade da instituição;

2.13. Critérios e práticas de sustentabilidade

- 2.13.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam, especialmente, na Lei nº 12.305, de 2010, no Decreto nº 7.746, de 5 de junho de 2012, na Resolução CNJ nº 594/2024, no Plano de Logística Sustentável do TRE/PA e no Guia Nacional de Contratações Sustentáveis da Advocacia-Geral da União:
 - a) recolhimento adequado de todos os consumíveis utilizados, bem como pelos resíduos gerados nos processos de manutenção e limpeza dos locais onde os serviços forem prestados, assegurando que esses resíduos sejam tratados de forma ambientalmente correta, conforme as normas vigentes;
 - b) Todos os componentes da solução ofertada deverão possuir funcionalidades que contribuam para a economia de energia elétrica, como o modo de economia de energia ou outras tecnologias sustentáveis, visando a redução do impacto ambiental das operações do Tribunal.

2.14. Requisitos da Arquitetura Tecnológica

- 2.14.1. A solução deverá observar integralmente os requisitos de arquitetura tecnológica descritos a seguir, considerando todo o ciclo de vida da solução de gestão de vulnerabilidades e o aprimoramento contínuo da gestão da exposição cibernética (CTEM), garantindo uma operação segura, eficiente e escalável.
- 2.14.2. A CONTRATADA deverá, periodicamente, identificar oportunidades de melhoria na arquitetura tecnológica utilizada para o pleno funcionamento da solução de gestão de vulnerabilidades, visando a otimização de performance, segurança cibernética e mitigação de vulnerabilidades, com foco na adaptação às ameaças emergentes e nas melhores práticas do setor.
- 2.14.3. A arquitetura da Solução de Segurança Cibernética objeto deste Estudo deverá observar, no mínimo, os seguintes princípios de excelência em segurança e operação:

- Permitir o uso de operações automatizadas e como código (Operations as Code): Ser capaz de automatizar operações de segurança, incluindo correções de vulnerabilidades e gerenciamento da exposição, permitindo a integração com ferramentas de automação e orquestração.
- Documentação e auditoria baseada em eventos: Utilizar anotações e registros detalhados em tempo real para a criação de documentação auditável e rastreável, possibilitando uma análise contínua de vulnerabilidades e riscos.
- Permitir mudanças constantes e ajustes frequentes: A arquitetura deve possibilitar que componentes da solução de gestão de vulnerabilidades e suas integrações com outras ferramentas sejam atualizados constantemente para refletir as necessidades dinâmicas de segurança e a mitigação de novas ameaças cibernéticas.
- Prever simulação e antecipação de cenários de ataques: ser capaz de realizar simulações de vetores de ataque e cenários de falhas utilizando ferramentas como o Attack Path Analysis, com foco na antecipação de ameaças, execução de testes e validação de requisitos de segurança antes da implementação em produção.

2.14.4. A arquitetura empregada na solução de gestão de vulnerabilidades e suas integrações deve:

- Ser precedida de planejamento: Toda alteração ou implementação na arquitetura da solução deverá ser precedida de um planejamento robusto, levando em consideração as melhores práticas de segurança e conformidade.
- Gerenciamento de capacidade de vulnerabilidades e exposição: A solução deve prever a capacidade de escalar o monitoramento de vulnerabilidades e gestão da exposição, evitando limitações inesperadas, e permitindo uma adaptação eficiente à expansão da superfície de ataque.
- Monitoramento e controle de gastos relacionados à gestão de riscos e ameaças: A solução deverá incluir mecanismos de alerta e controle de custos relacionados ao consumo de recursos de segurança, como varreduras de vulnerabilidades, detecção de ameaças e correções automatizadas.

2.14.5. Segurança como prioridade central: A arquitetura deverá ser projetada com padrões mínimos de segurança cibernética que incluam, mas não se limitem a:

- Controle de acesso robusto para assegurar que apenas usuários autorizados possam interagir com a plataforma e realizar ações de alto impacto.
- Mecanismos de log e monitoramento contínuo, para garantir que todas as ações e eventos sejam devidamente rastreados e auditáveis.
- Gestão segura de credenciais, assegurando a proteção de identidades e senhas, alinhada às melhores práticas recomendadas para a segurança de informações.
- Segmentação de rede e proteção de ativos críticos, prevenindo movimentos laterais de atacantes e minimizando a exposição de sistemas críticos.
- Adaptação às melhores práticas e recomendações de segurança cibernética: A arquitetura deve estar alinhada às recomendações de frameworks de segurança amplamente aceitos, como o MITRE ATT&CK, permitindo a correlação de técnicas adversárias e ações rápidas de mitigação de riscos.

2.15. Requisitos de Projeto e Implementação

2.15.1.A solução deverá observar integralmente os requisitos de Projeto e Implementação descritos a seguir e na solução como um todo, considerando todo o ciclo de vida do objeto e especificação dos produtos.

- A reunião inicial deverá ocorrer em até 10 (dez) dias úteis após a assinatura do contrato.
- É de total responsabilidade da empresa contratada a aquisição de informações, gerenciamento do projeto e garantia dos prazos contratados, cumprindo ao Fiscal do Contrato prover as informações necessárias à sua compleição.
- Além disso, os Serviços de Computação em nuvem (quaisquer itens), objeto da contratação, deverão ser executados observando um projeto definido pela CONTRATADA e aprovado pelo CONTRATANTE com:
- Arquitetura da solução prevista em nuvem, detalhando a infraestrutura, componentes e a interconexão entre eles.
- Deve atender requisitos de segurança da informação, abordando aspectos como controle de acesso, criptografia de dados, conformidade com regulamentações (como LGPD) e auditorias de segurança.
- As integrações e os desenvolvimentos de soluções de interoperabilidade, sempre que possível, serão pautados em plataformas livres, na arquitetura de micros serviços, utilizando modelos e frameworks disponibilizados no Portal do Software Público Brasileiro.
- As prospecções tecnológicas deverão evitar propostas que dependam exclusivamente de plataformas proprietárias e que dependam de único fornecedor, exceto quando autorizado pelo CONTRATANTE. Propostas devem preferencialmente adotar tecnologias abertas e compatíveis com padrões amplamente aceitos no mercado.

2.16. Requisitos de implantação

2.16.1. A solução contratada deverá observar integralmente os requisitos de Implantação da solução como um todo e no termo de sustentação do contrato, considerando todo o ciclo de vida do objeto e logística de implantação da solução.

2.16.2. Para a implantação da solução a CONTRATADA deverá fornecer dentro dos prazos estabelecidos no contrato a entrega das licenças, bem como a disponibilização dos acessos necessários para o gerenciamento das licenças fornecidas.

2.16.3. A CONTRATADA deverá adotar mecanismos de automação e de implantação contínua.

2.16.4. Deverão ser adotadas práticas ágeis pela CONTRATADA na operação, implantação e automação de processos e cargas de trabalho no ambiente.

2.16.5. A implantação de toda a solução somente será considerada finalizada após efetuados todos os testes operacionais pós-implantação, atestada pela Fiscal do Contrato e formalizada por meio do Termo de Recebimento Provisório - TRP.

2.17. Requisitos de experiência profissional

2.17.1. Os serviços relacionados ao objeto da contratação deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos mesmos.

2.17.1.1. A comprovação que trata este item deve ocorrer mediante apresentação de profissional especializado da CONTRATADA, que possua pelo menos uma das seguintes certificações:

- CISSP
- CISM
- CIA
- GSEC
- GCIH
- GMON
- Tenable.io Specialist
- Tenable.io Expert

2.18. Requisitos de formação da equipe

2.18.1. No âmbito da solução Tenable One, o planejamento e a implementação dos serviços de gestão de exposição cibernética (CTEM) deverão ser supervisionados por um especialista em gestão de vulnerabilidades e por um especialista em segurança cibernética da CONTRATADA, com experiência comprovada no uso do MITRE ATT&CK Framework e análise de superfícies de ataque.

2.18.2. No âmbito dos serviços de gestão de vulnerabilidades e análise de exposição, o provisionamento, configuração, monitoramento e correção de vulnerabilidades deverão ser operacionalizados por um administrador de segurança cibernética, com competências específicas na administração de ferramentas de segurança integradas, como o Tenable Vulnerability Management/Sc+ e Tenable Identity Exposure.

2.18.3. No âmbito dos serviços de gerenciamento de exposição e resposta a incidentes, as atividades deverão ser realizadas por ao menos um administrador de segurança cibernética, com a supervisão de um especialista em arquitetura de segurança e um especialista em gestão de riscos e vulnerabilidades, garantindo que todas as operações estejam alinhadas com as melhores práticas de mitigação e remediação de ameaças.

2.18.4. No âmbito dos serviços de treinamento, as atividades deverão ser executadas por ao menos um instrutor especializado em segurança cibernética, com experiência comprovada na formação de analistas de segurança, administradores e gestores, com foco na operação e utilização da plataforma Tenable One para gerenciamento de vulnerabilidades, análise de riscos e exposição, e resposta a incidentes.

2.19. Requisitos de metodologia de trabalho

2.19.1. A execução do objeto seguirá a seguinte dinâmica/etapas.

CONTRATAÇÃO DE SERVIÇOS CONTÍNUOS E ESPECIALIZADOS PARA GESTÃO DA EXPOSIÇÃO CIBERNÉTICA, POR MEIO DE PLATAFORMA INTEGRADA DE SEGURANÇA CIBERNÉTICA			
ETAPA	DESCRIÇÃO	PRODUTOS FINAIS A SEREM ENTREGUES	PRAZO MÁXIMO DA ENTREGA
1	FORNECIMENTO DO LICENCIAMENTO RELACIONADO À RENOVACÃO DO LICENCIAMENTO (GRUPO 1) OU SUBSCRIÇÃO DO SOFTWARE (GRUPO 2).	LICENÇA/SUBSCRIÇÃO DE SOFTWARE	15 (quinze) dias corridos, contados do recebimento da Ordem de Fornecimento.
2	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DO AMBIENTE ATUAL. (GRUPO 2)	AMBIENTE IMPLANTADO E CONFIGURADO	30 (trinta) dias corridos, contados do recebimento da Ordem de Fornecimento.
3	TREINAMENTO DA SOLUÇÃO CONTRATADA PARA ATÉ 10 PESSOAS, COM NO MÍNIMO 24 HORAS DE DURAÇÃO. (GRUPO 1 e GRUPO 2)	SERVIÇO / TREINAMENTO	30 (trinta) dias corridos, contados do recebimento da Ordem de Fornecimento.
4	SERVIÇO DE SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA, PELO PERÍODO DE 60 (SESENTA) MESES. (GRUPO 2)	SERVIÇO / APOIO OPERACIONAL	30 (trinta) dias corridos, contados do recebimento da Ordem de Fornecimento.

Do Encaminhamento Formal de Demandas

- 1) O gestor do contrato emitirá a Ordem de fornecimento de bens e serviços para a entrega dos bens desejados, conforme ANEXO III AO TERMO DE REFERÊNCIA.
- 2) O Contratado deverá fornecer os itens com as mesmas configurações e quantidades definidas na Ordem de Fornecimento.
- 3) O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.

Dos prazos

- 1) A contagem dos prazos da tabela "Dinâmica de execução do contrato" será em dias corridos, conforme indicação em cada etapa.
- 2) A contagem dos prazos de entrega pelo contratado será iniciada na data de confirmação do recebimento da ordem de fornecimento correspondente à entrega.

Mecanismos formais de comunicação

A comunicação entre a CONTRATANTE e a CONTRATADA se dará, preferencialmente, por meio escrito, sempre que se entender necessário o registro de ocorrência relacionada com a execução do contrato. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

- 1) *Ordem de Fornecimento de Bens e Serviços;*
- 2) *Ata de Reunião;*
- 3) *Ofício(s);*
- 4) *Sistema de abertura de chamados da CONTRATADA;*
- 5) *E-mails e Notificações Administrativas;*

Dinâmica de execução do contrato

- 1) Os serviços contratados deverão ser executados pela CONTRATADA em dias úteis e em horários de expediente regulares, entre às 08:00 e 12:00h e 13:00 e 17:00 horas. Em caso em que haja algum impedimento para a execução normal dos serviços ou que possam comprometer o funcionamento das unidades administrativas, a fiscalização poderá determinar a CONTRATADA à execução em horários alheios ao expediente, em feriados ou finais de semana, sem qualquer ônus extras ao Contratante.
- 2) Estão previstas reuniões durante a execução dos serviços dos Itens 4, 5 e 6, distribuídas assim: i) reunião inicial; ii) reunião para apresentar o anteprojeto das soluções; iii) reunião para apresentar o projeto básico; e iv) reunião para apresentar o orçamento.
- 3) Reuniões de *kick off* poderão ser exigidas pela Fiscalização, sem ônus algum para o CONTRATANTE.

Local e horário da prestação dos serviços

- 1) As licenças do software relacionados ao contratado, bem como suas chaves de ativação, devem ser disponibilizadas em até 15 (quinze) dias corridos após a emissão da Ordem de Fornecimento (OF)
- 2) Os serviços de garantia, manutenção, suporte e assistência técnica serão prestados no horário de 08:00hs às 17:00hs.
- 3) A demanda de serviços será encaminhada à CONTRATADA por meio de documentos oficiais de comunicação definidos neste Instrumento.
- 4) Fica a critério do CONTRATANTE, definir o horário de instalação e configuração da solução, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, se for o caso.
- 5) Atividades associadas à implantação com a necessidade eventual de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE.

2.20. Da participação de consórcios

2.20.1. Não será permitida a participação de empresas em consórcio, uma vez que o objeto consiste no fornecimento de solução de TIC cuja logística não se apresenta como complexa para fornecimento, ou seja, uma única licitante detém em seu portfólio de serviço condições de atender as demandas previstas, sem a necessidade de se consorciar com outra empresa para conseguir atender o objeto na sua completude. Desse modo, não há situação fática que comprove a necessidade da previsão do uso do instituto do consórcio no presente processo.

2.21. Da participação de pessoa física

2.21.1. Não será permitida a participação de pessoas físicas, pois a presente contratação exige estrutura mínima da contratada, com equipamentos, instalações e equipe

2.22. Da participação de cooperativas

2.22.1. Não será permitida a participação de cooperativas, tendo em vista que os serviços de suporte técnico previstos na garantia das licenças, bem como os serviços de operação assistida, presumem subordinação e exigem especialização técnica específica, o que incompatibiliza a natureza cooperativista, conforme preconiza a Lei nº 14.133, de 1º de abril de 2021, que rege as licitações e contratos no âmbito público brasileiro.

2.23. Indicação de marcas ou modelos

2.23.1. O projeto trata de uma expansão integrada com as soluções já em utilização no TRE-PA e outros Tribunais que demonstraram interesse na participação para contratação eventual e futura.

2.23.2. A indicação de marca neste projeto é justificada pela necessidade de continuidade e integração plena com as soluções já existentes, garantindo uma operação consistente e a interoperabilidade essencial entre ferramentas de segurança de alta complexidade, a saber, auxílio no processo de gestão de vulnerabilidades. A escolha de marcas já utilizadas pelo órgão permite que os sistemas atuais e futuros operem em sintonia, sem a introdução de incompatibilidades que poderiam prejudicar o desempenho e a segurança da infraestrutura de TI.

2.23.3. Além disso, o uso das soluções Tenable.SC e Tenable.Io WAS é motivado por sua ampla adoção por outros Tribunais Eleitorais que, em consultas prévias, demonstraram interesse na renovação dessas tecnologias. Essa escolha estratégica visa atender às demandas dos eventuais partícipes e maximizar os benefícios obtidos por meio de uma solução já consolidada no âmbito do Judiciário Eleitoral.

2.23.4. O uso dessas marcas facilita a manutenção e o suporte técnico, pois permite ao órgão contar com especialistas que dominam todas as nuances e características dos produtos do fabricante indicado. Essa expertise é particularmente valiosa em ambientes de segurança cibernética, onde a rapidez e precisão no atendimento técnico são fundamentais para proteger os dados institucionais e evitar interrupções nas operações críticas.

2.23.5. Outro motivo para a indicação de marca é a possibilidade de gerenciamento centralizado e integrado entre as ferramentas. A combinação das plataformas Tenable One, Tenable.SC e Tenable.Io WAS oferece uma visão consolidada e abrangente da infraestrutura de segurança, permitindo a administração eficiente e otimizando os esforços das equipes de TI.

2.23.6. A continuidade dessas marcas específicas também fortalece a segurança cibernética do órgão, já que o fabricante oferece soluções integradas e compatíveis entre si. Isso reduz as chances de brechas e vulnerabilidades ao expandir a infraestrutura tecnológica, promovendo uma defesa mais robusta contra ataques e ameaças.

2.23.7. A Administração também observou o princípio da padronização, considerando as ferramentas de segurança cibernética já adotadas e integradas à infraestrutura atual. O uso das soluções Tenable One, Tenable.SC e Tenable.Io WAS garante coerência, eficiência e compatibilidade total com as operações e necessidades de segurança vigentes, minimizando impactos operacionais e otimizando as defesas cibernéticas.

2.23.8. Assim, para a presente contratação, serão adotadas as soluções Tenable One, Tenable.SC e Tenable.Io WAS, da fabricante Tenable. Essas soluções foram escolhidas devido à sua compatibilidade técnica com as infraestruturas de segurança e monitoramento já utilizadas pelo Tribunal, bem como pela vantajosidade técnica e econômica demonstrada neste Estudo Técnico Preliminar (ETP). O Tenable One é reconhecido por sua capacidade de oferecer gestão contínua da exposição cibernética (CTEM), integrando módulos avançados de Vulnerability Management, Identity Exposure, Attack Path Analysis e Surface Management. O Tenable.SC proporciona uma abordagem robusta para gerenciamento de vulnerabilidades em ambientes locais, enquanto o Tenable.Io WAS oferece análises avançadas de segurança para aplicações web, alinhando-se perfeitamente às necessidades de conformidade e proteção do órgão.

2.23.9. A tabela a seguir lista os principais produtos relacionados à solução que trata a contratação e respectivos Part Numbers.

Produto	Descrição	Part Number
Tenable.io	Plataforma de gerenciamento de vulnerabilidades baseada na nuvem	TioVM
Tenable Security Center+	Gerenciamento de vulnerabilidades on-premises	Tsc-plus
Tenable.ot	Segurança para tecnologia operacional (OT) e sistemas SCADA	TONE-OT
Tenable Identity Exposure	Deteção de exposição em AD (Active Directory)	TONE-IE
Tenable Attack Surface Management - Daily Rate	Identifica, inventaria e monitora continuamente os ativos expostos na internet de uma organização, permitindo a visualização completa da superfície de ataque externa e a detecção proativa de riscos e vulnerabilidades.	TONE-TASM-DR
Tenable Attack Surface Management - Fortnightly		TONE-TASM-BW
Tenable Cloud Security Enterprise / Standard	Gerenciamento de segurança em nuvem pública (AWS, Azure, GCP)	TONE-TCS-ENT TONE-TCS-BAS
Tenable Vulnerability Management	Realiza a identificação, avaliação e priorização contínua de vulnerabilidades em ativos de TI	TONE-TIOVM
Tenable Web App Scanning (WAS)	Análise de vulnerabilidades em aplicações web	TONE-WAS

2.23.9.1. De forma geral, a solução Tenable One, uma vez que inclui diversos componentes, pode ser representada pelo Part Number T-ONE.

2.23.9.2. Deverão ser informados na proposta comercial as informações referente ao fabricante, a marca/modelo e os *part numbers* do(s) software(s) que compõem as soluções ofertadas. A omissão dessas informações acarretará na desclassificação da proposta. A solução ofertado deve estar em linha de produção, na data de entrega da proposta.

2.23.10. Justificativa para a indicação do Tenable One:

Vantagem	Justificativa
Compatibilidade Técnica	A plataforma Tenable One foi selecionada devido à sua total compatibilidade com as soluções de segurança já empregadas pelo Tribunal, como o Tenable.sc e o Nessus Professional. Essa compatibilidade proporciona uma integração contínua com as atuais ferramentas de monitoramento de vulnerabilidades e gestão de exposição, permitindo uma visão unificada e consolidada da postura de segurança cibernética do Tribunal. (considerando apenas os que desejarem fazer o upgrade da solução). Tenable.SC e Tenable.Io WAS: solução de gestão de vulnerabilidades existente no órgão (considerando apenas os que desejarem manter a solução). Neste caso, o Tribunal em questão já desenvolveu seus planos e processos de gestão de vulnerabilidade com base no(s) software(s) em questão.

Vantajosidade Técnica e Econômica	A escolha da Tenable One também foi motivada pela vantajosidade econômica, sendo uma solução que reúne múltiplos módulos de segurança em uma plataforma unificada. Isso otimiza os custos de licenciamento, manutenção e suporte, além de reduzir a necessidade de investimentos em treinamento para múltiplas ferramentas. A unificação dos módulos permite maior eficiência operacional, melhorando a detecção e resposta a ameaças de forma integrada. Tenable.SC e Tenable.Io WAS: as equipes técnicas dos Tribunais já desenvolveram expertise na utilização da solução. A adoção de outra tecnologia teria um impacto direto na curva de aprendizado e mudança de processos existentes.
Padronização	A padronização com as ferramentas de segurança e monitoramento existentes garante que a solução atenda às exigências de conformidade e continuidade operacional. Isso minimiza a necessidade de novos treinamentos extensivos ou mudanças disruptivas na infraestrutura de segurança cibernética. Além disso, a padronização facilita a implementação de políticas de segurança consistentes e alinhadas com as melhores práticas do setor, assegurando a proteção dos ativos críticos do Tribunal.

2.24. Vedação de marcas, modelos ou produtos

2.24.1. Não há registro de contrato de produtos adquiridos e utilizados anteriormente, associados à solução que trata este ETP, que não atenderam a requisitos indispensáveis ao pleno adimplemento da obrigação contratual.

2.24.2. Não serão admitidas ofertas de outras marcas, soluções parciais ou módulos em razão de incompatibilidade.

2.24.2.1. Portanto, a opção de contratar outras marcas neste projeto resta vedada, sendo justificada pela necessidade de manter a compatibilidade e evitar riscos associados a integrações complexas entre diferentes fabricantes. A fragmentação de soluções entre marcas distintas gera inconsistências e aumenta a probabilidade de problemas de comunicação entre sistemas, o risco de incompatibilidades, o que comprometeria a eficácia das operações e a segurança dos dados.

2.24.2.2. Além disso, a introdução de marcas alternativas pode resultar na perda de funcionalidades essenciais, exclusivas do fabricante indicado, que são cruciais para o cumprimento dos objetivos técnicos do projeto. Essas funcionalidades foram projetadas de forma específica para atender às demandas do órgão e, ao utilizar marcas diferentes, o órgão correria o risco de perder parte dessas capacidades estratégicas.

2.24.2.3. A presença de várias marcas também gera dificuldade no suporte técnico, pois exigia contratos e atendimentos com diferentes fornecedores. Isso tornaria o processo de suporte mais complexo e reduziria a capacidade de resposta da equipe em situações críticas, uma vez que o atendimento seria distribuído entre várias empresas, dificultando a eficiência e a eficiência do suporte.

2.24.2.4. Outro ponto importante é a necessidade de uniformização nos processos de atualização e correção de vulnerabilidades. Em um ambiente com diversos fabricantes, seria necessário seguir cronogramas e padrões diferentes para cada marca, o que aumenta as chances de falhas e dificulta a implementação de melhorias de segurança de forma sincronizada e consistente.

2.24.2.5. Por fim, o uso de múltiplas marcas eleva os custos operacionais e sobrecarrega os recursos administrativos com a gestão de contratos, documentos e suporte. Essa fragmentação implica um custo adicional sem agregar benefícios proporcionais, afetando qualidades de eficiência orçamentária e gestão de recursos institucionais. Dessa forma, a colocação de outras marcas permite ao órgão manter um ambiente coeso, seguro e financeiramente sustentável.

2.25. Necessidade de transição contratual

2.25.1. Estratégia de continuidade da solução em caso de interrupção contratual

Para garantir a continuidade da prestação dos serviços de gestão de exposição cibernética (CTEM) pela plataforma de gestão de vulnerabilidades Tenable, é essencial o monitoramento constante de sua execução e a identificação de riscos que possam comprometer a entrega do serviço. As ações a seguir devem ser adotadas para minimizar os impactos em caso de interrupção contratual:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	AÇÕES DE CONTINUIDADE / RESPONSÁVEIS
Encerramento por abandono, inadimplemento ou incapacidade da empresa contratada	Interrupção da gestão de vulnerabilidades e da proteção cibernética, impactando a segurança da superfície de ataque do Tribunal	Falta de comprometimento no cumprimento contratual	Aplicar sanção por descumprimento contratual	Acompanhar prazos de entrega e monitorar a qualidade dos serviços de segurança (Fiscal Técnico)
Atrasos e ausência de suporte técnico, com impacto na disponibilidade da solução	Vulnerabilidades críticas não tratadas, aumentando o risco de incidentes cibernéticos	Falta de suporte técnico adequado ou atrasos na resposta a incidentes	Acompanhar a regularidade da contratada por meio de relatórios e análises periódicas	Exigir carta de solidariedade do fabricante para garantir a continuidade do suporte (Fiscal Técnico e Administrativo)
Perda de conectividade com a plataforma Tenable	Interrupção dos serviços de monitoramento e análise de vulnerabilidades, impactando o acesso a dados críticos	Problemas de rede ou falha no provedor de conectividade	Implementar redundância de conectividade com provedores alternativos	Acionar a equipe de TI para coordenação com provedores de rede (Fiscal Técnico e Equipe de TI)
Falha no provisionamento de recursos de segurança	Incapacidade de escalar o monitoramento de vulnerabilidades ou alocar novos recursos em momentos críticos	Limitação técnica ou erro de configuração da plataforma	Monitoramento proativo da utilização de recursos e automação da escalabilidade	Ativar processo de contingência para redistribuição de cargas e ajustes (Fiscal Técnico e Equipe de Segurança)
Descontinuidade de serviços de terceiros integrados	Paralisação de serviços adquiridos por meio de parceiros, impactando as integrações críticas de segurança	Fim de contrato ou descontinuidade do fornecedor	Revisar a viabilidade de substituição por serviços equivalentes no mercado	Iniciar processo de aquisição de novas soluções compatíveis (Fiscal Técnico e Administrativo)

2.25.2. Estratégia de Independência do TRE-PA em Relação à Empresa Contratada

A contratação da plataforma Tenable para gestão contínua de vulnerabilidades e exposição cibernética utiliza padrões amplamente adotados no mercado de segurança cibernética, o que minimiza a dependência de um único fornecedor e facilita a migração para outras soluções caso seja necessário. As seguintes estratégias asseguram a

independência do TRE-PA:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	ESTRATÉGIA DE INDEPENDÊNCIA / RESPONSÁVEIS
Interrupção ou fim do fornecimento de suporte/garantia	Paralisação dos serviços de gestão de vulnerabilidades, prejudicando a segurança dos sistemas críticos	Término do contrato ou fim de vida útil da solução	Acompanhar o ciclo de vida da plataforma e monitorar SLAs	Migrar para nova solução compatível ou outro provedor de segurança cibernética (Fiscal Técnico)
Descontinuidade de créditos para a plataforma Tenable One ou serviços associados	Impossibilidade de renovação de créditos essenciais para a continuidade da operação	Desacordo contratual ou obsolescência da oferta	Monitorar a validade dos créditos e o consumo	Buscar alternativas de aquisição de créditos com novos fornecedores (Fiscal Técnico e Administrativo)
Obsolescência tecnológica da contratada	Redução da eficiência da gestão de vulnerabilidades e aumento dos riscos de segurança	Tecnologias desatualizadas ou suporte descontinuado	Monitorar continuamente a plataforma e buscar atualizações	Migrar para soluções mais modernas ou buscar provedores que ofereçam suporte contínuo (Fiscal Técnico)
Dependência excessiva de uma única solução de segurança	Dificuldade em migrar para outro provedor devido a lock-in tecnológico ou contratual	Dependência tecnológica e falta de interoperabilidade	Priorizar soluções baseadas em padrões abertos e interoperáveis	Assegurar que dados e serviços possam ser exportados/migrados sem prejuízo operacional (Fiscal Técnico e Equipe de TI)
Falta de fornecedores qualificados para suporte	Atraso na resolução de incidentes críticos, impactando a operação dos sistemas de segurança	Escassez de fornecedores com expertise na plataforma Tenable One	Análise contínua do mercado para identificar fornecedores alternativos	Implementar contratos de suporte paralelo para contingência (Fiscal Administrativo)

2.25.3. Ações para transição contratual

O TRE-PA deverá manter monitoramento constante do contrato, garantindo que eventos que possam comprometer a execução sejam mitigados. As seguintes ações devem ser adotadas para assegurar uma transição contratual eficaz:

ID	AÇÃO	RESPONSÁVEL	INÍCIO	FIM
01	Realizar reunião de alinhamento inicial com a nova contratada sobre a execução dos serviços de gestão de vulnerabilidades	Gestor do Contrato e Empresa Contratada	Até 5 dias após a assinatura do contrato	Até a apresentação e aprovação do plano de execução
02	Apresentar o Projeto de Execução Contratual, incluindo transferência de conhecimento e continuidade do serviço	Empresa Contratada	Até 15 dias após a assinatura do contrato	Até a aprovação do Projeto de Execução
03	Verificar a possibilidade de aproveitamento de componentes da solução anterior	Gestor do Contrato com Fiscal Técnico	Na fase de elaboração dos Estudos Técnicos Preliminares da nova contratação	—
04	Avaliar e aprovar o Projeto de Execução Contratual	Gestor do Contrato	Até 5 dias após a entrega do projeto	Até o início da execução
05	Iniciar a execução do Projeto de Execução Contratual	Empresa Contratada sob supervisão do Gestor do Contrato	Até 5 dias após a aprovação do projeto	Até o término do contrato
06	Avaliar a execução do Projeto de Execução Contratual	Gestor do Contrato com Fiscal Técnico	Até 5 dias após o início da execução	Até o término do contrato
07	Realizar a migração de dados para o novo provedor, garantindo a integridade e segurança das informações	Empresa Contratada com apoio da Equipe de TI	Após a aprovação do projeto	Até a conclusão da migração
08	Elaborar documento de aprovação formal do projeto para garantir a continuidade do contrato	Fiscal Administrativo e Gestor do Contrato	Até 5 dias após a avaliação do projeto	Após o cumprimento do plano de execução

2.25.4. Ações para encerramento contratual

Ao longo da vigência do contrato, o TRE-PA adotará ações de controle para o encerramento adequado, garantindo a transferência de conhecimento e a continuidade das operações de segurança. As ações a seguir devem ser seguidas:

ID	AÇÃO	RESPONSÁVEL	INÍCIO	FIM
----	------	-------------	--------	-----

01	Validar a entrega das versões finais dos serviços, incluindo scripts, configurações e documentações técnicas	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
02	Realizar a transferência final de conhecimento sobre a gestão de segurança e vulnerabilidades	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
03	Devolução de recursos materiais	Não aplicável, pela natureza digital dos serviços contratados	Após a assinatura do contrato	Ao término do contrato
04	Revogação de perfis/credenciais de acesso à plataforma Tenable One	Gestor do Contrato com Fiscal Técnico	Após a assinatura do contrato	Ao término do contrato
05	Eliminação de dados armazenados	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
06	Realizar o encerramento administrativo do contrato	Gestor do Contrato	5 dias antes do término do contrato	Ao término do contrato

2.25.5. Direitos de propriedade intelectual

Todos os ativos gerados ou manuseados durante a execução contratual da plataforma Tenable One, como configurações de sistemas, códigos-fonte, scripts de automação e documentações técnicas, serão de propriedade exclusiva do CONTRATANTE. Esses ativos não poderão ser copiados, modificados ou utilizados pela CONTRATADA sem a devida autorização.

A CONTRATADA deverá entregar toda a documentação técnica, configurações e artefatos produzidos, garantindo que o CONTRATANTE tenha total controle sobre a continuidade da operação e a possibilidade de auditorias ou replicações. O CONTRATANTE terá acesso irrestrito a quaisquer componentes customizados, mantendo controle sobre as versões e podendo realizar auditorias ou modificações conforme necessário.

Essa adaptação mantém a coesão com a contratação da Tenable One, focando nos requisitos de segurança cibernética, continuidade dos serviços e transição eficiente, garantindo que o Tribunal tenha controle total e flexibilidade durante todo o ciclo de vida contratual.

2.26. Da Habilitação Técnica

2.26.1. Existe a necessidade de inclusão de exigência de habilitação técnica, com a comprovação através de atestados de capacidade técnica, para a contratação da solução de Tecnologia da Informação (TI). Tal exigência garante que a empresa contratada possui conhecimento e expertise técnica adequada e suficiente para implementar e operar a solução de TI objeto da contratação de forma eficiente e segura, atendendo aos requisitos específicos do projeto, contribuindo para a consecução do objeto e a qualidade da solução contratada, sendo essencial para mitigar os riscos associados a uma contratação de grande vulto e complexidade, como a presente, pelos seguintes motivos:

- **Criticidade e Relevância do Objeto:** A contratação de uma Plataforma de Gerenciamento de Exposição Cibernética é estratégica e crítica para a segurança da informação de todos os órgãos partícipes da Ata. Uma falha no fornecimento, renovação ou suporte dessas licenças pode expor toda a infraestrutura de TI a vulnerabilidades severas, com potencial risco de paralisação de serviços essenciais, vazamento de dados sigilosos e danos à imagem institucional. Portanto, é indispensável que a contratada demonstre possuir capacidade operacional para lidar com um objeto de tal magnitude e importância.
- **Capacidade Operacional e Logística em Larga Escala:** O gerenciamento de um volume expressivo de licenças exige da empresa contratada uma estrutura robusta de gestão de ativos de software, processos de faturamento, controle de renovações e logística de entrega de chaves de ativação ou provisionamento em nuvem. Uma empresa que nunca operou em tal escala pode não possuir a maturidade de processos necessária, resultando em atrasos, erros de provisionamento e falhas no suporte, o que comprometeria a execução contratual. A exigência de 50% serve como um filtro para selecionar empresas que já demonstraram empiricamente possuir tal capacidade.
- **Complexidade da Gestão de uma Ata de Registro de Preços Compartilhada:** A presente Ata envolve múltiplos órgãos da Justiça Eleitoral. A futura contratada deverá gerenciar demandas pulverizadas, com diferentes pontos de contato, ciclos de faturamento e necessidades específicas de suporte em cada órgão partícipe. A experiência prévia com quantitativos elevados é um forte indicativo de que a empresa possui a estrutura administrativa e os sistemas de gestão necessários para lidar com a complexidade de uma contratação multi-institucional, evitando falhas de comunicação e de atendimento que poderiam ocorrer com um fornecedor sem experiência em contratos de grande porte.
- **Sustentabilidade e Continuidade do Contrato (60 meses):** O objeto não se resume a uma simples entrega de licenças. Ele inclui serviços de implantação e, crucialmente, garantia e suporte por um período de 60 meses (5 anos). É fundamental que a empresa contratada demonstre estabilidade e solidez no mercado. Uma experiência longa no fornecimento deste tipo de solução indica que a empresa não é uma "aventureira", possuindo maturidade de mercado para sustentar um relacionamento contratual de longo prazo, garantindo o suporte e a manutenção das condições durante toda a vigência do ajuste.
- **Mitigação do Risco de Descontinuidade do Fornecedor:** Contratar uma empresa sem um histórico comprovado em um contrato de 5 anos aumenta o risco de que ela enfrente dificuldades financeiras, operacionais ou mesmo encerre suas atividades antes do término do contrato. Isso deixaria a Administração desprovida do suporte técnico essencial e com a necessidade de realizar um novo e custoso procedimento licitatório de forma emergencial. A exigência de experiência minimiza este risco, selecionando empresas com maior probabilidade de permanência e estabilidade no mercado.

2.26.2. O objeto da presente contratação – o fornecimento de licenças de Plataforma de Gerenciamento de Exposição Cibernética, incluindo serviços de implantação e garantia estendida de 60 (sessenta) meses – é de natureza crítica para a segurança da informação e a continuidade das operações da Justiça Eleitoral no Pará. A gestão de exposição cibernética é um pilar fundamental na proteção de dados sensíveis, sistemas eleitorais e infraestrutura de tecnologia da informação, cuja falha ou interrupção pode acarretar prejuízos irreparáveis à missão institucional deste Tribunal.

2.26.3. Diante dessa complexidade e do volume de licenças a serem gerenciadas, afigura-se indispensável que o licitante demonstre ter capacidade operacional e experiência prévia em contratos de escala semelhante. Nesse contexto, e em conformidade com o disposto no art. 67, § 2º, da Lei nº 14.133/2021, que autoriza a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de maior relevância, foram definidos os quantitativos mínimos correspondente à 50% do total do principal item de cada grupo a ser licitado.

2.26.4. Esses quantitativos mínimos a serem exigidos revelam-se, portanto, proporcionais, pertinentes e indispensáveis, constituindo um parâmetro razoável para aferir a capacidade operacional do licitante, visto, ainda, a existência de outros itens a serem licitados, sem restringir indevidamente a competitividade do certame. Tal medida visa selecionar um parceiro comercial com comprovada aptidão para gerenciar contratos de escala e complexidade similares, garantindo a segurança jurídica e operacional que o objeto requer.

2.26.5. Considerando que o objeto contratual envolve uma relação jurídica de longo prazo, notadamente pela garantia de 60 (sessenta) meses, a contratação se assemelha, em seus efeitos e na necessidade de acompanhamento, a um serviço de natureza continuada. Desse modo, com amparo no art. 67, § 5º, da Lei nº 14.133/2021, será exigida a comprovação de experiência mínima de 3 (três) anos na execução de serviços de fornecimento de licenciamento de software.

2.27. Garantia da contratação

2.27. Será exigida a garantia da contratação de que tratam os [arts. 96 e seguintes da Lei nº 14.133, de 2021](#), no valor correspondente a 5% (cinco por cento) do valor global do contrato, tendo em vista o valor vultoso da contratação e o risco administrativo elevado em caso de inadimplemento da execução do contrato. A falha na

prestação deste serviço pode comprometer todo o ambiente computacional do Tribunal, sendo, portanto, necessária a garantia para, ao menos, mitigar os riscos da Administração e nas condições descritas nas cláusulas do contrato, assegurando, ainda que parcialmente, o ressarcimento de prejuízos sofridos pelas falhas.

2.27.1. O contrato oferece maior detalhamento das condições e regras que serão aplicadas em relação à garantia da contratação.

2.28. Vistoria

2.28.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

2.29. Tratamento diferenciado para ME e EPP

2.29.1. A presente contratação **não** observará o tratamento favorecido, diferenciado e simplificado para Microempresas (ME) e Empresas de Pequeno Porte (EPP), nos termos da Lei Complementar nº 123/2006 e do Decreto nº 8.538/2015, considerando o valor estimado da contratação superar os R\$ 80.000,00 (oitenta mil reais).

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS (VOLUMETRIA)

3.1. O dimensionamento do volume dos serviços consiste na identificação do quantitativo de licenças (subscrição), créditos a serem consumidos no período de vigência do contrato, e serviços agregados de treinamento/capacitação e suporte operacional. Deste modo, segue as informações referentes ao dimensionamento da demanda, fundamentadas no licenciamento atualmente utilizado, necessidade de upgrade de licenciamento do contrato atual e estimativas extraídas do levantamento de ativos no ambiente como workers de cluster Kubernetes.

3.2. CONTRATAÇÃO DE PLATAFORMA DE GERENCIAMENTO DE EXPOSIÇÃO

3.2.1. Premissas adotadas para contratação de software:

3.2.2. Para o dimensionamento, consideramos a contratação anterior liderada pelo TRE-PB, cujo objeto e volume da contratação é demonstrado no quadro a seguir:

ITEM ATA 101/2020	DESCRIÇÃO	QTDE LICENÇAS	IPs LICENCIADOS
14	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 128 endereços IP, por 36 meses de uso e suporte pelo fabricante. (solução baseada em nuvem pelo fabricante Tenable)	01	05
21	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante.	01	500
24	Instalação e configuração da solução.	01	---
25	Repasse tecnológico (Treinamento), com período mínimo de 20 horas.	01	---

3.2.3. Como ocorreram grandes mudanças na solução tanto em funcionalidades como nos tipos de licenciamentos, será viabilizada a opção de fazer o upgrade para as novas licenças e funcionalidades.

3.2.4. Em momento oportuno será oficializada a solicitação para informação da quantidade de licenças existente em cada TRE interessado em participar da licitação, considerando ainda a eventual necessidade de ampliação da referida quantidade de IPs atualmente licenciados no ambiente.

3.2.4.1. Nestes termos, o objeto da contratação deve incluir grupo específico contendo item de renovação do Tenable.sc e upgrade para o Tenable ONE, bem como contratação eventual e futura de novas licenças do Tenable ONE.

3.2.4.2. O objeto deve integrar as soluções de gestão de vulnerabilidades e exposição existentes no Tribunal. (Tenable.sc e Tenable Identity Exposure).

3.2.5. O objeto da contratação deve permitir o licenciamento por ativo, simplificando a gestão e aumentando a cobertura da superfície de ataque. Entende-se por ativo dispositivos de rede (firewalls, switches, servidores e desktops), FQDNs, usuários ativos do Active Directory, instâncias de computação em nuvem pública, hosts ou orquestradores de contêineres em nuvem pública, ativos sem servidor, repositórios de contêineres ou hosts de contêineres locais.

3.2.6. O quadro a seguir demonstra o número de licenças, ou quantidades específicas do TRE-PA para a contratação eventual e futura.

3.2.6.1. A estimativa de licenciamento foi baseada nos ativos (Assets) existentes e respectivo licenciamento necessário para a quantidade encontrada. A figura a seguir exibe a calculadora do fabricante utilizada, que demonstra a quantidade necessária para a quantidade de ativos correspondentes. Link da calculadora do fabricante - <https://docs.tenable.com/quick-reference/licensing-guide/Content/tenable-one-licensing.htm#Reclaiming-Licenses>

Product	Type	Licenses	Ratio	Assets
Cloud Products				
Tenable Vulnerability Management	Assets	500	1,00	500,00
Tenable Web App Scanning	FQDNs	5	1,00	5,00
CIEM	Cloud resource workloads	0	3,00	0,00
Tenable Cloud Security Standard	Cloud resource workloads	0	5,00	0,00
Tenable Cloud Security Enterprise	Cloud resource workloads	40	7,50	300,00
Tenable Identity Exposure	Identities	1800	0,50	900,00
Tenable Attack Surface Management Fortnightly Frequency	Observable objects	0	0,25	0,00
Tenable Attack Surface Management Daily Frequency	Observable objects	0	0,50	0,00
On-premise Products				
Tenable OT Security	Assets	0	1,50	0,00
Tenable Web App Scanning	FQDNs	0	1,00	0,00
Tenable Security Center+	IP addresses	0	1,00	0,00
Third-Party Applications				
Third-Party Application Assets	Assets	0	0,5	0,00
Totals				
Total Tenable One Cloud Assets		1,705,00		
Total Tenable One On-premise Assets		0,00		
Total Third-Party Application Assets		0,00		
Total Tenable One Assets		1,705,00		

ITEM	TIPO DE ATIVO	QUANTIDADE DE ASSETS	QUANTIDADE DE LICENÇAS
Tenable.Io WAS	FQDNs	5	5
Tenable Vulnerability Management	ASSETS	500	500
Tenable Cloud Security Enterprise	CLOUD RESOURCE WORKLOADS	40	40
Tenable Identity Exposure	IDENTITIES	1800	900
Total de Licenças			1.750

3.2.7. Estimativa de demanda dos Tribunais Regionais Eleitorais interessados na contratação.

3.2.7.1. Para a contratação que trata este ETP, optou-se utilizar o procedimento de contratação conjunta comumente utilizada na Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), o qual permite a modalidade de compra por mais de um Tribunal interessado na solução de em razão da necessidade de padronização de tecnologias, visando atender a arquitetura proposta na [Estratégia Nacional de Segurança Cibernética do Poder Judiciário \(ENSEC-PJ\)](#).

3.2.7.2. O IRP é a manifestação prévia de um órgão público, informando sua intenção de participar do processo de registro de preços. A utilização do IRP (Intenção de Registro de Preços) traz várias vantagens como a economia em escala, uma vez que é possível obter melhores condições comerciais e preços mais vantajosos; além da flexibilidade e conveniência, pois cada órgão público possui a liberdade de utilizar o registro de preços de acordo com suas necessidades e disponibilidade orçamentária. Isso permite uma maior flexibilidade na contratação de bens ou serviços, conforme a demanda surgir, sem a necessidade de realizar uma nova licitação.

3.2.7.3. Visando o levantamento de informações entre os Tribunais Regionais Eleitorais interessados na contratação, o TRE-PA efetuou o consulta inicial de

informações para dimensionamento da solução que trata este ETP. A referida consulta constitui do trabalho de planejamento conjunto após reunião realizada no dia 17 de fevereiro de 2024, por meio de videoconferência. Objetivando conhecer a realidade de cada TRE, ante os requisitos tratados na elaboração dos Estudos Preliminares da Contratação, foi encaminhado o formulário Google do evento 0002643628, cujas respostas encaminhadas constituíram o dimensionamento inicial da contratação.

3.2.7.4. Posteriormente, objetivando a pesquisa mais completa de informações entre os Tribunais Regionais Eleitorais interessados na contratação, a equipe de planejamento da contratação, conforme orientação do Ofício-Circular TSE GAB-DG Nº 36/2025 (evento 2680781), formulou consulta mediante o Ofício-Circular nº 112 / 2025 - TRE/PRE/DG/STI/CGSI (2796285) aos Tribunais Regionais Eleitorais interessados em integrar a futura Ata de Registro de Preços para que, na qualidade de participantes, manifestassem a concordância quanto ao objeto, condições e especificações técnicas do Termo de Referência, valores estimados e confirmação dos quantitativos demandados (art. 7º, VI, do Decreto n. 11.462/23).

O resultado da consulta foi consolidado na planilha intitulada "Consolidação das Respostas - Ofício-Circular 112/2025-CGSI" (SEI nº 2812556). As tabelas a seguir apresentam as referidas quantidades e itens selecionados pelos Regionais, incluindo o TRE-PA.

GRUPO 1: Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética Tenable.IO WAS e Tenable Security Center (SC+), garantindo a continuidade do uso das ferramentas atualmente implementadas nos Tribunais Regionais Eleitorais. O fornecimento inclui garantia técnica, suporte especializado e repasse de conhecimento na modalidade Hands On, assegurando a manutenção da efetividade na identificação e mitigação de vulnerabilidades. A renovação poderá ser prorrogada nos termos da legislação vigente, conforme as condições, quantidades e exigências estabelecidas no Termo de Referência.			
ITEM	1	2	3
DESCRIÇÃO	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Externos - Tenable.IO WAS, para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo o serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Internos - Tenable Security Center (SC+), para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).
UNIDADE	UND	UND	TURMA
TRE-AL	0	500	1
TRE-PA	5	500	1
TRE-MG	24	400	0
TRE-PB	5	500	1
TRE-PI	5	500	1
TOTAL	39	2400	4

Grupo 2: Fornecimento de subscrição de licenças de direito de uso, do software de Gerenciamento de Exposição Cibernética Tenable One para atualização (upgrade) da versão Tenable Security Center Plus (Tenable.SC+) e Tenable Identity Exposure, atualmente em uso nos Tribunais Regionais Eleitorais, incluindo a aquisição de novas licenças de subscrição do Tenable One, garantia técnica serviços de suporte técnico e repasse de conhecimento (Hands On), podendo se prorrogado nos termos da Lei, conforme condições, quantidades e exigências constantes do Termo de Referência.						
ITEM	4	5	6	7	8	9
DESCRIÇÃO	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable.io Web Application Scanning (WAS) para a subscrição do licenciamento Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable Security Center (SC+) para a subscrição do licenciamento do software Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	Contratação da subscrição do licenciamento do software de Gerenciamento de Exposição Cibernética Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	Serviço de Instalação, configuração e migração do ambiente atual.	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	Serviço de Operação Assistida e apoio operacional, pelo período de 60 (sessenta) meses, sob demanda
UNIDADE	UND	UND	UND	UND	TURMA	UND
TRE-PA	5	500	1200	1	1	1
TSE	0	0	2000	0	0	0
TRE-AL	0	500	1250	1	1	1
TRE-MA	0	300	0	1	1	0
TRE-ES	0	500	1300	1	1	1
TRE-TO	0	500	0	1	1	1
TRE-GO	0	1250	650	1	2	1
TRE-RJ	0	0	250	1	1	1
TRE-MT	0	0	1000	1	1	1
TRE-MS	0	700	260	1	1	1
TRE-PB	5	500	1800	1	1	1
TRE-RO	0	0	1250	1	1	1
TRE-PI	5	1800	1800	1	1	1
TRE-SP	0	0	3355	1	1	1
TRE-DF	0	1250	1250	1	1	1
TRE-SE	0	1100	0	1	1	1
TRE-AP	0	500	350	1	1	1
TRE-RN	5	250	1350	1	1	1
TRE-PR	0	0	550	1	1	1
TRE-BA	0	1500	1400	1	1	1
TRE-AM	10	500	0	1	1	1
TRE-CE	0	250	980	1	1	0
TOTAL	30	11900	21995	21	22	19

4. ANÁLISE COMPARATIVA DE SOLUÇÕES E LEVANTAMENTO DE MERCADO

Fundamentação: análise comparativa de soluções, que deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos

objetivos da contratação, observando o que dispõe as alíneas do inciso II do art. 11, da IN 94/2022 (inciso V do § 1º do art. 18 da Lei 14.133/2021 e Art. 11, inciso II da IN 94/2022).

Para a elaboração deste ETP, foram consideradas as orientações para Contratação de Soluções de TIC, incluindo os guias, manuais e modelos publicados pelo CNJ, AGU e Órgão Central do SISP, disponíveis no Portal Governo Digital. Adicionalmente, foram realizadas consultas ao Portal Nacional de Contratações Públicas (PNCP) e à Plataforma de Governança Digital Colaborativa do Poder Judiciário (Connect-Jus), a fim de analisar dados estruturados de contratações realizadas em todo o país.

4.1. Disponibilidade de solução similar (alínea a)

Foram realizadas buscas para identificar a disponibilidade de soluções similares em outros entes da Administração Pública. Embora diversos órgãos possuam contratos para gestão de vulnerabilidades, a análise detalhada revela que cada projeto possui particularidades que o tornam específico, como o ambiente tecnológico, a arquitetura, as integrações com sistemas legados e os modelos de licenciamento.

Apesar dessas especificidades, foram identificadas contratações com objetos semelhantes, que servem como referência de prática de mercado no setor público, conforme demonstrado na tabela abaixo:

ÓRGÃO	PREGÃO/CONTRATO/DISPENSA OU INEXIGIBILIDADE	OBJETO
TRIBUNAL SUPERIOR ELEITORAL	CONTRATO TSE Nº 44/2024	O presente contrato tem por objeto o fornecimento de subscrição de 2.500 (duas mil e quinhentas) licenças de direito de uso, do software de Gestão de Vulnerabilidades Tenable One Standard para atualização (upgrade) da versão Tenable Security Center Plus (Tenable.SC+) atualmente em uso no TSE, incluindo a garantia técnica, serviços de suporte técnico e repasse de conhecimento (Hands On).
TRIBUNAL REGIONAL ELEITORAL DE RORAIMA	CONTRATO Nº 65/2023	O objeto do presente instrumento é a contratação de empresa para fornecimento e instalação de solução de gestão de vulnerabilidades, visando a continuidade do processo de análise periódica das vulnerabilidades dos ativos de TI conectados à rede do TRE-RR.
TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA	CONTRATO Nº 4/2024	O objeto do presente instrumento é a contratação de empresa para fornecimento de licenças de Solução de Gerenciamento de Vulnerabilidades, fornecido como SaaS, incluindo instalação, configuração, suporte, garantia, repasse técnico e atualizações pelo período de 12 (doze) meses.
TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ	CONTRATO Nº 029/2023	O Presente instrumento tem por objeto a aquisição de solução que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseada em risco, dos ativos de Tecnologia da Informação, com análise contínua e adaptável de riscos e confiança, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações, conforme condições, especificações e quantidades constantes no Termo de Referência - ANEXO I e na proposta comercial.
TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS	CONTRATO Nº 191/2023	O presente instrumento tem por objeto fornecimento de solução de gestão de vulnerabilidades em ativos de TIC e análise dinâmica de aplicações web com gerenciamento e armazenamento em nuvem (modalidade on cloud), incluindo serviços de implantação, configuração, nos termos do edital, deste contrato e dos seus anexos.
TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO	CONTRATO Nº 37 / 2023	O presente contrato tem por objeto o licenciamento com suporte técnico e direito de atualização, no modelo de subscrição, para solução de Gestão de Vulnerabilidades dos Ativos de Tecnologia da Informação.

4.2. Alternativas do mercado (alínea b)

Para atender à demanda de aprimorar o gerenciamento da exposição cibernética, foram identificadas quatro alternativas estratégicas:

- 1) **Manter a infraestrutura atual sem expandir:** Preservar o ambiente de segurança existente, sem realizar novas aquisições ou atualizações.
- 2) **Substituir a solução atual por outra de fabricante distinto:** Realizar a troca completa das ferramentas atuais por uma nova plataforma de outro fornecedor.
- 3) **Expandir a infraestrutura com soluções de outros fabricantes:** Complementar o ambiente atual com ferramentas de diferentes fornecedores para atender a necessidades específicas.
- 4) **Ampliar a infraestrutura com soluções do mesmo fabricante:** Expandir a capacidade de segurança com novas soluções do mesmo fabricante das ferramentas já em uso (Tenable), garantindo compatibilidade nativa.

4.3. Existência de software público ou software de governo

Não foi identificado, no Portal do Software Público Brasileiro ou em outras plataformas governamentais, uma solução de software livre ou público que atenda de forma integral aos requisitos de gestão contínua de exposição cibernética (CTEM) detalhados neste estudo.

4.4. Políticas, modelos e padrões de governo

Não se aplica, pois o objeto da contratação é a aquisição de um serviço (SaaS) e licenciamento de software de mercado, não se tratando de desenvolvimento de software que exija aderência a padrões como e-Ping, e-Mag ou e-PWG.

4.5. Necessidades de adequação do ambiente

A princípio, não há necessidade de adequação do ambiente da Contratante para viabilizar a execução contratual, conforme detalhado no item 7 deste documento.

4.6. Diferentes modelos de prestação do serviço

O mercado de cibersegurança oferece diversos modelos de prestação de serviços. No entanto, para a necessidade de gestão integrada e contínua de vulnerabilidades, o modelo de **Software como Serviço (SaaS)** se mostrou o mais adequado, alinhado à solução viável identificada. Outros modelos, como o licenciamento perpétuo, foram analisados e considerados menos vantajosos, conforme detalhado no item a seguir.

4.7. Diferentes tipos de solução

Foram analisados diferentes modelos de licenciamento e entrega de soluções de TI, cujas características são resumidas na tabela abaixo:

Solução ou Alternativa	Descrição	Prós	Contras
------------------------	-----------	------	---------

Solução ou Alternativa	Descrição	Prós	Contras
Licenciamento Perpétuo	Pagamento único para direito de uso permanente do software.	Autonomia total sobre o software, sem pagamentos recorrentes.	Risco de obsolescência, custos adicionais para suporte e atualizações.
SaaS (Software como Serviço)	Acesso ao software via internet mediante assinatura, com hospedagem e atualizações gerenciadas pelo fornecedor.	Atualizações automáticas, previsibilidade de custos, alta escalabilidade e flexibilidade.	Menor controle direto sobre o software, dependência do fornecedor.
Assinatura On-premise	Software instalado localmente, com pagamento de assinatura para atualizações e suporte.	Controle total sobre o ambiente e maior segurança dos dados em servidores internos.	Responsabilidade da organização pela infraestrutura, gerando custos adicionais e exigindo equipe especializada.
IaaS (Infraestrutura como Serviço)	Disponibilização de infraestrutura de TI (servidores, redes) gerenciada por um provedor, com pagamento pelo uso.	Elimina a necessidade de investimento em hardware próprio e permite alta escalabilidade.	A complexidade de gerenciamento das aplicações e dados permanece com a organização.
PaaS (Plataforma como Serviço)	Fornecimento de uma plataforma completa para desenvolvimento, com infraestrutura gerenciada pelo fornecedor.	Facilita e acelera o desenvolvimento de aplicações.	A personalização pode ser limitada e há risco de dependência do fornecedor (lock-in).

A análise conclui que o modelo **SaaS** é o mais aderente aos objetivos de modernização, flexibilidade e eficiência operacional do Tribunal.

4.8. Contratação como aquisição de bens x como serviço por subscrição

A contratação será formalizada como **serviço**. A opção pelo modelo de serviço em detrimento da aquisição de bens (licenças perpétuas) é justificada pela escalabilidade, que permite ajustar recursos conforme a demanda, e pela atualização tecnológica contínua, que garante acesso às mais recentes funcionalidades de segurança sem custos adicionais de aquisição. Adicionalmente, o modelo de serviço por subscrição oferece maior previsibilidade financeira por meio de pagamentos únicos (upfront), conforme a demanda planejada e correspondente ao licenciamento do período, o que desonera a equipe interna de TI das tarefas de manutenção e suporte da infraestrutura subjacente. Essa prática serve para garantir o compromisso do cliente e cobrir os custos iniciais do fornecedor, sendo comum em setores como assinaturas, serviços e produtos digitais por subscrição.

4.9. Ampliação x Substituição da solução implantada

A análise comparativa entre as alternativas demonstrou que a **ampliação da solução implantada (Solução 4)** é a estratégia mais vantajosa em relação à **substituição completa (Solução 2)**. A substituição por um fabricante distinto implicaria em altos riscos operacionais, uma longa curva de aprendizado para a equipe técnica e potenciais incompatibilidades com a infraestrutura existente, gerando um período de vulnerabilidade durante a transição. A ampliação, por sua vez, aproveita a expertise já consolidada, garante a continuidade operacional e minimiza os riscos de integração.

4.10. Diferentes métricas de prestação do serviço e de pagamento

A contratação se refere à subscrição de software e serviços agregados, cujo pagamento será realizado **em parcela única**, mediante a prestação efetiva do serviço e a apresentação da respectiva nota fiscal. A métrica de licenciamento será por ativo, simplificando a gestão e permitindo uma cobertura abrangente da superfície de ataque.

Os serviços de "Suporte Técnico com Operação Assistida, pelo período de 60 (sessenta) meses" referente ao item 9 do GRUPO 2 desta contratação possuem **previsão de pagamento mensal**, conforme verificado no levantamento de mercado, portanto, **mediante aferição mensal da correta execução**.

4.11. Identificação das soluções

Id	Descrição da solução (ou cenário)
1	Manter a infraestrutura atual e não expandir.
2	Substituir toda a solução atual por outra, de diferente fabricante.
3	Expandir a infraestrutura com soluções de outros fabricantes.
4	Ampliar a infraestrutura com soluções do mesmo fabricante.

4.12. Análise Comparativa das Soluções

A escolha da solução mais adequada deve considerar os riscos e benefícios de cada cenário, especialmente por se tratar de solução que envolve diversos cenários inclusive com propostas on premise e SaaS. Os quadros a seguir detalham a comparação de cada solução.

REQUISITO	SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
	Solução 4		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
	Solução 4		X	
	Solução 1			X

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

Requisito Crítico	Solução 1: Manter	Solução 2: Substituir	Solução 3: Expandir com Terceiros	Solução 4: Ampliar com mesmo Fabricante
Integração e Compatibilidade	Inviável. Mantém a gestão de segurança fragmentada entre as ferramentas existentes.	Inviável. Alto risco de incompatibilidade com os sistemas legados e processos atuais do Tribunal.	Inviável. Risco elevado de falhas de comunicação entre sistemas e perda de funcionalidades essenciais.	Viável e Recomendado. Garante integração total e nativa com as ferramentas já em uso, permitindo uma operação coordenada e eficaz.
Risco Operacional	Alto. Aumento da exposição a ameaças cibernéticas devido à falta de evolução e atualização das ferramentas.	Crítico. Risco de interrupção dos serviços, insegurança operacional durante a transição e necessidade de uma longa curva de aprendizado.	Alto. O ambiente fragmentado aumenta a complexidade de gestão e o risco de zonas de exposição a vulnerabilidades.	Baixo. Mantém a continuidade, aproveita os padrões e rotinas já estabelecidos e minimiza a complexidade operacional.
Padronização e Gestão	Baixa. Preserva a fragmentação existente entre as soluções, dificultando uma visão unificada da superfície de ataque.	Baixa. Rompe com a padronização e rotinas já estabelecidas no Tribunal, especialmente com relação ao conhecimento absorvido pela equipe técnica e processos estabelecidos.	Inexistente. A multiplicidade de fornecedores dificulta o gerenciamento centralizado, a manutenção e o suporte técnico.	Alta. Fortalece a padronização, facilita o gerenciamento centralizado e otimiza os esforços da equipe de TI.
Resultado da Análise	Inviável.	Inviável.	Inviável.	Viável e Recomendado.

Justificativa da Escolha

A análise demonstra que a Solução 4 (Ampliar a infraestrutura com soluções do mesmo fabricante) é a única que atende plenamente aos requisitos de segurança, continuidade e eficiência da Justiça Eleitoral. As demais soluções foram consideradas inviáveis por introduzirem riscos operacionais, complexidade de gestão e potencial fragmentação da postura de segurança, o que é incompatível com os objetivos estratégicos de proteção cibernética da instituição.

Dentro desta estratégia, foram avaliadas duas abordagens: a renovação do licenciamento da solução nos moldes atuais (on-premise) ou a atualização (upgrade) para a plataforma integrada em nuvem (SaaS). A opção pelo upgrade para a solução SaaS (Tenable One) se mostra mais vantajosa, pois resolve a principal deficiência do modelo atual: a fragmentação entre as ferramentas de gestão de vulnerabilidades e de identidades, que não possuem integração nativa. A plataforma unificada permite o correlacionamento nativo de informações, proporcionando uma visão centralizada e completa da superfície de ataque, reduzindo a complexidade operacional e alinhando o Tribunal às estratégias mais modernas de Gerenciamento Contínuo da Exposição Cibernética (CTEM). De outro lado, visando proporcionar maior participação de Tribunais que optarem pela contratação conjunta, será franqueada a participação para manutenção do modelo atual de contratação por meio de um grupo específico para essa modalidade (Lote 1)

Portanto, a escolha recai sobre a ampliação da infraestrutura com soluções do mesmo fabricante, por ser a alternativa que, além de garantir a continuidade, moderniza a gestão de segurança e soluciona de forma eficaz a necessidade de integração e centralização das defesas cibernéticas do Tribunal.

4.12.1. Benefícios da solução que aufer os melhores resultados

A contratação de uma Plataforma de Gerenciamento de Exposição oferece uma série de benefícios significativos, trata-se de uma plataforma unificada de gestão de exposição ao risco que permite identificar, avaliar e priorizar ameaças em tempo real, facilitando ações corretivas e preventivas. Seguem abaixo os benefícios esperados:

Benefícios	Justificativa
Visão Abrangente da Superfície de Ataque	O Tenable One fornecerá uma visão consolidada de todos os ativos e ameaças em potencial na infraestrutura do TRE-PA. Ele monitora redes, dispositivos conectados, serviços na nuvem e aplicativos, permitindo que a equipe de segurança tenha uma visão global e detalhada da superfície de ataque. Essa visibilidade ampla é essencial para identificar pontos fracos e compreender o cenário geral de segurança do Tribunal.
Avaliação Proativa e Contínua de Vulnerabilidades	A plataforma permite uma avaliação contínua das vulnerabilidades, detectando-as antes que se tornem ameaças. O Tenable One utiliza inteligência artificial e aprendizado de máquina para aprimorar a detecção de vulnerabilidades, permitindo que as equipes de segurança atuem de maneira proativa. Isso reduz a janela de exposição e minimiza o risco de ataques que exploram vulnerabilidade recém-descobertas.
Priorização Baseada em Risco	Um dos principais diferenciais do Tenable One é sua capacidade de priorizar vulnerabilidades com base no risco. A plataforma considera o contexto do ambiente da empresa, o impacto potencial e a probabilidade de exploração, oferecendo uma classificação de risco que facilita a tomada de decisão. Isso é crucial para que as equipes possam concentrar esforços nas ameaças mais críticas, otimizando tempo e recursos.

Automação de Processos e Redução de Complexidade	O Tenable One ajuda a simplificar a gestão de segurança ao automatizar várias etapas do processo de identificação e remediação de vulnerabilidades. Essa automação permite que a equipe de segurança reduza a carga operacional e ganhe agilidade no combate a ameaças, contribuindo para uma gestão mais eficiente e uma resposta mais rápida a incidentes.
Conformidade com Regulamentações e Melhores Práticas	A plataforma facilita o cumprimento de regulamentações de segurança, como GDPR, PCI-DSS, HIPAA, entre outras. Ela oferece ferramentas para auditorias e relatórios que ajudam a empresa a se manter em conformidade com padrões de segurança e a evidenciar essas práticas para auditorias externas.
Relatórios Detalhados e Insights para Tomada de Decisão	Com o Tenable One, as empresas têm acesso a relatórios detalhados e personalizados, que incluem métricas de segurança, tendências e recomendações de melhorias. Esses relatórios fornecem insights valiosos que podem orientar a estratégia de segurança e auxiliar na comunicação dos riscos cibernéticos para os tomadores de decisão, alinhando os objetivos de segurança aos objetivos do Tribunal.
Integração com Outras Ferramentas de Segurança	A plataforma foi desenvolvida para integrar-se facilmente com outras ferramentas de segurança, SIEMs, soluções de orquestração de segurança e resposta a incidentes (SOAR), entre outras. Isso facilita a adoção do Tenable One no ecossistema de segurança já existente no tribunal, promovendo uma gestão centralizada e mais coesa.
Redução de Custo	Ao consolidar várias funcionalidades em uma única plataforma, o Tenable One contribui para a redução de custo do tribunal com soluções de segurança. A Justiça Eleitoral pode simplificar seu ambiente de segurança, eliminando a necessidade de várias soluções pontuais, reduzindo custos operacionais e obtendo melhor visibilidade com uma solução unificada.
Maior Resiliência e Proteção Contra Ameaças Emergentes	Por meio da análise preditiva, o Tenable One permite identificar e se preparar para ameaças emergentes. A plataforma realiza uma vigilância constante de novas tendências de ameaças e vulnerabilidades, atualizando seu banco de dados e algoritmos de segurança de acordo com o cenário de ameaças mais recente.

4.13. Análise quanto as condições semelhantes às do setor privado

A solução escolhida observa as diretrizes gerais e específicas da Resolução CNJ 468/2022 e da IN SGD/ME nº 94/2022, para a contratação de serviços de tecnologia, incluindo condições de aquisição e pagamento análogas às praticadas no setor privado, naquilo que é aplicável à Administração Pública. Foram realizadas pesquisas de mercado e consultas a informações de fornecedores para assegurar que as condições de preço, forma de pagamento e prazos estejam alinhadas às práticas comerciais vigentes, garantindo uma contratação eficiente e competitiva.

5. ANÁLISE COMPARATIVA DE CUSTOS

Fundamentação: análise comparativa de custos, que **deverá considerar apenas as soluções técnica e funcionalmente viáveis**, incluindo (i) cálculo dos custos totais de propriedade por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução e (ii) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados (inciso V do § 1º do art. 18 da Lei 14.133/2021 e Art. 11, inciso III da IN 94/2022).

5.1. Soluções inviáveis

5.1.1. São soluções inviáveis:

ID Solução	Solução ou Alternativa	Justificativa da inviabilidade
SOLUÇÃO 1	Manter uma infraestrutura atual e não expandir	Uma alternativa de manter a infraestrutura de segurança cibernética sem expansão ou atualizações adicionais apresenta algumas limitações para atender às crescentes demandas de segurança e de conformidade. Com o aumento contínuo das ameaças cibernéticas e a evolução das técnicas de ataque, essa opção torna-se inviável, pois eleva os riscos de exposição e vulnerabilidade do ambiente do Tribunal. A ausência de investimentos adicionais na expansão da infraestrutura prejudica a atualização dos mecanismos de monitoramento e resposta, deixando o ambiente desprotegido e desatualizado frente aos padrões de segurança modernos. Além disso, manter o sistema sem melhorias limita a capacidade de resposta a incidentes e a integração de novas funcionalidades que acompanham a evolução tecnológica, aumentando a exposição do Tribunal e dificultando a operacionalidade num cenário de cibersegurança em constante mudança.
SOLUÇÃO 2	Substituir toda a solução atual por outra, de diferente fabricante	Substituir completamente a solução atual por uma nova infraestrutura de outro fabricante implica um alto risco de interrupção operacional, pois exige uma adaptação completa da equipe, novos processos e uma longa curva de aprendizado. Essa alternativa é inviável para o Tribunal, que precisa de continuidade, integração e segurança na gestão de suas operações críticas. Uma substituição completa romperia com os padrões estabelecidos e resultaria em insegurança operacional e dificuldades de compatibilidade com a infraestrutura preexistente. Além disso, uma troca integral aumentaria o tempo de vulnerabilidade, pois a equipe levaria tempo para se adaptar ao novo sistema, expondo o ambiente a riscos de segurança justamente no período de transição. Portanto, essa opção não se alinha aos objetivos de padronização e estabilidade necessárias para a proteção integrada e eficiente do ambiente cibernético.
SOLUÇÃO 3	Expandir a infraestrutura com soluções de outros fabricantes	Expandir a infraestrutura atual com soluções de diferentes fabricantes cria um ambiente fragmentado, onde a falta de padronização entre os produtos dificulta a integração e o gerenciamento centralizado. Essa opção é inviável, pois compromete a interoperabilidade e a comunicação entre os sistemas, gerando falhas que aumentam a vulnerabilidade a ataques. A fragmentação resulta em um complexo de gerenciamento, dificultando a detecção de ameaças e a resposta ágil, fatores essenciais em um ambiente de segurança cibernética. Além disso, a multiplicidade de fornecedores e de padrões de segurança eleva os custos operacionais e reduz a eficácia das defesas, tornando mais difícil manter um suporte técnico coeso e eficiente. A introdução de soluções de diferentes fabricantes traria riscos de incompatibilidade e perda de funcionalidades críticas, inviabilizando a proteção integrada necessária para a segurança e a eficiência operacional do Tribunal.

5.2. Cálculo dos Custos Totais de Propriedade (Total Cost Ownership - TCO) das soluções viáveis

5.2.1. O Custo Total de Propriedade (TCO, sigla em inglês para Total Cost of Ownership) é um conceito utilizado para avaliar o custo total de uma solução tecnológica ao longo de sua vida útil. Ele engloba não apenas o custo de aquisição da solução em si, mas também os custos associados à sua implementação, operação, manutenção e eventual substituição, durante o ciclo de vida da solução.

5.2.2. O primeiro aspecto para se definir o Custo Total de Propriedade está na definição do ciclo de vida do objeto.

5.3 Ciclo de vida do objeto

5.3.1. O Ciclo de Vida de uma solução de cibersegurança abrange todas as fases necessárias à sua implementação e operação, desde o planejamento inicial até uma eventual descontinuidade. Este ciclo contempla o desenvolvimento, a implantação, o crescimento no uso e, por fim, a transição ou retirada da solução. Cada etapa exige ajustes na estratégia de contratação e gerenciamento, garantindo que a solução acompanhe a evolução das demandas de segurança ao longo do tempo.

5.3.2. Embora o ciclo de vida de uma solução envolva várias etapas, a análise deste estudo prioriza as fases mais críticas para o sucesso da contratação, especialmente no que tange à disponibilização inicial das licenças e das permissões de uso, passando por uma execução segura e eficiente desde o início do contrato. Logo, vamos

desconsiderar as etapas iniciais relativas ao seu desenvolvimento e criação.

5.3.3. As etapas seguintes incluem a instalação e configuração, a adequação às necessidades do Tribunal, a execução de testes específicos e o suporte contínuo durante a duração do contrato. Este ciclo também envolve monitoramento proativo, aprimoramentos e finalização ordenada para garantir que o encerramento da vigência ocorra de forma estruturada, mantendo os benefícios alcançados e possibilitando uma transição suave para futuras contratações.

5.3.4. Durante todo o período contratual, a solução deve garantir plena operacionalidade e desempenho, com todas as funcionalidades críticas habilitadas para garantir que os objetivos de segurança e proteção cibernética do Tribunal sejam atendidos de maneira constante e eficaz.

5.3.5. É indispensável observar que toda contratação tem um período determinado. Ao término do contrato, é necessário avaliar pontos cruciais, como o estabelecimento de novos requisitos que possam melhorar o desempenho, além da análise sobre a possível substituição da solução ou atualização tecnológica caso haja avanços inovadores em metodologias e funcionalidades que possam ampliar a eficiência e a eficiência segurança na próxima vigência contratual.

- 5.4. Considerações:**
- 5.4.1. O TCO leva em consideração diversos aspectos, tais como:
- Custo de contratação (aquisição ou serviços);
 - Implantação e integração;
 - Custos operacionais;
 - Custos de manutenção;
 - Custos de recursos humanos especializados; e
 - Custos de atualização.

5.5. TCO – Memória de Cálculo

5.5.1. Conforme descrito neste estudo técnico, a equipe responsável pelo planejamento da contratação não encontrou nenhum projeto análogo no âmbito da Administração Pública que tenha adotado um modelo capaz de atender às necessidades e requisitos previamente delineados neste documento.

5.5.2. Podem até existir necessidades similares, conforme demonstrado, mas ainda não se materializaram sob a forma de uma contratação.

5.5.3. Diante disso, para atender a essa demanda, a equipe de planejamento da contratação realizou uma busca no mercado, envolvendo empresas do setor e potenciais fornecedores do objeto. A solicitação concentrou suas buscas em empresas que já forneceram para entes públicos.

5.5.4. Nas solicitações, constam pedidos dos seguintes dados, de acordo com as orientações exaradas junto ao Acórdão n. 1.432/2024 - TCU - Plenário:

5.5.4.1. Dados da empresa, como razão social, CNPJ, endereço completo, telefone e endereço de e-mail;

5.5.4.2. Dados do representante legal, como nome completo, CPF, cargo, telefone e endereço eletrônico;

5.5.4.3. Detalhamento da solução conforme quadro estimado;

5.5.4.4. Informações quanto ao fabricante, nome da solução, versão, part number ou qualquer outra informação que permita identificar a solução que serviu de base para a estimativa dos custos.

5.5.4.5. Esse levantamento foi feito em cotações de preços que possibilitaram a elaboração do quadro apresentado a seguir.

5.5.4.6. Total Cost of Ownership - TCO

5.5.5.6.1. Considerando os termos dispostos no art. 107 da Lei n. 14.133/2021 “Art. 107. Os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes”, criamos uma projeção dos custos obtidos, para o período de 5 (cinco) anos. Os quadros a seguir demonstram, com base nas contratações públicas encontradas, o valor médio unitário para itens que compõe os Grupos 1 e 2, objeto da contratação.

			CONTRATOS							MÉDIA VALOR UNITÁRIO
GRUPO 1	ITEM	DESCRIÇÃO	CTO TRT8 N° 55/2022	CTO TJ-PA N° 029/2023	PE 54/2024 MPDFT	CTO No 37 / 2023 TRE-ES	PE 759/2023 DATAPREV	ATA RP TSE N° 14/2024	CTO TRE-RR N° 65/2023	
	1	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Externos - Tenable.IO WAS, para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo o serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	R\$ 1.150,00	R\$ 1.150,00	---	---	---	---	---	R\$ 1.150,00
	2	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Internos - Tenable Security Center (SC+), para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo o serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	R\$ 1.115,00	R\$ 1.115,00	R\$ 263,00	R\$ 582,00	R\$ 188,00	---	---	R\$ 652,60

3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 24 horas de duração.	R\$ 86.000,00	R\$ 86.000,00	---	---	---	R\$ 23.220,00	R\$ 13.800,00	R\$ 18.510,00
---	---	---------------	---------------	-----	-----	-----	---------------	---------------	---------------

		CONTRATOS								
GRUPO 2	ITEM	DESCRIÇÃO	ATA RP TSE Nº 14/2024	CTO Nº 4/2024 TCE-RO	CTO TRT8 Nº 56/2022	CTO TJ-PA Nº 029/2023	CTO TRE-RR Nº 65/2023	CTO 191/2023	PE SRP 5/2024 - PRODEPA	MÉDIA VALOR UNITÁRIO
	4	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable.io Web Application Scanning (WAS) para a subscrição do licenciamento Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.					R\$ 522,00		R\$ 2.221,00	R\$ 1.371,50
	5	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable Security Center (SC+) para a subscrição do licenciamento do software Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	R\$ 995,00				R\$ 906,37		R\$ 2.320,00	R\$ 1.407,12
	6	Contratação da subscrição do licenciamento do software de Gerenciamento de Exposição Cibernética Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	R\$ 1.330,00					R\$ 778,99	R\$ 2.320,00	R\$ 1.330,00
	7	Serviço de Instalação, configuração e migração do ambiente atual.	R\$ 43.445,00				R\$ 37.900,00			R\$ 40.672,50
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	R\$ 23.220,00	R\$ 4.000,00		R\$ 86.000,00	R\$ 13.800,00			R\$ 31.755,00
	9	Serviço de Operação Assistida e apoio operacional, pelo período de 60 (sessenta) meses, sob demanda.	R\$ 99.311,00		R\$ 300.000,00					R\$ 199.655,50

5.6. Metodologia Adotada

- 5.6.1. A adoção da média como método para a estimativa de preços é respaldada por uma análise cuidadosa das contratações públicas juntadas para a análise deste ETP. A primeira justificativa para evitar o uso da mediana e do menor preço reside na baixa dispersão observada entre os valores apresentados. Quando as cotações são próximas entre si, a média se torna uma representação mais fiel do valor de mercado do item em questão, evitando distorções que poderiam surgir ao considerar valores extremos. A utilização da mediana, embora útil em alguns contextos, pode não refletir a realidade do mercado quando a variação é limitada, já que ela se concentra em um ponto central que pode não ser representativa da maioria das ofertas.
- 5.6.2. Além disso, o uso do menor preço pode levar a decisões que priorizem a economia imediata em detrimento da qualidade e da eficiência dos serviços ou produtos adquiridos. Essa abordagem pode resultar em contratações que não atendam às expectativas ou que excluam revisões e substituições mais frequentes, gerando custos adicionais ao longo do tempo. Assim, a escolha da média promove uma análise mais equilibrada, que considera a totalidade das propostas e permite uma avaliação mais ampla da competitividade entre os fornecedores.
- 5.6.3. Portanto, a média não reflete apenas uma melhor representatividade dos preços praticados no mercado, mas também garante que a decisão de compra seja fundamentada em uma perspectiva que valoriza tanto a qualidade quanto a previsões financeiras. Com essa abordagem, a administração pública pode garantir que os recursos sejam utilizados de maneira eficiente, resultando em contratações que atendam às necessidades institucionais e que se alinhem com as melhores práticas de gestão. Essa metodologia, portanto, é fundamental para a realização de uma contratação responsável e eficaz.
- 5.6.4. Cumpre salientar que a estimativa de preços de mercado (definitiva) deve ser realizada pela unidade competente, como o apoio do integrante técnico, de acordo com a Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, abrangendo, inclusive, consulta direta a fornecedores e outras fontes recomendadas. O levantamento demonstrado anteriormente, assim como aquele demonstrado no item 8. **ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO**, tem o objetivo de servir de parâmetro estimativo do TCO e valor da contratação para efeito de análise do ETP.

5.7. Mapa comparativo dos custos totais de propriedade (TCO) (OPCIONAL)

- 5.7.1. Não se aplica, uma vez que apenas um cenário se mostrou viável.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO A SER CONTRATADA (descrição/especificação da solução escolhida)

Fundamentação: A descrição da solução como um todo deverá indicar a solução escolhida e conter, de forma detalhada, motivada e justificada, o quantitativo de bens e serviços necessários para a sua composição, considerado todo o ciclo de vida do objeto, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso (inciso VII do § 1º do art. 18 da Lei 14.133/2021).

- 6.1. LICENCIAMENTO PARA SOLUÇÃO DE ANÁLISE DINÂMICA EM APLICAÇÕES WEB, PELO PERÍODO DE 60 MESES (TENABLE.IO WAS)**
- 6.1.1. Características Gerais
- 6.1.1.1. A solução deve ser licenciada pelo número aplicações por FQDN (Fully Qualified Domain Name);
- 6.1.1.2. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

- 6.1.1.2.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.
- 6.1.1.3. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com aplicações terceiras.
- 6.1.1.4. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;
- 6.1.1.5. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);
- 6.1.1.6. O escaneamento para as aplicações expostas, deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 6.1.1.7. Os scanners on premises e em nuvem deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 6.1.1.8. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
- 6.1.1.9. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
- 6.1.1.10. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
- 6.1.1.11. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);
- 6.1.1.12. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
- 6.1.1.13. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;
- 6.1.1.14. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
- 6.1.1.15. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
- 6.1.1.16. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;
- 6.1.1.17. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;
- 6.1.1.18. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;
- 6.1.2. Dos requisitos e relatórios e painéis gerenciais
- 6.1.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- 6.1.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 6.1.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 6.1.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;
- 6.1.2.5. A solução deve permitir a customização de dashboards/relatórios;
- 6.1.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 6.1.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 6.1.2.8. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 6.1.2.9. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 6.1.2.10. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 6.1.2.11. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 6.1.3. Funcionalidades de Análise Dinâmica de vulnerabilidades de Aplicações Web
- 6.1.3.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 6.1.3.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 6.1.3.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);
- 6.1.3.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 6.1.3.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- 6.1.3.6. A solução deve possuir templates prontos de varreduras entre simples e extensos;
- 6.1.3.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 6.1.3.8. Cookies, Headers, Formulários e Links;
- 6.1.3.9. Nomes e valores de parâmetros da aplicação;
- 6.1.3.10. Elementos JSON e XML;
- 6.1.3.11. Elementos DOM;
- 6.1.3.12. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 6.1.3.13. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
- 6.1.3.14. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 6.1.3.15. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 6.1.3.16. A solução deve instituir no mínimo os seguintes limites:
- 6.1.3.17. Número máximo de URLs para crawl e navegação;
- 6.1.3.18. Número máximo de diretórios para varreduras;
- 6.1.3.19. Número máximo de elementos DOM;
- 6.1.3.20. Tamanho máximo de respostas;
- 6.1.3.21. Limite de requisições de redirecionamentos;
- 6.1.3.22. Tempo máximo para a varredura;
- 6.1.3.23. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
- 6.1.3.24. Número máximo de requisições HTTP por segundo;
- 6.1.3.25. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
- 6.1.3.26. Limite em segundos para timeout de requisições de rede;
- 6.1.3.27. Número máximo de timeouts antes que a varredura seja abortada;
- 6.1.3.28. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 6.1.3.29. A solução deve enviar notificações através de no mínimo E-mail e SMS;

- 6.1.3.30. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
- 6.1.3.31. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 6.1.3.32. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 6.1.3.33. A solução deve ser compatível com avaliação de web services REST e SOAP;
- 6.1.3.34. Deverá suportar no mínimo os seguintes esquemas de autenticação:
- 6.1.3.35. Autenticação básica (digest);
- 6.1.3.36. NTLM;
- 6.1.3.37. Form de login;
- 6.1.3.38. Autenticação de Cookies;
- 6.1.3.39. Autenticação através de Selenium;
- 6.1.3.40. Autenticação através de Bearer;
- 6.1.3.41. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;
- 6.1.3.42. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
- 6.1.3.43. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 6.1.3.44. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- 6.1.3.45. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 6.1.3.46. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
- 6.1.3.47. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
- 6.1.3.48. Payload injetado;
- 6.1.3.49. Evidência em forma de resposta da aplicação;
- 6.1.3.50. Detalhes da requisição HTTP;
- 6.1.3.51. Detalhes da resposta HTTP;
- 6.1.3.52. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
- 6.1.3.53. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
- 6.1.3.54. A solução deve possuir suporte a varreduras de componentes para no mínimo:
- 6.1.3.55. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

6.2. LICENCIAMENTO DE PLATAFORMA DE GESTÃO DE VULNERABILIDADES E AUDITORIA DE CONFIGURAÇÕES DE ATIVOS DE REDE, PELO PERÍODO DE 60 MESES (TENABLE.SC)

6.2.1. CARACTERÍSTICAS GERAIS

- 6.2.1.1. A solução deve ser licenciada para realizar:
 - 6.2.1.1.1. varreduras (scans) de vulnerabilidades;
 - 6.2.1.1.2. avaliação de configuração e conformidade (baseline e compliance);
 - 6.2.1.1.3. varreduras em ambientes Windows e Linux;
 - 6.2.1.1.4. detecção de hot fix, service pack, peer to peer, registros e portas de serviço habilitadas.
- 6.2.1.2. A solução proposta poderá ser disponibilizada em uma arquitetura em nuvem e/ou on-premise
- 6.2.1.3. Caso a solução seja em nuvem, obrigatoriamente seus dados e metadados deverão ser tratados em território nacional, conforme recomendação e instrução normativa do gabinete de segurança da informação: IN 05 de 31 de agosto de 2021.
- 6.2.1.4. A solução deve fazer parte do catálogo de produtos comercializados pelo fabricante e nenhum de seus componentes poderá apresentar indicação de: End-of-Support, End-of-Sales ou End-of-Life até a data da publicação do Edital.
 - 6.2.1.4.1. A solução não deverá constar em listas dos respectivos fabricantes que indiquem que não serão mais desenvolvidos, atualizados, suportados ou comercializados durante a vigência do contrato.
- 6.2.1.5. Caso a solução seja on-premise, os componentes de software que integram o ambiente da solução serão instalados em máquinas virtuais oferecidas pela contratante e deverão ser compatíveis com os virtualizadores: VMware, Microsoft Hyper-V ou XenServer-Citrix.
 - 6.2.1.5.1. Cada máquina virtual oferecida pela contratante para a solução será limitada, em sua totalidade, a até 16 vCPUs, 64 GB de memória RAM e 2 TB de armazenamento (aceita-se documentação).
- 6.2.1.6. A solução deverá utilizar TLS v1.2 ou superior para comunicação entre a console de gerenciamento e os dispositivos de varredura (scanners)
- 6.2.1.7. A ferramenta deve ser licenciada para realizar a varredura (scan) em no mínimo XXXX IPs internos.
 - 6.2.1.7.1. Estes objetos podem ser: dispositivos de rede (IP), FQDN, Imagens de Containers e controladores de domínio.
- 6.2.1.8. As ferramentas de varreduras (scanners) de rede deverão ser instaladas nas dependências da contratante e deverão possuir compatibilidade para instalação com, no mínimo, um dos seguintes sistemas operacionais servidores a serem fornecidos pela contratante:
 - 6.2.1.8.1. Windows Server 2019;
 - 6.2.1.8.2. Debian 8 e superiores ;
 - 6.2.1.8.3. Debian 10;
 - 6.2.1.8.4. Red Hat Enterprise Linux Server 5.0 (64 bits) ou superiores;
 - 6.2.1.8.5. Red Hat Enterprise Linux Server 7;
 - 6.2.1.8.6. Linux Ubuntu 18.04 ou 20.04 ou superiores;
 - 6.2.1.8.7. Virtual Appliance com sistema operacional com o devido hardening para execução da solução.
- 6.2.1.9. Se a ferramenta fizer o uso de banco de dados proprietários como Oracle, SQL Server entre outros, as licenças do banco de dados deverão ser fornecidas com a solução.
- 6.2.1.10. A solução deve ser licenciada para no mínimo 12 scanners ativos.
 - 6.2.1.10.1. A contabilização das licenças será considerada por IPs , Usuários Ativos no Microsoft Active Directory , FQDN únicos.
 - 6.2.1.10.2. Ter opção para desvincular licenças atreladas aos diferentes tipos de ativos conforme necessidade do contratante.

- 6.2.1.10.3. Não deve ter nenhum tipo de limite vinculado a licenciamento para realizar escaneamentos simultâneos (além do limite operacional dos equipamentos).
- 6.2.1.10.4. Não deverá ser computado às licenças o simples discovery ou técnicas passivas de detecção de ativos de TI.
- 6.2.1.10.5. A contabilização da licença deve ser efetivada no momento em que é realizado o scanner completo.
- 6.2.1.10.6. A gerência centralizada deve demonstrar os Ativos de TI vinculados ao licenciamento da solução, com no mínimo a data de ativação dos mesmos. A desvinculação entre Ativo de TI/licença deve acontecer no prazo máximo de 90 dias.
- 6.2.1.11. Ser capaz de passivamente detectar ativos tecnológicos de diferentes tipos como por exemplo, servidores, endpoints, aplicações web, máquinas virtuais, IoT.
- 6.2.1.12. Efetuar a coleta passiva, no mínimo:
 - 6.2.1.12.1. Por meio do recebimento de tráfego de rede via SPAN port ou TAP, ou;
 - 6.2.1.12.2. Por meio de integração com outras fontes de evento como DHCP, LDAP / AD ou DNS.
 - 6.2.1.12.3. Identificar vulnerabilidades através da análise passiva.
 - 6.2.1.12.4. Ser compatível com Ipv4, Ipv6, TCP e UDP.
- 6.2.1.13. A ferramenta deve funcionar sem a necessidade de agentes instalados nos servidores que serão alvo de análise de vulnerabilidade.
- 6.2.1.14. A ferramenta deve permitir a integração com Microsoft Active Directory para a autenticação de usuários.
- 6.2.1.15. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
- 6.2.1.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
- 6.2.1.17. A base de vulnerabilidades conhecidas deve ser atualizada automaticamente durante a vigência do contrato sem intervenção de administrador.
 - 6.2.1.17.1. Todas as vezes que a base de vulnerabilidade for atualizada automaticamente, um alerta deve ser emitido para o administrador.
- 6.2.1.17.2. A solução deve receber a atualização automática de novas versões do produto, via internet, inclusive através de proxy.
- 6.2.1.18. A ferramenta deve ser capaz de:
 - 6.2.1.18.1. Utilizar listas de vulnerabilidades da SANS/FBI e IAVA (Information Assurance Vulnerability Alert) ou base própria baseada nas informações de diversos CERTs mundiais, fabricantes, Dark Web, dentre outros;
 - 6.2.1.18.2. integrar-se com base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
 - 6.2.1.18.3. ser capaz de identificar no mínimo 51.000 CVE (Common Vulnerabilities and Exposures);
 - 6.2.1.18.4. utilizar identificadores CVE (Common Vulnerabilities and Exposures) associados às vulnerabilidades identificadas para geração de relatórios, gerenciamento de riscos e mitigação de ameaças.
- 6.2.1.19. A ferramenta deve permitir a autenticação:
 - 6.2.1.19.1. com certificados SSL;
 - 6.2.1.19.2. via API REST.
- 6.2.1.20. A ferramenta deve fornecer em instalação padrão, diferentes dashboards para análise das informações coletadas em varreduras.
- 6.2.1.21. A ferramenta deve possibilitar, por meio da console central de gerenciamento, o método de varredura (scan) ativo.
- 6.2.1.22. A ferramenta deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv2 score.
- 6.2.1.23. A ferramenta deve possuir um sistema de pontuação e priorização das vulnerabilidades.
 - 6.2.1.23.1. O algoritmo de priorização deve analisar vulnerabilidades presentes na National Vulnerability Database (NVD).
- 6.2.1.24. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
 - 6.2.1.24.1. CVSSv3 Impact Score;
 - 6.2.1.24.2. Idade da vulnerabilidade;
 - 6.2.1.24.3. Número de produtos afetados pela vulnerabilidade;
- 6.2.1.25. A ferramenta deve permitir integração via API REST para automação de processos com aplicações terceiras.
- 6.2.1.26. A ferramenta deve possuir sistema de alertas com ações definidas para cada alerta, entre elas:
 - 6.2.1.26.1. Gerar relatório pré-definido com base nas condições de um alerta;
 - 6.2.1.26.2. Envio de e-mail com base nas condições de um alerta;
 - 6.2.1.26.3. Envio de mensagem syslog com base nas condições de um alerta;
 - 6.2.1.26.4. Iniciar varredura (scan) sob demanda com base em condições pré-definidas;
 - 6.2.1.26.5. Criação de Ticket no sistema de chamados interno da solução.
- 6.2.1.27. A ferramenta deve possuir a funcionalidade de discovery para a descoberta automática de computadores, servidores e ativos de rede.
 - 1.27.1. A ferramenta deve ser capaz de identificar novos hosts no ambiente sem a necessidade de execução manual de uma varredura pelo administrador, devendo ser possível desempenhar essa funcionalidade através do agendamento prévio da ação de discovery.
- 6.2.1.28. A ferramenta deve permitir determinar quais portas estão abertas em um determinado ativo após a realização de um scan (agendado ou realizado imediatamente).
- 6.2.1.29. A ferramenta deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
 - 6.2.1.29.1. Aplicações;
 - 6.2.1.29.2. Bancos de dados;
 - 6.2.1.29.3. Dispositivos de rede;
 - 6.2.1.29.4. Hypervisors;
 - 6.2.1.29.5. Servidores.
- 6.2.1.30. A ferramenta deve oferecer capacidade de configuração dinâmica de grupos de ativos através de, no mínimo, as seguintes características:
 - 6.2.1.30.1. Sistema Operacional;
 - 6.2.1.30.2. Endereço IP;
 - 6.2.1.30.3. Nome DNS;
 - 6.2.1.30.4. Nome NetBIOS;
 - 6.2.1.30.5. NetBIOS Workgroup;
 - 6.2.1.30.6. Endereço MAC;
 - 6.2.1.30.7. SSH Fingerprint;
 - 6.2.1.30.8. Porta TCP;

- 6.2.1.30.9. Porta UDP;
- 6.2.1.30.10. Dias desde a descoberta do ativo;
- 6.2.1.30.11. Exploit disponível;
- 6.2.1.30.12. XREF;
- 6.2.1.30.13. Hosts com Antivirus Desatualizado;
- 6.2.1.30.14. Host com Browsers específicos (Opera, Chrome, Safari, Firefox);
- 6.2.1.30.15. Hosts com Browser TOR instalado;
- 6.2.1.30.16. Hosts com software VOIP instalados;
- 6.2.1.30.17. Hosts com clientes SQL instalados.
- 6.2.1.31. A ferramenta deve permitir a configuração de políticas de varreduras diferentes a serem aplicadas a grupos de servidores específicos.
- 6.2.1.32. O acesso à console de gerenciamento deve ser através do protocolo HTTPS e com interface via navegador web.
- 6.2.1.33. A console de gerenciamento deve ser compatível com os seguintes navegadores web em suas versões:
 - 6.2.1.33.1. Mozilla Firefox 74.0 e superiores (aceita-se documentação, exceto para a versão mais recente);
 - 6.2.1.33.1.1 Mozilla Firefox versão mais recente;
 - 6.2.1.33.2. Microsoft Internet Explorer 10 e superiores;
 - 6.2.1.33.3. Google Chrome 81.0.4044.92 e superiores
 - 6.2.1.33.3.1 Google Chrome versão mais recente;
 - 6.2.1.33.4. Safari 11.1.2 e superiores;
 - 6.2.1.33.5. Microsoft Edge 80.0.361.109 e superiores
 - 6.2.1.33.5.1 Microsoft Edge versão mais recente.
- 6.2.1.34. A ferramenta deve permitir o cadastramento dos ativos alvo dos escaneamentos por meio de interface web e por API REST.
- 6.2.1.35. A ferramenta deve indicar o procedimento para a correção ou mitigação das vulnerabilidades encontradas.
- 6.2.1.36. A ferramenta deve indicar a criticidade e o risco associado a cada vulnerabilidade encontrada.
- 6.2.1.37. A ferramenta deve possuir sistema para a sinalização de falsos positivos.
- 6.2.1.38. A ferramenta deve possuir controle de acesso baseado em perfis de usuário.
 - 6.2.1.38.1. A ferramenta deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência.
- 6.2.1.39. A ferramenta deve ser aderente às melhores práticas previstas nos principais frameworks de mercado, atendendo a pelo menos 3 dos 5 itens a seguir:
 - 6.2.1.39.1. SANS 20 Critical Security Controls;
 - 6.2.1.39.2. CIS Benchmark L1 e L2;
 - 6.2.1.39.3. ISO 27000;
 - 6.2.1.39.4. NIST Cybersecurity Framework;
 - 6.2.1.39.5. NERC CIP.
- 6.2.1.40. A ferramenta deve permitir a configuração de usuários com permissão somente de leitura e com permissões administrativas.
- 6.2.1.41. A ferramenta deve suportar o uso de IPv4 e IPv6 para o seu funcionamento.
- 6.2.1.42. A ferramenta deve suportar sincronismo de horário através do protocolo NTP (Network Time Protocol).
- 6.2.1.43. A comunicação da console de gerência com os scanners de rede deve ser criptografada.
- 6.2.1.44. A solução adotada pela CONTRATADA deverá ser capaz de verificar vulnerabilidades em gerenciadores de virtualização como Hyper-V e VMware.
- 6.2.1.45. A solução adotada deverá apresentar capacidade para análise de vulnerabilidades no Active Directory (AD).
- 6.2.1.46. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;
- 6.2.1.47. A solução deve possuir ações preventivas de hardening para o Active Directory;
- 6.2.1.48. A solução deve identificar ataque específicos para a estrutura do Active Directory;
- 6.2.1.49. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 6.2.1.50. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
- 6.2.1.51. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 6.2.1.52. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 6.2.1.53. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
- 6.2.1.54. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 6.2.1.55. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
- 6.2.1.56. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 6.2.1.57. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 6.2.1.58. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 6.2.1.59. A solução deve realizar alterações no Active Directory, seus objetos e atributos;
- 6.2.1.60. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 6.2.1.61. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 6.2.1.62. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 6.2.1.63. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 6.2.1.64. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
 - 6.2.1.64.1. Não depender de agentes ou sensores para coleta de informações do AD;
 - 6.2.1.64.2. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;
 - 6.2.1.64.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
- 6.2.1.65. A solução deve possuir capacidade de receber atualizações em horários programados.
- 6.2.1.66. Todo o tráfego de informações entre a Solução e a Internet deve ser criptografado.

- 6.2.1.67. A solução deve suportar vários scanners conectados simultaneamente. Deverá a CONTRATADA utilizar quantos scanners sejam necessários para atender o sizing de itens de configuração especificados neste Termo de Referência, sem que haja necessidade de licenciamento adicional.
- 6.2.1.68. A solução deve possuir capacidade de atualizar os scanners automaticamente.
- 6.2.1.69. A solução deve possuir em sua base de vulnerabilidades, para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, TEMPORAL e ENVIRONMENTAL, a partir da versão 2 e superior, referência (CVE, CWE, BugTraQ ou outra fonte), solução e link para o download da correção (se aplicável), contramedidas (se aplicável), informação e fonte de exploit.
- 6.2.1.70. A solução deve ser entregue em sua última versão disponível e contar com suporte integral durante toda a vigência do contrato.
- 6.2.1.71. A solução não poderá estar em versão beta.
- 6.2.1.72. A solução deve permitir varreduras por: endereço IP, faixa de IP, agrupamento de ativos, nome NetBIOS e CIDR Notation.
- 6.2.1.73. A solução deve possibilitar a integração com a solução de Cofre de Senhas do fabricante Senha Segura sendo permitida integração via API.
- 6.2.1.74. A solução deve permitir o cadastramento de credenciais utilizadas para escaneamento para que seja permitido o uso de tais credenciais para futuros escaneamentos, sem que o administrador da ferramenta saiba a senha destas credenciais.
- 6.2.2. VARREDURAS**
- 6.2.2.2.1. A ferramenta deve permitir scan manual (sob demanda) e scan agendado, programado para ser executado em determinado dia e horário via interface WEB e API REST.
- 6.2.2.2.2. A ferramenta deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia.
- 6.2.2.2.2.1. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, a varredura deve ser capaz de ser reiniciada de onde parou quando o período permitido se iniciar novamente.
- 6.2.2.2.3. A ferramenta deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede.
- 6.2.2.2.4. A ferramenta deve realizar varreduras em sistemas operacionais, em appliances físicos e virtuais, incluindo no mínimo:
- 6.2.2.2.4.1. Windows Server 2000 e superiores;
- 6.2.2.2.4.1.1 Windows Server 2008, 2012 e 2019;
- 6.2.2.2.4.2. Red Hat Enterprise Linux 5.0 Server e superiores;
- 6.2.2.2.4.2.1 Red Hat Enterprise Linux 7 Server;
- 6.2.2.2.4.3. AIX 6.1 e superiores ;
- 6.2.2.2.4.4. SUN Solaris 9.0 e superiores ;
- 6.2.2.2.4.5. Debian ;
- 6.2.2.2.4.6. CentOS 5 e superiores ;
- 6.2.2.2.4.7. Oracle Linux 5.0 e superiores ;
- 6.2.2.2.4.8. Linux Ubuntu 12.04 e superior .
- 6.2.2.2.5. A ferramenta deve realizar varreduras em aplicações que utilizem os principais protocolos de rede, tais como
- 6.2.2.2.5.1. HTTP;
- 6.2.2.2.5.2. HTTPS;
- 6.2.2.2.5.3. SMTP;
- 6.2.2.2.5.4. Telnet;
- 6.2.2.2.5.5. FTP;
- 6.2.2.2.5.6. SFTP;
- 6.2.2.2.5.7. SSH;
- 6.2.2.2.5.8. NTP;
- 6.2.2.2.5.9. RDP;
- 6.2.2.2.5.10. SNMP;
- 6.2.2.2.5.11. POP3;
- 6.2.2.2.5.12. IMAP;
- 6.2.2.2.5.13. SIP;
- 6.2.2.2.5.14. DNS;
- 6.2.2.2.5.15. LDAP.
- 6.2.2.2.6. A ferramenta deve realizar varreduras em banco de dados incluindo, no mínimo:
- 6.2.2.2.6.1. Oracle Database Enterprise Edition – versão 10.2.0.1.0 e superiores;
- 6.2.2.2.6.1.1 Oracle Database Enterprise Edition – versão 18.0.0.0.0.
- 6.2.2.2.6.2. Microsoft SQL Server – versão 2000 e superiores;
- 6.2.2.2.6.2.1 Microsoft SQL Server – versão 2012, 2014 e 2017.
- 6.2.2.2.6.3. MySQL Server – versão 5.0 e superiores;
- 6.2.2.2.6.3.1 MySQL Server – versão 5.6 e 8.0.
- 6.2.2.2.6.4. PostgreSQL Server – versão 9.0 e superiores;
- 6.2.2.2.6.4.1 PostgreSQL Server – versão 9.6 e 11.3.
- 6.2.2.2.6.5. MongoDB – versão 2.0 e superiores;
- 6.2.2.2.6.5.1 MongoDB - versão 3.4 e 4.0.
- 6.2.2.2.7. A ferramenta deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.
- 6.2.2.2.8. A ferramenta deve ser configurável para permitir a otimização das configurações de varredura.
- 6.2.2.2.9. A ferramenta deve fornecer a capacidade de escalar privilégios nos ativos que serão varridos, desde o acesso de usuário padrão até acesso administrativo.
- 6.2.2.2.10. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux.
- 6.2.3. AUDITORIA DE CONFIGURAÇÃO**
- 6.2.3.1. A ferramenta deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino.
- 6.2.3.2. A ferramenta deve fornecer benchmarks de auditoria de segurança e configuração.

6.2.3.3. A ferramenta deve fornecer dashboards visuais, contendo as verificações e controles de segurança verificados com indicação de sucesso ou falha, com base nos principais frameworks de segurança reconhecidos pela indústria, tais como:

6.2.3.3.1. CIS Benchmark L1 e L2 .

6.2.3.4. A ferramenta deve fornecer auditoria de programas antivírus para a determinação da presença e do status de inicialização para no mínimo os seguintes produtos:

6.2.3.4.1. TrendMicro - Office Scan e Deep Security.;

6.2.3.4.2. McAfee VirusScan;

6.2.3.4.3. Microsoft Endpoint Protection;

6.2.3.4.4. Kaspersky;

6.2.3.4.5. Symantec - Endpoint Protection, Endpoint Security e Data Center Security.

6.2.3.5. A ferramenta deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para os sistemas operacionais abaixo:

6.2.3.5.1. Microsoft Windows ;

6.2.3.5.2. Linux .

6.2.4. RELATÓRIOS

6.2.4.1. A solução deve permitir a exportação de seus relatórios nos seguintes formatos: PDF e CSV ou PDF e XLS.

6.2.4.2. A ferramenta deve suportar o envio automático de relatórios para destinatários específicos através de e-mail.

6.2.4.3. A ferramenta deve possuir relatórios pré-definidos.

6.2.4.3.1. A solução deve possuir console própria de relatórios, com uma lista de relatórios prontos, com pelo menos 10 opções pré-definidas.

6.2.4.4. A ferramenta deve permitir a customização de relatórios.

6.2.4.4.1. A ferramenta deve permitir a customização do conteúdo de cada relatório;

6.2.4.4.2. A solução deve emitir relatório do tipo resumo gerencial, com possibilidade de seleção das informações que irão compor o mesmo.

6.2.4.5. A ferramenta deve ser capaz de executar relatórios manuais (sob demanda) e periódicos de acordo com a frequência (agendamento) estabelecida pelo administrador.

6.2.4.6. A ferramenta deve permitir definir a frequência (agendamento) na geração dos relatórios para no mínimo:

6.2.4.6.1. Diário;

6.2.4.6.2. Mensal;

6.2.4.6.3. Semanal.

6.2.4.7. A ferramenta deve possibilitar a criação de relatórios baseado nos seguintes alvos:

6.2.4.7.1. Todos os ativos;

6.2.4.7.2. Grupo de ativos;

6.2.4.7.3. Ativos específicos.

6.2.4.8. A ferramenta deve gerar relatórios agrupando as informações por:

6.2.4.8.1. Vulnerabilidade;

6.2.4.8.2. Criticidade;

6.2.4.8.3. Ativo;

6.2.4.8.4. Risco;

6.2.4.8.5. Aplicação web.

6.2.4.9. Os relatórios devem conter informações sobre:

6.2.4.9.1. As vulnerabilidades;

6.2.4.9.2. Se existe exploit disponível;

6.2.4.9.3. Informações do ativo;

6.2.4.9.4. Remediação.

6.2.4.10. A solução deve emitir relatórios de vulnerabilidades com os resultados encontrados nas varreduras efetuadas no ambiente da contratante.

6.3. PLATAFORMA SAAS DE GERENCIAMENTO DE EXPOSIÇÃO COM O SERVIÇO DE IMPLANTAÇÃO E TAMBÉM O DE GARANTIA DOS EQUIPAMENTOS E/OU SOFTWARES PELO PERÍODO DE 60 MESES.

6.3.1. Módulo de Gestão de Vulnerabilidade e Auditoria de Configuração de ativos.

6.3.1.1. Características gerais

6.3.1.1.1. A solução deve realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance);

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

6.3.1.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

6.3.1.1.4. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (assets);

6.3.1.1.5. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

6.3.1.1.5.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

6.3.1.1.6. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com aplicações terceiras.

6.3.1.1.7. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP;

6.3.1.1.8. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

6.3.1.1.9. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

6.3.1.1.9.1. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

6.3.1.1.10. A solução deve permitir o agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

6.3.1.1.10.1. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

- 6.3.1.1.10.2. O escaneamento para os dispositivos expostos deve ser realizado através de SCANS (ENGINE) do próprio fabricante alocados no Brasil;
- 6.3.1.1.10.3. Os scanners e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;
- 6.3.1.1.10.4. O acesso a console de gerenciamento deve ser fornecido para pelo menos 10 usuários simultâneos;
- 6.3.1.1.10.5. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);
- 6.3.1.1.10.6. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;
- 6.3.1.1.10.7. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);
- 6.3.1.1.10.8. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;
- 6.3.1.1.10.9. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;
- 6.3.1.1.10.10. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;
- 6.3.1.1.10.11. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;
- 6.3.1.1.10.12. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);
- 6.3.1.1.10.13. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;
- 6.3.1.1.10.14. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;
- 6.3.1.1.10.15. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;
- 6.3.1.1.10.16. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:
 - 6.3.1.1.10.16.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

6.3.1.2. Relatórios e painéis gerenciais

- 6.3.1.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;
- 6.3.1.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;
- 6.3.1.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;
- 6.3.1.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;
- 6.3.1.2.5. A solução deve permitir a customização de dashboards/relatórios;
- 6.3.1.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas;
- 6.3.1.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;
- 6.3.1.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;
- 6.3.1.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
- 6.3.1.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;
- 6.3.1.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 6.3.1.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

6.3.1.3. Varreduras

- 6.3.1.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;
- 6.3.1.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;
- 6.3.1.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;
- 6.3.1.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;
- 6.3.1.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;
- 6.3.1.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
- 6.3.1.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
- 6.3.1.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:
 - 6.3.1.3.8.1. CyberArk;
 - 6.3.1.3.8.2. BeyondTrust;
 - 6.3.1.3.8.3. Thycotic;
 - 6.3.1.3.8.4. Centrify;
- 6.3.1.3.9. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;
- 6.3.1.3.10. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;
- 6.3.1.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
- 6.3.1.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:
 - 6.3.1.3.12.1. Cloud Services;
 - 6.3.1.3.12.2. Data Leakage;
 - 6.3.1.3.12.3. Database;
 - 6.3.1.3.12.4. IoT;
 - 6.3.1.3.12.5. Mobile Devices;
 - 6.3.1.3.12.6. Operating System;
 - 6.3.1.3.12.7. Peer-To-Peer;
 - 6.3.1.3.12.8. SCADA;
 - 6.3.1.3.12.9. Web Servers;
 - 6.3.1.3.12.10. Web Clients;

- 6.3.1.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;
- 6.3.1.3.14. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;
- 6.3.1.4. Análise e priorização de vulnerabilidades
 - 6.3.1.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;
 - 6.3.1.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:
 - 6.3.1.4.2.1. CVSS Impact Score;
 - 6.3.1.4.2.2. Idade da Vulnerabilidade;
 - 6.3.1.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;
 - 6.3.1.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;
 - 6.3.1.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;
 - 6.3.1.4.2.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;
 - 6.3.1.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;
 - 6.3.1.4.3. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;
- 6.3.1.5. Análise de Risco do Ambiente
 - 6.3.1.5.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
 - 6.3.1.5.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;
 - 6.3.1.5.3. Deve ser capaz de calcular a criticidade dos ativos da organização;
 - 6.3.1.5.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;
 - 6.3.1.5.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;
 - 6.3.1.5.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;
 - 6.3.1.5.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;
 - 6.3.1.5.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
 - 6.3.1.5.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);
 - 6.3.1.5.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
 - 6.3.1.5.11. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;
 - 6.3.1.5.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
 - 6.3.1.5.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
 - 6.3.1.5.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;
 - 6.3.1.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;
- 6.3.1.6. Gerenciamento da Análise de Ataques exploráveis
 - 6.3.1.6.1. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;
 - 6.3.1.6.2. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;
 - 6.3.1.6.3. Deve prover a evidência relacionada a descoberta do ataque;
 - 6.3.1.6.4. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;
 - 6.3.1.6.5. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;
 - 6.3.1.6.6. Deve prover quais ferramentas e possíveis malwares associados ao ataque;
 - 6.3.1.6.7. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;
 - 6.3.1.6.8. Deve disponibilizar uma biblioteca com 'Queries' para a busca de objetos no mínimo os seguintes segmentos:
 - 6.3.1.6.8.1. Rede;
 - 6.3.1.6.8.2. Endpoint;
 - 6.3.1.6.8.3. Active Directory;
 - 6.3.1.6.8.4. Permissão;
 - 6.3.1.6.8.5. Ransomware;
 - 6.3.1.6.8.6. Vetores;
 - 6.3.1.6.8.7. Credenciamento;
 - 6.3.1.6.9. Deve suportar no mínimo 90 técnicas de ataques;
 - 6.3.1.6.10. Deve permitir analisar, ao menos, os seguintes caminhos das superfícies de ataques:
 - 6.3.1.6.10.1. Aplicações WEB (DAST);
 - 6.3.1.6.10.2. Nuvem;
 - 6.3.1.6.10.3. Active Directory;
 - 6.3.1.6.10.4. Infraestrutura (Desktops, Servidores).
 - 6.3.1.6.11. Deve apresentar os resultados em forma ilustrativa (Dashboard).
 - 6.3.1.6.12. O Dashboard deve oferecer uma visão dos seus ativos vulneráveis considerando:
 - 6.3.1.6.12.1. Número de ativos críticos vulneráveis;
 - 6.3.1.6.12.2. Número de caminhos de ataque que levam a esses ativos críticos;
 - 6.3.1.6.12.3. Número de descobertas abertas e sua gravidade;

- 6.3.1.6.12.4. Matriz para visualizar caminhos com diferentes combinações de valores alvo;
- 6.3.1.6.12.5. Lista de tendências de caminhos de ataque.
- 6.3.1.6.13. Deve listar as diferenças entre os intervalos de tempo e mostrar uma seta direcional a fim de indicar se o valor aumentou ou diminuiu.
- 6.3.1.6.14. Deve permitir que o caminho de ataque leve a um ativo crítico.
- 6.3.1.6.15. Deve apresentar o número total alcançado de ativos críticos;
- 6.3.1.6.16. Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares.
- 6.3.1.6.17. Deve ser possível identificar o host suspeito;
- 6.3.1.6.18. Deve ser possível identificar o usuário suspeito;
- 6.3.1.6.19. Deve ser possível identificar o IP suspeito;
- 6.3.1.6.20. Deve permitir visualização em modo ilustrativo do caminho de ataque;
- 6.3.1.6.21. Deve ser possível identificar qual a técnica utilizada pelo atacante, tais como:
 - 6.3.1.6.21.1. Network Sniffing;
 - 6.3.1.6.21.2. LSASS Memory;
 - 6.3.1.6.21.3. Remote Desktop Protocol;
 - 6.3.1.6.21.4. Exploração de serviços remotos;
 - 6.3.1.6.21.5. System Services Discovery;
 - 6.3.1.6.21.6. Modificação da Política de Grupo;
 - 6.3.1.6.21.7. Mecanismo de Controle de Elevação de Abuso.
- 6.3.1.6.22. Deve permitir a comunicação com o framework MITRE ATT&CK ®.
- 6.3.1.6.23. Deve trazer o número de identificação MITRE ATT&CK para a descoberta;
- 6.3.1.6.24. A descoberta no MITRE ATT&CK deve abordar as seguintes ações:
 - 6.3.1.6.24.1. A técnica MITRE ATT&CK associada ao achado.
 - 6.3.1.6.24.2. A origem da descoberta.
 - 6.3.1.6.24.3. O alvo da descoberta.
 - 6.3.1.6.24.4. O status para indicar a ação tomada na descoberta, por exemplo, Em andamento.
- 6.3.1.6.25. Deve ser possível exportar uma descoberta como CSV.
- 6.3.1.6.26. Deve ser possível arquivar uma descoberta.
- 6.3.1.6.27. Deve ser possível ver o histórico do log da descoberta.
- 6.3.1.6.28. Deve permitir alterar o status do caminho de ataque descoberto para, pelo menos:
 - 6.3.1.6.28.1. Em Progresso;
 - 6.3.1.6.28.2. Em Revisão;
 - 6.3.1.6.28.3. Feito;
- 6.3.1.7. Descoberta de ativos
 - 6.3.1.7.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;
 - 6.3.1.7.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:
 - 6.3.1.7.2.1. Enumeração de Hosts;
 - 6.3.1.7.2.2. Identificação de Sistema Operacional (SO);
 - 6.3.1.7.2.3. Port Scan (Portas comuns);
 - 6.3.1.7.2.4. Port Scan (Todas as portas);
 - 6.3.1.7.2.5. Customizado;
 - 6.3.1.7.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;
 - 6.3.1.7.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:
 - 6.3.1.7.4.1. Descoberta de Host;
 - 6.3.1.7.4.2. Ping o host remoto;
 - 6.3.1.7.4.3. Usar descoberta rápida;
 - 6.3.1.7.4.4. Métodos de ping;
 - 6.3.1.7.4.4.1. ARP;
 - 6.3.1.7.4.4.2. TCP;
 - 6.3.1.7.4.4.3. ICMP;
 - 6.3.1.7.4.4.4. UDP;
 - 6.3.1.7.4.5. Escaneamento de descoberta de dispositivos de OT/SCADA;
 - 6.3.1.7.4.6. Escaneamento de descoberta em redes de impressora;
 - 6.3.1.7.4.7. Escaneamento em redes Novell;
 - 6.3.1.7.4.8. Tecnologia de Wake-on-LAN;
 - 6.3.1.7.5. Port Scanning;
 - 6.3.1.7.6. Portas;
 - 6.3.1.7.6.1. Considerar portas não escaneadas como fechadas;
 - 6.3.1.7.6.2. Range de portas a serem escaneadas;
 - 6.3.1.7.7. Enumerar Portas locais:
 - 6.3.1.7.7.1. SSH (netstat);
 - 6.3.1.7.7.2. WMI (netstat);
 - 6.3.1.7.7.3. SNMP;
 - 6.3.1.7.8. Descoberta de Serviços:

- 6.3.1.7.8.1. Sondar todas as portas para encontrar serviços;
- 6.3.1.7.8.2. Procurar por serviços baseado em SSL/TLS;
- 6.3.1.7.8.3. Enumerar todas as cifras SSL/TLS;
- 6.3.1.7.9. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na console de gerenciamento;
- 6.3.1.7.10. A solução deve descobrir passivamente quando um host é adicionado na rede;
- 6.3.1.8. Avaliação de vulnerabilidade
 - 6.3.1.8.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;
 - 6.3.1.8.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;
 - 6.3.1.8.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;
 - 6.3.1.8.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;
 - 6.3.1.8.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;
 - 6.3.1.8.6. A solução deve identificar vulnerabilidades específicas para o Active Directory com os seguintes padrões de verificação:
 - 6.3.1.8.6.1. Contas administrativas vulneráveis a Kerberoasting attack;
 - 6.3.1.8.6.2. Utilização de criptografia vulnerável com autenticação Kerberos;
 - 6.3.1.8.6.3. Contas com pré-autenticação do Kerberos desabilitada;
 - 6.3.1.8.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;
 - 6.3.1.8.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;
 - 6.3.1.8.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;
 - 6.3.1.8.6.7. Verificação de validade de chaves mestras “Kerberos KRBtgt”;
 - 6.3.1.8.6.8. Verificação de “SID History Injection”;
 - 6.3.1.8.6.9. Verificação de “Printer Bug Exploit”;
 - 6.3.1.8.6.10. Verificação de “Primary Group ID”;
 - 6.3.1.8.6.11. Verificação de usuários com Passwords em branco;
 - 6.3.1.8.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;
 - 6.3.1.8.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;
 - 6.3.1.8.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;
 - 6.3.1.8.10. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;
 - 6.3.1.8.11. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;
 - 6.3.1.8.11.1. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;
 - 6.3.1.8.12. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;
 - 6.3.1.8.13. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;
 - 6.3.1.8.14. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Trellic, etc;
 - 6.3.1.8.15. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);
 - 6.3.1.8.16. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;
 - 6.3.1.8.17. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);
 - 6.3.1.8.18. A solução deve possuir importação de arquivos .YARA;
 - 6.3.1.8.19. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;
- 6.3.1.9. Auditoria de Configuração
 - 6.3.1.9.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;
 - 6.3.1.9.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;
 - 6.3.1.9.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:
 - 6.3.1.9.3.1. Center for Internet Security Benchmarks (CIS);
 - 6.3.1.9.3.2. Defense Information Systems Agency (DISA) STIGs;
 - 6.3.1.9.3.3. Health Insurance Portability and Accountability Act (HIPAA);
 - 6.3.1.9.3.4. Payment Card Industry Data Security Standards (PCI DSS);
 - 6.3.1.9.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Trellic Endpoint Security, Microsoft Endpoint Protection e Kaspersky;
 - 6.3.1.9.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;
 - 6.3.1.9.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;
 - 6.3.1.9.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

6.3.2. Módulo de Análise Dinâmica de Vulnerabilidades para Aplicações Web

- 6.3.2.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 6.3.2.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 6.3.2.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

- 6.3.2.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 6.3.2.5. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;
- 6.3.2.6. A solução deve possuir templates prontos de varreduras entre simples e extensos;
- 6.3.2.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 6.3.2.7.1. Cookies, Headers, Formulários e Links;
 - 6.3.2.7.2. Nomes e valores de parâmetros da aplicação;
 - 6.3.2.7.3. Elementos JSON e XML;
 - 6.3.2.7.4. Elementos DOM;
- 6.3.2.8. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 6.3.2.9. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
- 6.3.2.10. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 6.3.2.11. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 6.3.2.12. A solução deve instituir no mínimo os seguintes limites:
- 6.3.2.12.1. Número máximo de URLs para crawl e navegação;
 - 6.3.2.12.2. Número máximo de diretórios para varreduras;
 - 6.3.2.12.3. Número máximo de elementos DOM;
 - 6.3.2.12.4. Tamanho máximo de respostas;
 - 6.3.2.12.5. Limite de requisições de redirecionamentos;
 - 6.3.2.12.6. Tempo máximo para a varredura;
 - 6.3.2.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
 - 6.3.2.12.8. Número máximo de requisições HTTP por segundo;
- 6.3.2.13. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
- 6.3.2.13.1. Limite em segundos para timeout de requisições de rede;
 - 6.3.2.13.2. Número máximo de timeouts antes que a varredura seja abortada;
- 6.3.2.14. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 6.3.2.15. A solução deve enviar notificações através de no mínimo E-mail e SMS;
- 6.3.2.16. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
- 6.3.2.17. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 6.3.2.18. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 6.3.2.19. A solução deve ser compatível com avaliação de web services REST e SOAP;
- 6.3.2.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:
- 6.3.2.20.1. Autenticação básica (digest);
 - 6.3.2.20.2. NTLM;
 - 6.3.2.20.3. Form de login;
 - 6.3.2.20.4. Autenticação de Cookies;
 - 6.3.2.20.5. Autenticação através de Selenium;
 - 6.3.2.20.6. Autenticação através de Bearer;
- 6.3.2.21. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;
- 6.3.2.22. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;
- 6.3.2.23. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 6.3.2.24. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- 6.3.2.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 6.3.2.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
- 6.3.2.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
- 6.3.2.27.1. Payload injetado;
 - 6.3.2.27.2. Evidência em forma de resposta da aplicação;
 - 6.3.2.27.3. Detalhes da requisição HTTP;
 - 6.3.2.27.4. Detalhes da resposta HTTP;
- 6.3.2.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
- 6.3.2.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
- 6.3.2.30. A solução deve possuir suporte a varreduras de componentes para no mínimo:
- 6.3.2.30.1. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

6.3.3. Módulo de Análise de Infraestrutura Sobre Código em Ambiente de Imagens em Contêiner, DevOps e GitOps.

- 6.3.3.1. A solução deve detectar e configurações incorretas da infraestrutura de nuvem em fases de design, construção e tempo de execução do seu ciclo de vida de desenvolvimento de software;
- 6.3.3.2. A solução deve prevenir problemas de segurança identifique e remova falhas na nuvem durante desenvolvimento antes de chegarem à produção;
- 6.3.3.3. A solução deve ser possível avaliar modelos de infraestrutura como código (IaC), com integrações nativas em:
- 6.3.3.3.1. Terraform;
 - 6.3.3.3.2. AWS CloudFormation;

6.3.3.3.3. Azure Resource Manager;

6.3.3.3.4. Kubernetes;

6.3.3.4. A solução deve prevenir o desvio de postura na nuvem identifique discrepâncias entre o IaC e sua nuvem em execução ambiente;

6.3.3.5. A solução deve fornecer sugestões de correção automaticamente por meio de pull ou mesclagem;

6.3.3.6. A solução deve contextualizar riscos compreender as vulnerabilidades de aplicativos no contexto de suas configurações de infraestrutura para obter uma imagem real do risco que eles presente;

6.3.3.7. A solução deve prover integração no mínimo com as seguintes plataformas abaixo:

6.3.3.7.1. Jira;

6.3.3.7.2. Slack;

6.3.3.7.3. AWS SNS;

6.3.3.7.4. Jenkins;

6.3.3.7.5. Terraform Cloud;

6.3.3.7.6. CircleCI;

6.3.3.7.7. Splunk;

6.3.3.7.8. AWS CloudTrail;

6.3.3.8. A solução deve possuir integração com no mínimo os seguintes Repositórios:

6.3.3.8.1. Bitbucket;

6.3.3.8.2. GitHub;

6.3.3.8.3. GitLab;

6.3.3.8.4. Azure DevOps;

6.3.3.9. A solução deve possuir funcionalidade de monitoramento dos repositórios sempre que houver alteração de código uma verificação automática via IaC deve apresentar a diferença;

6.3.3.10. A solução deve possuir políticas de análise em ambiente de nuvem para no mínimo as seguintes plataformas:

6.3.3.10.1. AWS;

6.3.3.10.2. Azure;

6.3.3.10.3. GCP;

6.3.3.10.4. Kubernetes;

6.3.3.11. A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard:

6.3.3.11.1. CIS;

6.3.3.11.2. NIST;

6.3.3.11.3. ISO-27001;

6.3.3.11.4. HIPAA;

6.3.3.11.5. PCI-DSS;

6.3.3.11.6. CCM;

6.3.3.11.7. GDPR;

6.3.3.12. A solução deve analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

6.3.3.13. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;

6.3.3.14. A solução deve integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da contratante;

6.3.3.15. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

6.3.3.16. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

6.3.3.17. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

6.3.3.18. A solução deve identificar containers que não foram analisados antes de sua implementação em produção;

6.3.3.19. A solução deve analisar as camadas (layers) de um container;

6.3.3.20. A solução deve identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

6.3.3.21. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

6.3.3.22. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

6.3.3.23. A solução deve inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

6.3.3.24. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

6.3.3.24.1. JFrog;

6.3.3.24.2. Red Hat Quay;

6.3.3.24.3. Sonatype Nexus Repository;

6.3.3.24.4. AWS ECR;

6.3.3.24.5. Microsoft Azure Container;

6.3.3.25. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;

6.3.3.26. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

6.3.3.27. A solução deve prover integração com as seguintes plataformas de integração contínua: Azure Pipelines, GitHub Action, GitLab Pipeline, Jenkins Pipeline, Terraform Cloud Run Task, e Kubernetes;

6.3.4. Modulo de Análise em Ambiente Microsoft Active Directory

6.3.4.1. A solução deve identificar fraquezas ocultas em configurações do dedicadas ao Active Directory;

6.3.4.2. A solução deve possuir ações preventivas de hardening para o Active Directory;

- 6.3.4.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;
- 6.3.4.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 6.3.4.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
- 6.3.4.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 6.3.4.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 6.3.4.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;
- 6.3.4.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 6.3.4.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
- 6.3.4.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 6.3.4.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 6.3.4.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 6.3.4.14. A solução não deve realizar alterações no Active Directory, seus objetos e atributos;
- 6.3.4.15. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 6.3.4.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 6.3.4.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 6.3.4.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 6.3.4.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
 - 6.3.4.19.1. Não depender de agentes ou sensores para coleta de informações do AD;
 - 6.3.4.19.2. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;
 - 6.3.4.19.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;
- 6.3.4.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:
 - 6.3.4.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;
 - 6.3.4.20.2. Validação de contas desativadas em grupos privilegiados;
 - 6.3.4.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHuristics;
 - 6.3.4.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;
 - 6.3.4.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;
 - 6.3.4.20.6. Validação de contas com senhas que nunca expiram;
 - 6.3.4.20.7. Validação de senhas reversíveis em GPOs;
 - 6.3.4.20.8. Validação de uso de senhas reversíveis em contas de usuário;
 - 6.3.4.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;
 - 6.3.4.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;
 - 6.3.4.20.11. Validação se o domínio possui um nível funcional desatualizado;
 - 6.3.4.20.12. Validação de contas de usuário utilizando senha antiga;
 - 6.3.4.20.13. Validação se o atributo AdminCount está definido em usuários padrão;
 - 6.3.4.20.14. Validação do uso recente da conta de administrador padrão;
 - 6.3.4.20.15. Validação de usuários com permissão para ingressar computadores no domínio;
 - 6.3.4.20.16. Validação de contas dormentes;
 - 6.3.4.20.17. Validação de computadores executando um sistema operacional obsoleto;
 - 6.3.4.20.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
 - 6.3.4.20.19. Validação de direitos perigosos configurados no Schema do AD;
 - 6.3.4.20.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;
 - 6.3.4.20.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
 - 6.3.4.20.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
 - 6.3.4.20.23. Validação da última alteração de senha do KDC;
 - 6.3.4.20.24. Validação da última alteração da senha da conta SSO do Azure AD;
 - 6.3.4.20.25. Validação de contas que podem ter senha em branco/vazia;
 - 6.3.4.20.26. Validação de utilização do grupo nativo Protected Users;
 - 6.3.4.20.27. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;
 - 6.3.4.20.28. Validação de possível senha em clear-text;
 - 6.3.4.20.29. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
 - 6.3.4.20.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
 - 6.3.4.20.31. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
 - 6.3.4.20.32. Validação de contas anormais nos grupos administrativos padrão do AD;
 - 6.3.4.20.33. Validação de consistência no container adminSDHolder;
 - 6.3.4.20.34. Validação de delegação Kerberos perigosa;
 - 6.3.4.20.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
 - 6.3.4.20.36. Validação de políticas de senha fracas aplicadas aos usuários;
 - 6.3.4.20.37. Validação das permissões relacionadas às contas do Azure AD Connect;
 - 6.3.4.20.38. Validação do ID do grupo primário do usuário (Primary Group ID);
 - 6.3.4.20.39. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
 - 6.3.4.20.40. Controladores de domínio gerenciados por usuários ilegítimos;

- 6.3.4.20.41. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
- 6.3.4.20.42. Validação de uso de protocolo Netlogon inseguro (ZeroLogon/CVE-2020-1472);
- 6.3.4.21. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
- 6.3.4.21.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
- 6.3.4.21.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
- 6.3.4.21.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
- 6.3.4.21.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 6.3.4.22. Detecção e Resposta a Ataques:
- 6.3.4.22.1. Monitorar continuamente os indicadores de possíveis ataques como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injection nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
- 6.3.4.22.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
- 6.3.4.22.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
- 6.3.4.22.4. Apresentação de ataques em uma linha do tempo;
- 6.3.4.22.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;
- 6.3.4.22.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 6.3.4.23. A solução deve ser capaz de enviar alertas por e-mail;
- 6.3.4.24. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
- 6.3.4.25. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 6.3.4.26. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
- 6.3.4.27. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 6.3.4.28. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 6.3.4.29. A solução deve ser licenciada pelo número de usuários habilitados;

7. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Fundamentação: providências a serem adotadas pela Administração previamente à celebração do contrato (inciso X do § 1º do art. 18 da Lei 14.133/2021 e Art. 9º, inciso XI da IN 58/2022).

7.1. A Equipe de Planejamento da Contratação apresenta a seguir as necessidades de recursos materiais e humanos do TRE-PA, no que se refere à implantação, uso e à manutenção da Solução de TIC, para que o contrato possa ser devidamente executado e a solução de TIC atinja seus objetivos:

TIPO DE NECESSIDADE	UNIDADE RESPONSÁVEL	DESCRIÇÃO
Infraestrutura tecnológica	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Mudança ou Configuração	SDC/CGSI	Implantação e configuração de novas licenças da solução será feito pela equipe de Defesa Cibernética.
Infraestrutura elétrica	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Obtenção de licenças	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Logística de implantação	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Espaço físico	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Mobiliário	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Impacto ambiental	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Capacitação fiscalização / gestão contratual	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Recursos Humanos	Fiscal técnico	Acompanhar as entregas relacionadas à solução contratada.
	Fiscal técnico	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.

8. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

- 8.1. A estimativa preliminar dos preços foi elaborada com base em preços fornecidos diretamente pelos fabricantes, exclusivamente, por meio de contratações públicas. A análise comparativa dessa referência visa assegurar que os valores estimados estejam em conformidade com as práticas de mercado, observando o princípio da economicidade previsto no art. 3º da Lei nº 14.133/2021 (Nova Lei de Licitações).
- 8.2. Para confirmação da estimativa, foi realizada uma pesquisa de preços em observância aos parâmetros estabelecidos pela Instrução Normativa Seges/ME nº 65/2021, que regulamenta a metodologia de pesquisa de preços para contratações públicas, e pela Instrução Normativa SGD-ME nº 94/2022, que dispõe sobre critérios específicos para a contratação de bens e serviços de TIC. Esses instrumentos normativos garantem maior precisão no levantamento de preços e promovem a competitividade e a transparência nos processos licitatórios. Observamos, ainda, as orientações exaradas junto ao Acórdão n. 1.432/2024 - TCU - Plenário.
- 8.3. A demanda inicial foi estimada com base nas quantidades estimadas para o TRE-PA, conforme quadros a seguir:

	ITEM	DESCRIÇÃO	CATSER	QTDE	VALOR UNITÁRIO	TOTAL
--	------	-----------	--------	------	----------------	-------

GRUPO 1	1	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Externos - Tenable.IO WAS, para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo o serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	27464 - Licenciamento de Direitos Permanentes de Uso de Software para Servidor	5	R\$ 1.150,00	R\$ 5.750,00
	2	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Internos - Tenable Security Center (SC+), para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	27464 - Licenciamento de Direitos Permanentes de Uso de Software para Servidor	500	R\$ 652,60	R\$ 326.300,00
	3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 24 horas de duração.	3840 - Treinamento Informática - Sistema / Software	1	R\$ 18.510,00	R\$ 18.510,00
TOTAL GERAL (GRUPO 1)						R\$ 350.560,00

Tabela 1 - Bens e serviços de compõe a o objeto da contratação Grupo 1 / TRE-PA

	ITEM	DESCRIÇÃO	CATSER	QTDE	VALOR UNITÁRIO	TOTAL
GRUPO 2	4	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable.io Web Application Scanning (WAS) para a subscrição do licenciamento Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	27502 - Cessão Temporária de Direitos Sobre Programas de Computador (Locação de Software)	5	R\$ 1.371,50	R\$ 6.857,50
	5	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable Security Center (SC+) para a subscrição do licenciamento do software Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	27502 - Cessão Temporária de Direitos Sobre Programas de Computador (Locação de Software)	500	R\$ 1.407,12	R\$ 703.560,00
	6	Contratação da subscrição do licenciamento do software de Gerenciamento de Exposição Cibernética Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	26077 - Software como Serviço (SaaS)	1200	R\$ 1.330,00	R\$ 1.596.000
	7	Serviço de Instalação, configuração e migração do ambiente atual.	26972 - Serviços de instalação, transição e configuração / parametrização de software	1	R\$ 40.672,50	R\$ 40.672,50
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	1	R\$ 31.755,00	R\$ 31.755,00
	9	Serviço de Operação Assistida e apoio operacional, pelo período de 60 (sessenta) meses, sob demanda.	27324 - Serviços de Pesquisa, Análise e Desenvolvimento em Tecnologia Informação e Comunicação (TIC)	1	R\$ 199.655,50	R\$ 199.655,50
TOTAL GERAL (GRUPO 2)						R\$ 2.578.500,50

Tabela 2 - Bens e serviços de compõe a o objeto da contratação Grupo 2 / TRE-PA

8.4. A estimada total, com base no ambiente tecnológico dos Tribunais participantes, considerou o custo para um período de 60 (sessenta) meses. Essa projeção busca assegurar que todos os aspectos operacionais e de suporte técnico sejam cobertos, conforme detalhado nos quadros abaixo:

GRUPO	ITEM	DESCRIÇÃO	CATSER	UNIDADE	QTDE	VALOR UNITÁRIO	TOTAL
O 1	1	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Externos - Tenable.IO WAS, para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo o serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	27464 - Licenciamento de Direitos Permanentes de Uso de Software para Servidor	LICENÇA	39	R\$ 1.150,00	R\$ 44.850,00

2	Renovação do licenciamento da Solução de Gerenciamento de Exposição Cibernética para FQDNs Internos - Tenable Security Center (SC+), para ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, incluindo serviço de instalação, configuração, repasse técnico, suporte, garantia e atualizações do fabricante, pelo período de 60 (sessenta) meses.	27464 - Licenciamento de Direitos Permanentes de Uso de Software para Servidor	LICENÇA	2.400	R\$ 652,60	R\$ 1.566.240,00
3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 24 horas de duração.	3840 - Treinamento Informática - Sistema / Software	TURMA	4	R\$ 18.510,00	R\$ 74.040,00
TOTAL GERAL (GRUPO 1)						R\$ 1.685.130,00

Tabela 1 - Bens e serviços de compõe a o objeto da contratação Grupo 1, Tribunais Partícipes

GRUPO 2	ITEM	DESCRIÇÃO	CATSER	UNIDADE	QTDE	VALOR UNITÁRIO	TOTAL
	4	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable.io Web Application Scanning (WAS) para a subscrição do licenciamento Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	27502 - Cessão Temporária de Direitos Sobre Programas de Computador (Locação de Software)	LICENÇA	30	R\$ 1.371,50	R\$ 41.145,00
	5	Atualização (upgrade) do software de Gerenciamento de Exposição Cibernética Tenable Security Center (SC+) para a subscrição do licenciamento do software Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	27502 - Cessão Temporária de Direitos Sobre Programas de Computador (Locação de Software)	LICENÇA	11900	R\$ 1.407,12	R\$ 16.744.728
	6	Contratação da subscrição do licenciamento do software de Gerenciamento de Exposição Cibernética Tenable One, incluindo garantia técnica do fabricante, pelo período de 60 (sessenta) meses.	26077 - Software como Serviço (SaaS)	LICENÇA	21995	R\$ 1.330,00	R\$ 29.253.350
	7	Serviço de Instalação, configuração e migração do ambiente atual.	26972 - Serviços de instalação, transição e configuração / parametrização de software	SERVIÇO	21	R\$ 40.672,50	R\$ 854.122,5
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	TURMA	22	R\$ 31.755,00	R\$ 698.610
	9	Serviço de Suporte Técnico com Operação Assistida, pelo período de 60 (sessenta) meses.	27324 - Serviços de Pesquisa, Análise e Desenvolvimento em Tecnologia Informação e Comunicação (TIC)	MÊS	19	R\$ 199.655,50	R\$ 3.793.454,5
TOTAL GERAL (GRUPO 2)							R\$ 51.385.410,00

Tabela 2 - Bens e serviços de compõe a o objeto da contratação Grupo 2, Tribunais Partícipes

8.5. O levantamento de custos realizado neste Estudo Técnico Preliminar (ETP) considerou, conforme mencionado, apenas as contratações públicas apontadas. Deste modo, cumpre ressaltar que os valores finais informados são meramente estimativos para a análise preliminar do estudo técnico, uma vez que as contratações isoladas utilizadas como referência não consideram a potencial economia de escala esperada para o presente certame, que agrega a demanda de múltiplos órgãos. Sendo assim, entende-se que os custos finais da licitação só serão conhecidos após a ampla pesquisa de mercado.

9. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

Fundamentação: descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável (inciso XII do § 1º do art. 18 da Lei 14.133/2021).

9.1. Nesta contratação não há qualquer tipo de impactos ambientais, ou eventuais processos relacionados a resíduos resultantes da contratação, tais como embalagens, logística reversa, dentre outros, uma vez que trata-se de fornecimento de solução do tipo SaaS (Software como Serviço).

10. ESTRATÉGIA DA CONTRATAÇÃO DO OBJETO

10.1. Formas e critérios de seleção do Fornecedor

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO por lote.

10.2. Regime de execução

10.2. Os bens e serviços serão obtidos mediante EXECUÇÃO INDIRETA sendo a EMPREITADA POR PREÇO GLOBAL o regime de execução mais adequado para o objeto pretendido – tendo em vista a precisão dos quantitativos de itens - e o tipo e critério de julgamento da licitação, o MENOR PREÇO por lote, para a seleção da proposta mais vantajosa.

10.3. A prestação de serviços não envolve “dedicação exclusiva de mão de obra” – nos termos do art. 17 da IN 05/SEGES/MPDG de 26/05/2017 – uma vez que o CONTRATADO poderá compartilhar os recursos humanos e materiais disponíveis para execução simultânea de outros contratos. A prestação dos serviços também não gera vínculo empregatício entre os empregados do CONTRATADO e o TRE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

10.3. Parcelamento do objeto

Parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viável e economicamente vantajoso, observado o disposto nos §§ 2º e 3º do art. 40 e § 1º do art. 47 da Lei Federal nº 14.133/2021, justificando-se a decisão de parcelamento ou não da solução. Conforme os §§ 2º e 3º do art. 40 e o § 1º do art. 47 da Lei 14.133/2021, o parcelamento deve ser adotado sempre que tecnicamente viável e economicamente vantajoso, visando ampliar a competitividade e a participação de potenciais fornecedores.

Neste sentido, uma análise quanto a possibilidade de parcelamento de uma solução de cibersegurança e gerenciamento de vulnerabilidades no Tribunal revela que a fragmentação desse projeto não se mostra uma alternativa técnica, administrativa, econômica e nem operacionalmente viável.

Em contratações que envolvem proteção cibernética, a integridade e a interoperabilidade das soluções são essenciais para garantir uma defesa contínua e coordenada contra ameaças cibernéticas, um aspecto que é seriamente comprometido pelo parcelamento.

A natureza integrada dos serviços de segurança cibernética – que abrange desde a detecção e análise de vulnerabilidades até o monitoramento em tempo real, a resposta a incidentes e a aplicação de medidas corretivas – demanda um gerenciamento centralizado e uma execução unificada para garantir uma proteção eficiente.

Dividir o objeto entre diversos fornecedores introduz uma fragmentação que impacta diretamente a eficiência operacional e a robustez da infraestrutura de segurança.

Cada fornecedor adicional implica novos desafios de interoperabilidade, trazendo riscos de incompatibilidade que podem prejudicar o desempenho das soluções, além de criar zonas de sombreamento que podem possibilitar exploração de ataques e vulnerabilidades.

Isso é particularmente crítico na cibersegurança, onde a necessidade de resposta rápida e coordenada exige um fluxo contínuo de informações e uma integração total entre os sistemas de monitoramento, gestão de vulnerabilidades e respostas a incidentes. A pulverização do objeto certamente aumenta o risco de falhas e vulnerabilidades decorrentes de inconsistências na comunicação entre componentes, abrindo, como dito acima, brechas exploráveis por agentes maliciosos e comprometendo a integridade dos dados e dos sistemas do Tribunal.

Além disso, a fragmentação do objeto introduz complexidade adicional ao gerenciamento de riscos, o que se traduz em uma maior dificuldade para monitorar e mitigar vulnerabilidades. A multiplicidade de fornecedores dificulta a centralização das operações de segurança e reduz a eficácia de uma visão holística sobre as ameaças, visto que cada prestador de serviço tem acesso a uma parte da solução e depende de forma detalhada para garantir uma defesa coesa. Essa fragmentação, além de impactar o tempo de resposta, prejudica a comunicação entre as áreas, aumentando a probabilidade de atrasos e falhas na execução das ações corretivas.

O aspecto econômico também representa um fator importante na decisão de inviabilizar o parcelamento. Nas contratações integradas, a administração pública tem mais poder de negociação, obtendo condições financeiras mais vantajosas, como descontos proporcionais ao volume e economia de escala em contratos unificados.

O Tribunal, ao contratar um objeto integral, reduz os encargos administrativos e as despesas indiretas associadas a processos de pagamento e gestão de múltiplos contratos. Contratar um único fornecedor não apenas facilita o monitoramento e a fiscalização das obrigações contratuais, mas também reduz os custos adicionais, como taxas administrativas, despesas de coordenação e gestão de contratos múltiplos.

A contratação de uma solução completa com um único fornecedor também proporciona maior estabilidade e continuidade operacional. Um contrato integrado garante uma única fonte de suporte e atualização tecnológica, o que é crucial em cibersegurança, pois garante que o fornecedor responsável tenha domínio total sobre o ambiente do Tribunal e possa responder rapidamente a incidentes e adaptar o sistema conforme o cenário de ameaças evolutivas. A continuidade na prestação dos serviços é um ponto crítico na proteção de sistemas sensíveis, como os de cibersegurança, e evita interrupções e lacunas na cobertura de segurança.

Do ponto de vista técnico, o parcelamento prejudica a capacidade de atualização e evolução contínua da solução, uma vez que cada componente fragmentado precisaria ser compatível com os demais, complicando as atualizações e limitando a flexibilidade do Tribunal para se adaptar rapidamente a novas novidades ou melhorias tecnológicas. Uma solução cibernética exige adaptações frequentes, e a necessidade de manter a compatibilidade de segurança entre vários fornecedores requer uma aplicação ágil de melhorias, expondo o ambiente a um risco de desatualização. Uma solução integral, ao contrário, permite um controle centralizado de verificações, facilitando o acompanhamento das vulnerabilidades e o aprimoramento das defesas, mantendo uma infraestrutura alinhada aos padrões mais elevados de segurança.

Por fim, o parcelamento em itens prejudica o cumprimento das regulamentações de segurança da informação. Normas como a Lei Geral de Proteção de Dados (LGPD) e outras disposições nacionais e internacionais de segurança bloqueiam um nível de conformidade que pode ser difícil de manter em um ambiente fragmentado. A falta de padronização entre fornecedores exige a implementação de políticas de segurança consistentes e aumenta o risco de incidentes que possam resultar em avaliações legais e prejuízos à imagem institucional do Tribunal. A contratação em grupos, portanto, garante que todos os aspectos de conformidade e governança de segurança sejam mantidos de forma coesa e unificada, facilitando as auditorias e o cumprimento dos requisitos legais de proteção de dados e segurança.

Considerando esses fatores técnicos, operacionais e econômicos, a contratação por itens de uma solução de cibersegurança e vulnerabilidades se mostra inviável. A abordagem de contratação por grupos é, sem dúvida, a mais adequada para garantir uma proteção robusta e eficiente ao ambiente digital do Tribunal, preservando a continuidade, a segurança e a conformidade permitida para enfrentar as ameaças cibernéticas modernas.

10.4. Justificativa para o agrupamento de itens.

O agrupamento dos itens do objeto em dois lotes, tem por objetivo a padronização da contratação uma vez que os itens agrupados estão associadas a mesma solução tecnológica (on premise e SaaS) e possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores, conforme demonstrado, traz ineficiência e custo na gestão e fiscalização da contratação.

Além disso, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou provoca a perda de economia de escala. Neste sentido, justifica-se o agrupamento em lotes (G1 e G2), uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

De outro lado, justifica-se a adoção do agrupamento em lotes em razão da padronização e interoperabilidade de componentes que fazem parte da solução de segurança da informação que compõe cada grupo, visando garantir a integração e compatibilidade entre diferentes componentes e plataformas, sem a necessidade de integrações de diferentes soluções/fornecedores. Ao agrupar a aquisição de softwares em lotes distintos, busca-se não apenas otimizar recursos financeiros e administrativos, mas também garantir uma abordagem coordenada que permita a criação de soluções e que entreguem resultados de forma sinérgica. Essa estratégia proporciona um ambiente propício para o desenvolvimento de sistemas que se complementam, facilitam a troca de dados e informações, reduzem redundâncias e, por consequência, promovem maior agilidade operacional e eficácia nos processos internos do órgão contratante.

Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um fornecedor e melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Termo de Referência.

Isto posto, o agrupamento nos lotes G1 e G2 visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existente no TRE-PA, serviços prestados, a contratação será realizada através de dois Lotes distintos G1 e G2.

10.5. Adoção do Sistema de Registro de Preços (SRP)

Justifica-se pela necessidade de promover flexibilidade e eficiência nas contratações públicas, especialmente em contextos onde o consumo é incerto e pode variar ao longo do tempo, como ocorre em serviços de tecnologia e infraestrutura. O SRP oferece uma vantagem estratégica para permitir que a Administração realize uma única licitação para registrar os preços, possibilitando aquisições conforme a demanda, sem a obrigatoriedade de contratação imediata.

Esse sistema é especificamente adequado para serviços que exigem contratações frequentes e flexíveis, com entregas em momentos diferentes, conforme previsto no art. 3º do Decreto nº 11.462/2023 e pelos artigos 82 a 86 da Lei nº 14.133/2021. Dessa forma, o SRP atende de maneira eficiente às necessidades dinâmicas de crescimento e adaptação das infraestruturas tecnológicas e de segurança cibernética da Administração Pública, permitindo contratações parceladas ou escalonadas.

As principais vantagens do SRP incluem:

Vantagem	Justificativa
Redução do Volume de Fornecimento Antecipado	A Administração requisita os serviços ou bens registrados apenas quando há demanda concreta, eliminando o complemento complementar e otimizando o uso dos recursos financeiros.
Adequação à Imprevisibilidade do Consumo	O SRP é ideal para cenários onde é prever o consumo exato ao longo do tempo, permitindo que a Administração registre preços e adquira serviços conforme a necessidade, alinhando-se ao difícil crescimento variável das operações e à expansão de novas frentes de trabalho.
Agilidade nas Aquisições	Com preços e condições previamente estabelecidas, o processo de aquisição se torna mais rápido e simples, permitindo que o órgão solicite os serviços conforme necessário, sem precisar abrir novas licitações para cada demanda específica.
Redução no Número de Licitações	O SRP permite que itens de natureza semelhante, necessários para diversos projetos ou unidades, sejam adquiridos sob um mesmo registro de preços, resultando em maior eficiência e menor sobrecarga administrativa.
Planejamento Orçamentário Facilitado	Ao centralizar a definição de preços e condições, o SRP facilita o planejamento financeiro a longo prazo, proporcionando maior previsibilidade nos gastos e melhor gestão dos recursos públicos.
Maior Poder de Negociação	Ao consolidar a demanda de diferentes órgãos ou setores em um único processo, o SRP fortalece o poder de compra da Administração, possibilitando condições mais vantajosas e descontos devido ao volume.

Conformidade e Padronização	O SRP ajuda a padronizar as aquisições, garantindo que todos os órgãos adquiram bens e serviços com critérios uniformes de qualidade e segurança, alinhados às diretrizes e regulamentações vigentes.

11. AVALIAÇÃO QUANTO À NECESSIDADE DE CLASSIFICAÇÃO DO ETP, NOS TERMOS DA LEI Nº 12.527/2011 (OBRIGATÓRIO)

11.1. Considerando não se tratar de licitação cujas informações nele constantes sejam sensíveis e imprescindíveis à segurança da sociedade e do Estado, não há necessidade de se atribuir qualquer tipo de classificação ao presente documento, nos termos dispostos na Lei nº 12.527/2011.

12. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

Fundamentação: A Declaração de viabilidade da contratação está disposta no inciso V do artigo 11 da IN 94/2022, e nela estabelece que haverá “a justificativa da solução escolhida, que deverá abranger a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.”

12.1. Esta equipe de planejamento declara viável a presente contratação com base neste Estudo Técnico Preliminar, consoante o inciso V do art. 11 da IN 94, de 23 de dezembro de 2022, - SGD-ME.

12.2. Assinam eletronicamente este ETP, o integrante técnico, integrante demandante e o integrante administrativo, conforme equipe de planejamento designada nos autos, além da autoridade máxima da área de TIC.



Documento assinado eletronicamente por **ANTONIO EDIVALDO DE OLIVEIRA GASPAR, Coordenador**, em 16/11/2025, às 17:02, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **FELIPE HOUAT DE BRITO, Secretário**, em 16/11/2025, às 17:30, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **CHARLES ALEX DOS SANTOS BATISTA, Coordenador substituto**, em 17/11/2025, às 09:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2856632** e o código CRC **0668CE21**.

0003409-70.2025.6.14.8000

2856632v2