



TRIBUNAL REGIONAL ELEITORAL DO PARA
Rua João Diogo 288 - Bairro Campina - CEP 66015-902 - Belém - PA

TERMO DE REFERÊNCIA
Lei nº 14.133, de 1º de abril de 2021
SERVIÇOS - TIC

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. OBJETO DA CONTRATAÇÃO

Registro de preços para eventual e futura contratação de **solução de gerenciamento de exposição cibernética**, composta por disponibilização e renovação de licenças, implantação, repasse técnico, treinamento, garantia e manutenção dos equipamento e/ou softwares por 60 meses, conforme condições, quantidades e exigências estabelecidas neste Instrumento e seus anexos.

	ITEM	DESCRIÇÃO	CATSER	PART NUMBER	UNIDADE	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	TIO-WAS	LICENÇA	39	R\$ 2.092,07	81.590,73
	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	TSCCV-M	LICENÇA	2400	R\$ 1.942,72	4.662.528,00
	3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	N/A	TURMA	4	R\$ 25.792,11	103.168,44
TOTAL GERAL (GRUPO 1)								R\$ 4.847.287,17

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

	ITEM	DESCRIÇÃO	CATSER	PART NUMBER	UNIDADE	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)	T-ONE	LICENÇA	30	R\$ 1.648,90	49.467,00
	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)	T-ONE	LICENÇA	11.900	R\$ 1.650,10	19.636.190,00
	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)	T-ONE	LICENÇA	21.995	R\$ 1.722,24	37.880.668,80
	7	Serviço de Instalação, configuração e migração do ambiente atual.	26972 - Serviços de instalação, transição e configuração / parametrização de software	N/A	SERVIÇO	21	R\$ 33.793,09	709.654,89
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	N/A	TURMA	22	R\$ 31.202,80	686.461,60
	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)	N/A	SERVIÇO	19	R\$ 554.045,32	10.526.861,08
TOTAL GERAL (GRUPO 2)								R\$ 69.489.303,37

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

1.1.2. Os códigos, unidades de fornecimento e descrições oriundas do CATSER (Sistema de Compras do Governo Federal) podem eventualmente divergir da

descrição e especificações constantes deste Termo de Referência, devendo prevalecer as especificações detalhadas deste Instrumento.

1.1.3. 1.9. O(s) serviço(s) objeto desta contratação não contempla item de Catálogo de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP, previsto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

1.3. Os serviços objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar (ETP).

1.4. O objeto será adjudicado pelo menor preço global por lote, respeitando os valores máximos por item, conforme especificações constantes neste Termo de Referência.

1.5. **Farão parte do Registro de Preços, como órgãos participantes**, os seguintes Tribunais Regionais Eleitorais - TREs, os quais serão responsáveis pelas suas respectivas contratações: **TRE-AL, TRE-AM, TRE-AP, TRE-BA, TRE-CE, TRE-DF, TRE-ES, TRE-GO, TRE-MA, TRE-MG, TRE-MS, TRE-MT, TRE-PB, TRE-PI, TRE-PR, TRE-RJ, TRE-RN, TRE-RO, TRE-SE, TRE-SP, TRE-TO e Tribunal Superior Eleitoral (TSE).**

1.5.1. **Durante a vigência da ata de registro de preços, será permitida a adesão aos Tribunais Regionais Eleitorais que não participaram do procedimento de IRP**, em razão da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

1.6. A validade da Ata de Registro de Preços será de 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso, conforme art. 84 da Lei nº 14.133/2021.

1.7. O prazo de vigência da contratação será de **60 (sessenta) meses** contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.7.1. O serviço é enquadrado como continuado tendo em vista a necessidade permanente (ou prolongada) para manutenção da atividade administrativa do órgão de garantia da segurança cibernética, sendo a vigência plurianual mais vantajosa considerando as justificativas constantes do Estudo Técnico Preliminar.

1.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos, bem como os resultados e benefícios a serem alcançados, encontram-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice I deste Termo de Referência.

2.2. 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.*

2.3. O objeto da contratação está alinhado com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com o Planejamento Estratégico Institucional e com a Estratégia Nacional de TIC (ENTIC-JUD - 2021-2026), conforme demonstrado abaixo:

2.3.1. Alinhamento do Plano Estratégico - PEJEP 2021/2026:

- 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).

2.3.2. A contratação possui alinhamento com os seguintes processos internos da Resolução CNJ nº 370 de 28/01/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

- Processos Internos:

- Objetivo 7 - Aprimorar a Segurança da Informação e a Gestão de Dados

Além disso, a presente contratação tem por objetivo atender os requisitos dos seguintes artigos da Resolução CNJ nº 370:

Art. 31. Cada órgão do Poder Judiciário deverá seguir as diretrizes propostas pelo CNJ na adoção de arquitetura e plataforma de serviços em nuvem, atendendo aos requisitos de segurança da informação e proteção de dados.

Art. 35. Recomenda-se utilizar serviços em nuvem que simplifiquem a estrutura física, viabilizem a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário.

2.3.3. A referida contratação está prevista no PDTI TRE-PA 2025/2026 (associada ao Item 4. SOC 24/7, pág. 10), cujas ações estruturantes incluem as contratações da Coordenadoria de Gestão da Segurança da Informação e Infraestrutura de Datacenter. A referida contratação oferece ferramentas para a análise de dados de segurança, identificação de tendências, vulnerabilidades e padrões de ataque, permitindo a adoção de medidas preventivas e corretivas.

- URL: <https://www.tre-pa.jus.br/institucional/governanca-institucional/governanca-de-ti-i/governanca-de-ti>

2.3.4. Foram observadas as vedações contidas nos arts. 8º e 9º da Resolução CNJ 468/2022 e nos arts. 3º, 4º e 5º da IN SGD nº 94/2022, no que aplicável ao objeto.

2.3. 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 sujeitos a exploração em razão de vulnerabilidades não mapeadas.

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.

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.

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 gerenciamento de exposição cibernética, 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.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

LOTE 1		
ITEM	DESCRIÇÃO	UNI M
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.	LICEN
3.1. Características Gerais 3.1.1 A solução deve ser licenciada pelo número aplicações por FQDN (Fully Qualified Domain Name); 3.1.2. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros; 3.1.2.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA. 3.1.3. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representational State Transfer) para automação de processos e integração com a 3.1.4. A solução deve possuir integração via API no mínimo as seguintes linguagens: Python, Powershell, Ruby, javascript, Java, Swift e PHP; 3.1.5. A solução deve possuir métodos de consulta via api e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE); 3.1.6. O escaneamento para as aplicações expostas, deve ser realizados através de SCANS (ENGINE) do próprio fabricante alocados no Brasil; 3.1.7. Os scanners on premises e em nuvem deverão ser gerenciados por uma única plataforma, de maneira centralizada; 3.1.8. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos; 3.1.9. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM); 3.1.10. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção; 3.1.11. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs); 3.1.12. 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 funciona 3.1.13. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards; 3.1.14. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito; 3.1.15. 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 3.1.16. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura; 3.1.17. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura; 3.1.18. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email; 3.1.19. Dos requisitos e relatórios e painéis gerenciais 3.1.19.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados; 3.1.19.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de de 3.1.19.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução; 3.1.19.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo; 3.1.19.5. A solução deve permitir a customização de dashboards/relatórios; 3.1.19.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo aceitas soluções fragmentadas; 3.1.19.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV; 3.1.19.8. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável); 3.1.19.9. A solução deve suportar o envio automático de relatórios para destinatários específicos;		

- 3.1.19.10. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
- 3.1.19.11. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
- 3.1.20. Funcionalidades de Análise Dinâmica de vulnerabilidades de Aplicações Web**
- 3.1.20.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;
- 3.1.20.2. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);
- 3.1.20.3. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);
- 3.1.20.4. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;
- 3.1.20.5. 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
- 3.1.20.6. A solução deve possuir templates prontos de varreduras entre simples e extensos;
- 3.1.20.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:
- 3.1.20.8. Cookies, Headers, Formulários e Links;
- 3.1.20.9. Nomes e valores de parâmetros da aplicação;
- 3.1.20.10. Elementos JSON e XML;
- 3.1.20.11. Elementos DOM;
- 3.1.20.12. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
- 3.1.20.13. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
- 3.1.20.14. A solução deve excluir determinadas URLs da varredura através de expressões regulares;
- 3.1.20.15. A solução deve excluir determinados tipos de arquivos através de suas extensões;
- 3.1.20.16. A solução deve instituir no mínimo os seguintes limites:
- 3.1.20.17. Número máximo de URLs para crawl e navegação;
- 3.1.20.18. Número máximo de diretórios para varreduras;
- 3.1.20.19. Número máximo de elementos DOM;
- 3.1.20.20. Tamanho máximo de respostas;
- 3.1.20.21. Limite de requisições de redirecionamentos;
- 3.1.20.22. Tempo máximo para a varredura;
- 3.1.20.23. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
- 3.1.20.24. Número máximo de requisições HTTP por segundo;
- 3.1.20.25. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
- 3.1.20.26. Limite em segundos para timeout de requisições de rede;
- 3.1.20.27. Número máximo de timeouts antes que a varredura seja abortada;
- 3.1.20.28. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
- 3.1.20.29. A solução deve enviar notificações através de no mínimo E-mail e SMS;
- 3.1.20.30. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;
- 3.1.20.31. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;
- 3.1.20.32. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
- 3.1.20.33. A solução deve ser compatível com avaliação de web services REST e SOAP;
- 3.1.20.34. Deverá suportar no mínimo os seguintes esquemas de autenticação:
- 3.1.20.35. Autenticação básica (digest);
- 3.1.20.36. NTLM;
- 3.1.20.37. Form de login;
- 3.1.20.38. Autenticação de Cookies;
- 3.1.20.39. Autenticação através de Selenium;
- 3.1.20.40. Autenticação através de Bearer;
- 3.1.20.41. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;
- 3.1.20.42. 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 co
- 3.1.20.43. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;
- 3.1.20.44. 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_Pro);
- 3.1.20.45. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;
- 3.1.20.46. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;
- 3.1.20.47. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:
- 3.1.20.48. Payload injetado;
- 3.1.20.49. Evidência em forma de resposta da aplicação;
- 3.1.20.50. Detalhes da requisição HTTP;
- 3.1.20.51. Detalhes da resposta HTTP;
- 3.1.20.52. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;
- 3.1.20.53. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;
- 3.1.20.54. A solução deve possuir suporte a varreduras de componentes para no mínimo:
- 3.1.20.55. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI.

ITEM	DESCRIÇÃO	UNI M
------	-----------	----------

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.	LICEN
---	--	-------

3.2. Características Gerais

- 3.2.1. A solução deve ser licenciada para realizar:
 - 3.2.1.1 varreduras (scans) de vulnerabilidades;
 - 3.2.1.2. avaliação de configuração e conformidade (baseline e compliance);
 - 3.2.1.3. varreduras em ambientes Windows e Linux;
 - 3.2.1.4. detecção de hot fix, service pack, peer to peer, registros e portas de serviço habilitadas.
- 3.2.2. A solução proposta poderá ser disponibilizada em uma arquitetura em nuvem e/ou on-premise
- 3.2.3. Caso a solução seja em nuvem, obrigatoriamente seus dados e metadados deverão ser tratados em território nacional, conforme recomendação e instrução normativa do g da informação: IN 05 de 31 de agosto de 2021.
- 3.2.4. A solução deve fazer parte do catálogo de produtos comercializados pelo fabricante e nenhum de seus componentes poderá apresentar indicação de: End-of-Support, Enc Life até a data da publicação do Edital.
 - 3.2.4.1. A solução não deverá constar em listas dos respectivos fabricantes que indiquem que não serão mais desenvolvidos, atualizados, suportados ou comercializados c contrato.
- 3.2.5. 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 dev com os virtualizadores: VMware, Microsoft Hyper-V ou XenServer-Citrix.
 - 3.2.5.1. 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 armazenam documentação).
- 3.2.6. A solução deverá utilizar TLS v1.2 ou superior para comunicação entre a console de gerenciamento e os dispositivos de varredura (scanners)
- 3.2.7. A ferramenta deve ser licenciada para realizar a varredura (scan) em no mínimo XXXX IPs internos.
 - 3.2.7.1. Estes objetos podem ser: dispositivos de rede (IP), FQDN, Imagens de Containers e controladores de domínio.
- 3.2.8. As ferramentas de varreduras (scanners) de rede deverão ser instaladas nas dependências da contratante e deverão possuir compatibilidade para instalação com, no mínimo sistemas operacionais servidores a serem fornecidos pela contratante:
 - 3.2.8.1. Windows Server 2019;
 - 3.2.8.2. Debian 8 e superiores ;
 - 3.2.8.3. Debian 10;
 - 3.2.8.4. Red Hat Enterprise Linux Server 5.0 (64 bits) ou superiores;
 - 3.2.8.5. Red Hat Enterprise Linux Server 7;
 - 3.2.8.6. Linux Ubuntu 18.04 ou 20.04 ou superiores;
 - 3.2.8.7. Virtual Appliance com sistema operacional com o devido hardening para execução da solução.
- 3.2.9. 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.
- 3.2.10. A solução deve ser licenciada para no mínimo 12 scanners ativos.
 - 3.2.10.1. A contabilização das licenças será considerada por IPs , Usuários Ativos no Microsoft Active Directory , FQDN únicos.
 - 3.2.10.2. Ter opção para desvincular licenças atreladas aos diferentes tipos de ativos conforme necessidade do contratante.
 - 3.2.10.3. Não deve ter nenhum tipo de limite vinculado a licenciamento para realizar escaneamentos simultâneos (além do limite operacional dos equipamentos).
 - 3.2.10.4. Não deverá ser computado às licenças o simples discovery ou técnicas passivas de detecção de ativos de TI.
 - 3.2.10.5. A contabilização da licença deve ser efetivada no momento em que é realizado o scanner completo.
 - 3.2.10.6. A gerência centralizada deve demonstrar os Ativos de TI vinculados ao licenciamento da solução, com no mínimo a data de ativação dos mesmos. A desvincu TI/licença deve acontecer no prazo máximo de 90 dias.
- 3.2.11. Ser capaz de passivamente detectar ativos tecnológicos de diferentes tipos como por exemplo, servidores, endpoints, aplicações web, máquinas virtuais, IoT.
- 3.2.12. Efetuar a coleta passiva, no mínimo:
 - 3.2.12.1. Por meio do recebimento de tráfego de rede via SPAN port ou TAP, ou;
 - 3.2.12.2. Por meio de integração com outras fontes de evento como DHCP, LDAP / AD ou DNS.
 - 3.2.12.3. Identificar vulnerabilidades através da análise passiva.
 - 3.2.12.4. Ser compatível com Ipv4, Ipv6, TCP e UDP.
- 3.2.13. A ferramenta deve funcionar sem a necessidade de agentes instalados nos servidores que serão alvo de análise de vulnerabilidade.
- 3.2.14. A ferramenta deve permitir a integração com Microsoft Active Directory para a autenticação de usuários.
- 3.2.15. 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
- 3.2.16. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;
- 3.2.17. A base de vulnerabilidades conhecidas deve ser atualizada automaticamente durante a vigência do contrato sem intervenção de administrador.
 - 3.2.17.1. Todas as vezes que a base de vulnerabilidade for atualizada automaticamente, um alerta deve ser emitido para o administrador.
 - 3.2.17.2. A solução deve receber a atualização automática de novas versões do produto, via internet, inclusive através de proxy.
- 3.2.18. A ferramenta deve ser capaz de:
 - 3.2.18.1. Utilizar listas de vulnerabilidades da SANS/FBI e IAVA (Information Assurance Vulnerability Alert) ou base própria baseada nas informações de diverso fabricantes, Dark Web, dentre outros;
 - 3.2.18.2. integrar-se com base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
 - 3.2.18.3. ser capaz de identificar no mínimo 51.000 CVE (Common Vulnerabilities and Exposures);
 - 3.2.18.4. utilizar identificadores CVE (Common Vulnerabilities and Exposures) associados às vulnerabilidades identificadas para geração de relatórios, gerenciamento de ameaças.
- 3.2.19. A ferramenta deve permitir a autenticação:
 - 3.2.19.1. com certificados SSL;
 - 3.2.19.2. via API REST.
- 3.2.20. A ferramenta deve fornecer em instalação padrão, diferentes dashboards para análise das informações coletadas em varreduras.

- 3.2.21. A ferramenta deve possibilitar, por meio da console central de gerenciamento, o método de varredura (scan) ativo.
- 3.2.22. A ferramenta deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv2 score.
- 3.2.23. A ferramenta deve possuir um sistema de pontuação e priorização das vulnerabilidades.
 - 3.2.23.1. O algoritmo de priorização deve analisar vulnerabilidades presentes na National Vulnerability Database (NVD).
- 3.2.24. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
 - 3.2.24.1. CVSSv3 Impact Score;
 - 3.2.24.2. Idade da vulnerabilidade;
 - 3.2.24.3. Número de produtos afetados pela vulnerabilidade;
- 3.2.25. A ferramenta deve permitir integração via API REST para automação de processos com aplicações terceiras.
- 3.2.26. A ferramenta deve possuir sistema de alertas com ações definidas para cada alerta, entre elas:
 - 3.2.26.1. Gerar relatório pré-definido com base nas condições de um alerta;
 - 3.2.26.2. Envio de e-mail com base nas condições de um alerta;
 - 3.2.26.3. Envio de mensagem syslog com base nas condições de um alerta;
 - 3.2.26.4. Iniciar varredura (scan) sob demanda com base em condições pré-definidas;
 - 3.2.26.5. Criação de Ticket no sistema de chamados interno da solução.
- 3.2.27. A ferramenta deve possuir a funcionalidade de discovery para a descoberta automática de computadores, servidores e ativos de rede.
 - 3.2.27.1. A ferramenta deve ser capaz de identificar novos hosts no ambiente sem a necessidade de execução manual de uma varredura pelo administrador, devendo ser p
essa funcionalidade através do agendamento prévio da ação de discovery.
- 3.2.28. A ferramenta deve permitir determinar quais portas estão abertas em um determinado ativo após a realização de um scan (agendado ou realizado imediatamente).
- 3.2.29. A ferramenta deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
 - 3.2.29.1. Aplicações;
 - 3.2.29.2. Bancos de dados;
 - 3.2.29.3. Dispositivos de rede;
 - 3.2.29.4. Hypervisors;
 - 3.2.29.5. Servidores.
- 3.2.30. A ferramenta deve oferecer capacidade de configuração dinâmica de grupos de ativos através de, no mínimo, as seguintes características:
 - 3.2.30.1. Sistema Operacional;
 - 3.2.30.2. Endereço IP;
 - 3.2.30.3. Nome DNS;
 - 3.2.30.4. Nome NetBIOS;
 - 3.2.30.5. NetBIOS Workgroup;
 - 3.2.30.6. Endereço MAC;
 - 3.2.30.7. SSH Fingerprint;
 - 3.2.30.8. Porta TCP;
 - 3.2.30.9. Porta UDP;
 - 3.2.30.10. Dias desde a descoberta do ativo;
 - 3.2.30.11. Exploit disponível;
 - 3.2.30.12. XREF;
 - 3.2.30.13. Hosts com Antivirus Desatualizado;
 - 3.2.30.14. Host com Browsers específicos (Opera, Chrome, Safari, Firefox);
 - 3.2.30.15. Hosts com Browser TOR instalado;
 - 3.2.30.16. Hosts com software VOIP instados;
 - 3.2.30.17. Hosts com clientes SQL instalados.
- 3.2.31. A ferramenta deve permitir a configuração de políticas de varreduras diferentes a serem aplicadas a grupos de servidores específicos.
- 3.2.32. O acesso à console de gerenciamento deve ser através do protocolo HTTPS e com interface via navegador web.
- 3.2.33. A console de gerenciamento deve ser compatível com os seguintes navegadores web em suas versões:
 - 3.2.33.1. Mozilla Firefox 74.0 e superiores (aceita-se documentação, exceto para a versão mais recente);
 - 3.2.33.1.1 Mozilla Firefox versão mais recente;
 - 3.2.33.2. Microsoft Internet Explorer 10 e superiores;
 - 3.2.33.3. Google Chrome 81.0.4044.92 e superiores
 - 3.2.33.3.1 Google Chrome versão mais recente;
 - 3.2.33.4. Safari 11.1.2 e superiores;
 - 3.2.33.5. Microsoft Edge 80.0.361.109 e superiores
 - 3.2.33.5.1 Microsoft Edge versão mais recente.
- 3.2.34. A ferramenta deve permitir o cadastramento dos ativos alvo dos escaneamentos por meio de interface web e por API REST.
- 3.2.35. A ferramenta deve indicar o procedimento para a correção ou mitigação das vulnerabilidades encontradas.
- 3.2.36. A ferramenta deve indicar a criticidade e o risco associado a cada vulnerabilidade encontrada.
- 3.2.37. A ferramenta deve possuir sistema para a sinalização de falsos positivos.
- 3.2.38. A ferramenta deve possuir controle de acesso baseado em perfis de usuário.
 - 3.2.38.1. A ferramenta deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência.
- 3.2.39. A ferramenta deve ser aderente às melhores práticas previstas nos principais frameworks de mercado, atendendo a pelo menos 3 dos 5 itens a seguir:
 - 3.2.39.1. SANS 20 Critical Security Controls;
 - 3.2.39.2. CIS Benchmark L1 e L2;
 - 3.2.39.3. ISO 27000;

3.2.39.4. NIST Cybersecurity Framework;

3.2.39.5. NERC CIP.

3.2.40. A ferramenta deve permitir a configuração de usuários com permissão somente de leitura e com permissões administrativas.

3.2.41. A ferramenta deve suportar o uso de IPv4 e IPv6 para o seu funcionamento.

3.2.42. A ferramenta deve suportar sincronismo de horário através do protocolo NTP (Network Time Protocol).

3.2.43. A comunicação da console de gerência com os scanners de rede deve ser criptografada.

3.2.44. A solução adotada pela CONTRATADA deverá ser capaz de verificar vulnerabilidades em gerenciadores de virtualização como Hyper-V e VMware.

3.2.45. A solução adotada deverá apresentar capacidade para análise de vulnerabilidades no Active Directory (AD).

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

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

3.2.48. A solução deve identificar ataque específicos para a estrutura do Active Directory;

3.2.49. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizada os times envolvidos;

3.2.50. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

3.2.51. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

3.2.52. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;

3.2.53. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

3.2.54. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

3.2.55. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

3.2.56. A solução deve prover interface web para gerenciamento de todas as funcionalidades;

3.2.57. A solução deve possuir capacidade nativa de criação de dashboards customizados;

3.2.58. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

3.2.59. A solução deve realizar alterações no Active Directory, seus objetos e atributos;

3.2.60. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

3.2.61. A solução deve suportar ambientes com múltiplas florestas e domínios;

3.2.62. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

3.2.63. A solução deve suportar reter os eventos coletados por no mínimo um ano;

3.2.64. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

3.2.64.1. Não depender de agentes ou sensores para coleta de informações do AD;

3.2.64.2. 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 espere serviço como parte do grupo Domain User;

3.2.64.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

3.2.65. A solução deve possuir capacidade de receber atualizações em horários programados.

3.2.66. Todo o tráfego de informações entre a Solução e a Internet deve ser criptografado.

3.2.67. A solução deve suportar vários scanners conectados simultaneamente. Deverá a CONTRATADA utilizar quantos scanners sejam necessários para atender o sizing de itens especificados neste Termo de Referência, sem que haja necessidade de licenciamento adicional.

3.2.68. A solução deve possuir capacidade de atualizar os scanners automaticamente.

3.2.69. 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 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), contram informação e fonte de exploit.

3.2.70. A solução deve ser entregue em sua última versão disponível e contar com suporte integral durante toda a vigência do contrato.

3.2.71. A solução não poderá estar em versão beta.

3.2.72. A solução deve permitir varreduras por: endereço IP, faixa de IP, agrupamento de ativos, nome NetBIOS e CIDR Notation.

3.2.73. A solução deve possibilitar a integração com a solução de Cofre de Senhas do fabricante Senha Segura sendo permitida integração via API.

3.2.74. A solução deve permitir o cadastramento de credenciais utilizadas para escaneamento para que seja permitido o uso de tais credenciais para futuros escaneamentos, sendo a ferramenta saiba a senha destas credenciais.

3.2.75. VARREDURAS

3.2.75.1. 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

3.2.75.2. A ferramenta deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados horários do dia.

3.2.75.2.1. 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 permitido se iniciar novamente.

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

3.2.75.4. A ferramenta deve realizar varreduras em sistemas operacionais, em appliances físicos e virtuais, incluindo no mínimo:

3.2.75.4.1. Windows Server 2000 e superiores;

3.2.75.4.1.1 Windows Server 2008, 2012 e 2019;

3.2.75.4.2. Red Hat Enterprise Linux 5.0 Server e superiores;

3.2.75.4.2.1 Red Hat Enterprise Linux 7 Server;

3.2.75.4.3. AIX 6.1 e superiores ;

3.2.75.4.4. SUN Solaris 9.0 e superiores ;

3.2.75.4.5. Debian ;

3.2.75.4.6. CentOS 5 e superiores ;

3.2.75.4.7. Oracle Linux 5.0 e superiores ;

3.2.75.4.8. Linux Ubuntu 12.04 e superior .

3.2.75.5. A ferramenta deve realizar varreduras em aplicações que utilizem os principais protocolos de rede, tais como

3.2.75.5.1. HTTP;

- 3.2.75.5.2. HTTPS;
- 3.2.75.5.3. SMTP;
- 3.2.75.5.4. Telnet;
- 3.2.75.5.5. FTP;
- 3.2.75.5.6. SFTP;
- 3.2.75.5.7. SSH;
- 3.2.75.5.8. NTP;
- 3.2.75.5.9. RDP;
- 3.2.75.5.10. SNMP;
- 3.2.75.5.11. POP3;
- 3.2.75.5.12. IMAP;
- 3.2.75.5.13. SIP;
- 3.2.75.5.14. DNS;
- 3.2.75.5.15. LDAP.

3.2.75.6. A ferramenta deve realizar varreduras em banco de dados incluindo, no mínimo:

- 3.2.75.6.1. Oracle Database Enterprise Edition – versão 10.2.0.1.0 e superiores;
 - 3.2.75.6.1.1 Oracle Database Enterprise Edition – versão 18.0.0.0.0.
- 3.2.75.6.2. Microsoft SQL Server – versão 2000 e superiores;
 - 3.2.75.6.2.1 Microsoft SQL Server – versão 2012, 2014 e 2017.
- 3.2.75.6.3. MySQL Server – versão 5.0 e superiores;
 - 3.2.75.6.3.1 MySQL Server – versão 5.6 e 8.0.
- 3.2.75.6.4. PostgreSQL Server – versão 9.0 e superiores;
 - 3.2.75.6.4.1 PostgreSQL Server – versão 9.6 e 11.3.
- 3.2.75.6.5. MongoDB – versão 2.0 e superiores;
 - 3.2.75.6.5.1 MongoDB - versão 3.4 e 4.0.

3.2.75.7. A ferramenta deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

3.2.75.8. A ferramenta deve ser configurável para permitir a otimização das configurações de varredura.

3.2.75.9. A ferramenta deve fornecer a capacidade de escalar privilégios nos ativos que serão varridos, desde o acesso de usuário padrão até acesso administrativo.

3.2.75.10. 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 p:

3.2.76. AUDITORIA DE CONFIGURAÇÃO

3.2.76.1. A ferramenta deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino.

3.2.76.2. A ferramenta deve fornecer benchmarks de auditoria de segurança e configuração.

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

- 3.2.76.3.1. CIS Benchmark L1 e L2 .

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

- 3.2.76.4.1. TrendMicro - Office Scan e Deep Security.;
- 3.2.76.4.2. McAfee VirusScan;
- 3.2.76.4.3. Microsoft Endpoint Protection;
- 3.2.76.4.4. Kaspersky;
- 3.2.76.4.5. Symantec - Endpoint Protection, Endpoint Security e Data Center Security.

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

- 3.2.76.5.1. Microsoft Windows ;
- 3.2.76.5.2. Linux .

3.2.77. RELATÓRIOS

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

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

3.2.77.3. A ferramenta deve possuir relatórios pré-definidos.

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

3.2.77.4. A ferramenta deve permitir a customização de relatórios.

- 3.2.77.4.1. A ferramenta deve permitir a customização do conteúdo de cada relatório;
- 3.2.77.4.2. A solução deve emitir relatório do tipo resumo gerencial, com possibilidade de seleção das informações que irão compor o mesmo.

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

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

- 3.2.77.6.1. Diário;
- 3.2.77.6.2. Mensal;
- 3.2.77.6.3. Semanal.

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

- 3.2.77.7.1. Todos os ativos;
- 3.2.77.7.2. Grupo de ativos;
- 3.2.77.7.3. Ativos específicos.

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

- 3.2.77.8.1. Vulnerabilidade;
- 3.2.77.8.2. Criticidade;

3.2.77.8.3. Ativo;

3.2.77.8.4. Risco;

3.2.77.8.5. Aplicação web.

3.2.77.9. Os relatórios devem conter informações sobre:

3.2.77.9.1. As vulnerabilidades;

3.2.77.9.2. Se existe exploit disponível;

3.2.77.9.3. Informações do ativo;

3.2.77.9.4. Remediação.

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

ITEM	DESCRIÇÃO	UNIM
3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	T

Especificação técnica mínima

- 3.3.1. Trata-se do serviço de treinamento da solução, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de todos os componentes da solução de forma que o(s) servidor(es) e/ou colaboradores capacitado(s) possam colocar a solução em produção, bem como planejar mudança ambiente.
- 3.3.2. O TREINAMENTO, deverá possuir carga horária mínima de 20 (vinte) horas, e deverá ser realizado preferencialmente na forma remota (ao vivo), com emissão de certificado sendo que, a critério do CONTRATANTE, poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação e materiais participantes adicionais do tipo “ouvintes”.
- 3.3.3. O CONTRATANTE solicitará a realização do treinamento à CONTRATADA mediante Abertura - ORDEM DE SERVIÇO de treinamento (ANEXO I-III), sendo que esse deve ser emitido até 45 (quarenta e cinco) dias corridos após o recebimento da Abertura da ORDEM DE SERVIÇO pela CONTRATADA.
- 3.3.4. A CONTRATADA deverá comprovar, previamente à realização do Treinamento, que o(s) INSTRUCTOR(ES) selecionado(s) para ministrar o treinamento possuem qualificação com o conteúdo programático a ser ministrado, incluindo certificados ou declaração do fabricante da solução.
- 3.3.5. O CONTRATANTE poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca do instrutor. Caso a deficiência seja sanada sem prejuízo para o andamento do curso, esse será suspenso devendo a CONTRATADA agendar novo curso, sem ônus adicional ao CONTRATANTE.
- 3.3.6. O treinamento deverá, ainda, observar o seguinte:
- Deverá oferecer carga horária total de no mínimo 20 (vinte) horas.
 - Serão aceitos apenas treinamentos online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.
 - A CONTRATADA deve prover capacitação técnica em turma com no máximo 10 (dez) participantes.
 - Se o treinamento na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.
 - Possuir o conteúdo organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com fixação;
 - Incluir apostilas e manuais dos equipamentos e softwares necessários para a prática dos exercícios propostos no material do treinamento;
 - Prover os acessos que irão compor o laboratório do treinamento que deverão ser iguais aos adquiridos pelo ou, quando não for possível, por ambientes similares e suas funcionalidades;
 - Abranger todas as funcionalidades especificadas nesta especificação técnica;
 - Serem fornecidos certificados de participação para cada participante (exceto para aqueles na condição de ouvintes);
 - Todos os manuais, apostilas e demais documentos devem estar nos idiomas Português (ou Inglês, quando não disponíveis em Português); e
 - Os cursos devem ser ministrados no idioma Português.
- 3.3.7. Após realização do curso será feita uma avaliação de satisfação junto aos participantes, cujo resultado deverá alcançar a média de, pelo menos, 70% (setenta por cento) dos critérios avaliados, para validação e emissão do Termo de Aceite Definitivo. Caso não alcance o resultado esperado, o treinamento deverá ser ministrado novamente.
- 3.3.8. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.
- 3.3.9. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.
- 3.3.9.1. A licitante proponente deverá entregar, na fase de habilitação, uma declaração afirmando que oferta o treinamento da solução e que a ementa e todo o material oferecido pelo fabricante da solução, bem como, indicar na proposta o calendário contendo as datas e as localidades de realização do Treinamento.
- 3.3.9.2. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o treinamento ofertado atende os requisitos indicados.
- 3.3.9.3. É facultado ao Tribunal a realização de diligências e verificação da autenticidade da declaração e demais documentos comprobatórios.
- 3.3.10. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de vigência do Contrato, a contar da entrega do calendário.
- 3.3.11. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação da solução, ficando a critério da administração e baseada no calendário a ser fornecido pela contratada.
- 3.3.12. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato.
- 3.3.13. A contratada deverá fornecer material didático individual que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento deverá ser atualizado e poderá estar em inglês ou português.
- 3.3.15. A pedido do Contratante, o treinamento poderá ser gravado e disponibilizado ao Fiscal da CONTRATANTE;
- 3.3.16. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 5 (cinco) dias úteis após o término do treinamento, o certificado de participação no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia desse certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.
- 3.3.16.1. O certificado de conclusão do curso deverá ser emitido pelo fabricante ou pela empresa a ser contratada.
- 3.3.17. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor.
- 3.3.18. O treinamento ofertado deve seguir os modelos padrão de capacitação disponíveis no mercado naquilo que couber.
- 3.3.19. Não serão aceitos treinamentos não oficiais ou cujo conteúdo ministrado não abranja a utilização da solução para o fim a que se destina, bem ainda, aqueles cujos certificados forem emitidos no prazo máximo de 5 dias contados da conclusão da capacitação.
- A não aceitação da capacitação implicará no não pagamento dos serviços realizados.
 - A empresa a ser contratada deverá emitir certificados de participação contendo a exata carga horária do treinamento e a participação do treinando.
- 3.3.20. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo constante no Anexo deste Termo de Referência (Anexo I-VII - Formulário de avaliação da solução).
- No Formulário, será utilizada escala de até 5 (cinco) pontos para cada quesito. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para ser considerado proveitoso.
 - O resultado da Avaliação de Instrutor/Tutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como 'satisfatório' no mínimo 6 (seis) dos 10 (dez) itens avaliados;
 - Caso o resultado da Avaliação de Instrutor/Tutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito;
 - Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE;
 - Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

CONSIDERAÇÕES GERAIS PARA OS ITENS 4, 5 E 6

1. As licenças de uso do Tenable One Standard deverão ser válidas por 60 meses, contados a partir da data do recebimento definitivo do fornecimento da solução.
2. As licenças deverão ser acompanhadas de sua Garantia técnica do fabricante, conforme definições contidas no **item 3.4** deste Termo de Referência.
3. A chave de ativação das licenças a que se referem tanto o item 4, quanto dos itens 5 e 6, deverão ser registradas na console do produto pela Contratada.
4. A solução deverá ser hospedada em nuvem, na infraestrutura de responsabilidade do seu fabricante.

ITEM	DESCRIÇÃO	UNID D/ MED
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.	LICEN

Especificação técnica mínima

- 3.4.1. Conversão (upgrade) da licença atual do Tenable.io Web Application Scanning (WAS) para a subscrição Tenable One, abrangendo a totalidade dos ativos gerenciados pelo cliente;
- 3.4.2. Continuidade dos serviços de varredura de vulnerabilidades em aplicações web, agora integrados ao portfólio completo do Tenable One, ampliando a visibilidade de ataques;
- 3.4.3. Manutenção de todas as funcionalidades pré-existentes da solução Tenable.io WAS, garantindo compatibilidade e continuidade operacional sem impacto à utilização pelo cliente;
- 3.4.4. A solução Tenable One deve contemplar, no mínimo, os seguintes componentes e funcionalidades relacionadas ao upgrade Tenable.io Web Application Scanning (WAS):
 - a) Identificação automatizada de vulnerabilidades em aplicações web e APIs;
 - b) Detecção de falhas conforme padrões OWASP Top 10;
 - c) Suporte a testes autenticados e não autenticados;
 - d) Capacidade de executar scans dinâmicos e personalizáveis.
- 3.4.5. Requisitos de Licenciamento
 - a) A subscrição do Tenable One deverá ser válida por 60 (sessenta) meses;
 - b) A solução deverá incluir a capacidade de monitoramento de, no mínimo, (quantidade de ativos a serem especificados) ativos dentro do escopo contratado;
 - c) A licitação deve prever a transferência completa dos direitos de uso da licença adquirida para a CONTRATANTE;
 - d) O licenciamento deve incluir todas as atualizações de software, patches e releases disponibilizados pelo fabricante durante o período de vigência do contrato.

ITEM	DESCRIÇÃO	UNID D/ MED
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.	LICEN

Especificação técnica mínima

- 3.5.1. Conversão (upgrade) da licença do Tenable Security Center (SC+) para a subscrição Tenable One, garantindo a migração sem perda de funcionalidades existentes.
- 3.5.2. Manutenção da capacidade de gestão centralizada de vulnerabilidades com a adição de novas funcionalidades para análise de exposição cibernética.
- 3.5.3. Expansão da visibilidade para ativos em ambientes híbridos e multi-cloud, ampliando a cobertura para novas superfícies de ataque.
- 3.5.4. A solução Tenable One deve contemplar, no mínimo, os seguintes componentes e funcionalidades relacionadas ao upgrade Tenable Security Center (SC+):
 - a) Identificação e priorização de vulnerabilidades em ativos de TI, servidores, endpoints e dispositivos de rede;
 - b) Análises baseadas em inteligência de ameaças e pontuações de risco contextualizadas;
 - c) Integração com bases de conhecimento de segurança para correção proativa.
- 3.5.5. Requisitos de Licenciamento
 - a) A subscrição do Tenable One deverá ser válida por 60 (sessenta) meses;
 - b) A solução deverá incluir a capacidade de monitoramento de, no mínimo, (quantidade de ativos a serem especificados) ativos dentro do escopo contratado;
 - c) A licitação deve prever a transferência completa dos direitos de uso da licença adquirida para a CONTRATANTE;
 - d) O licenciamento deve incluir todas as atualizações de software, patches e releases disponibilizados pelo fabricante durante o período de vigência do contrato.

ITEM	DESCRIÇÃO	UNID D/ MED
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.	USUÁ

Especificação técnica mínima**6.6.1. Módulo de Gestão de Vulnerabilidade e Auditoria de Configuração de ativos.****6.6.1.1. 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 integrações 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 nuvem 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 fornecida 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 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 Resource 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 gestão 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 centralizada;
- 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 de 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 no 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 C
 - 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 expl 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 c (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 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 vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo da quantidade de vulnerabilidades corrigidas por criticidade;
 - 6.3.1.5.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa a fim 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

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 KRBGTGT";

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 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

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 cor 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, Mi Point, Palo Alto Networks, Cisco, Fortinet, Trellix, 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 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, Mi 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 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 reconhecido: 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: Trei Scan, McAfee VirusScan, Trellix 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 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 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 r

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, A JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Light 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 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

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 malwares 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 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 de 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 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 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 Task, e Kubernetes;

6.3.4. Módulo de Análise em Ambiente Microsoft Active Directory

6.3.4.1. A solução deve identificar fraquezas ocultas em configurações do 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 ataques 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, controlando o 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 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, Lsa 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;

ITEM	DESCRIÇÃO	UNID D/ MED
7	Serviço de Instalação, configuração e migração do ambiente atual.	SERVI

Especificação técnica mínima

3.7.1. Serviço de instalação: os serviços de instalação lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir.

3.7.1.1. Fase de abertura:

- a.) Validar e Homologar escopo do projeto;
- b.) Validar objetivos e premissas do projeto;
- c.) Validar riscos e restrições do projeto;
- d.) Identificar e validar os requisitos do projeto;
- e.) Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;
- f.) Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;
- g.) Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.

3.7.2. Fase de planejamento:

3.7.2.1. A CONTRATADA deverá elaborar um documento denominado "plano de projeto" com o planejamento das alterações a serem realizadas no ambiente da COI incluindo a descrição da situação atual (As-Is), os procedimentos a serem executados, e a situação final desejada (To-Be), em até 10 dias corridos da data da Reunião Planejamento. O plano de projeto, deverá conter ainda as seguintes informações:

- a) Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;
- b) Definir os parâmetros de configuração básicos e avançados a serem implementados;
- c) Apresentação do cronograma do projeto com os prazos e responsabilidades;
- d) Efetuar o levantamento e apresentar os pré-requisitos do projeto;
- e) O Plano do Projeto será objeto de análise e aprovação da equipe técnica da CONTRATANTE.

3.7.3. Fase de execução:

3.7.3.1. O serviço de instalação consiste na implantação, configuração da solução, objeto da contratação, de forma remota, em conformidade com o disposto nesta especificação no Edital e seus Anexos, e entrega final da solução em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE. Os seguintes requisitos e atividades estão relacionados à fase de execução:

- a) A instalação da solução, incluindo todos os componentes e acessórios, será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pela CONTRATANTE;
- b) Os serviços de implantação somente serão iniciados mediante aprovação da CONTRATANTE.
- c) O prazo para instalação e configuração da solução/plataforma tecnológica, bem como a integração com os dispositivos necessários a serem protegidos (quantidade de dispositivos), deverá ser concluída em no máximo de 30 (trinta) dias corridos contados da data de assinatura do contrato. Nesse prazo, já estão incluídas as reuniões iniciais de alinhamento, aprovação do Plano de Implantação e demais tratativas.
- d) A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
- e) Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração técnicos.
- f) Nos casos de atuações remotas, deverá pré-agendar com a equipe do CONTRATANTE os horários necessários para os acessos necessários de acordo com as políticas de segurança do CONTRATANTE.
- g) As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno e/ou finais de semana, de acordo com a definição do CONTRATANTE.
- h) Nesta etapa, o CONTRATANTE não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe técnica do CONTRATANTE acompanhará os serviços e a console de administração, bem como a integração com os dispositivos do CONTRATANTE, mantendo sempre o alinhamento com a Política de Informação do Tribunal.
- i) A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
- j) Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração técnicos.
- k) Nos casos de atuações remotas, deverá pré-agendar com a equipe do CONTRATANTE os horários necessários para os acessos necessários de acordo com as políticas de segurança do CONTRATANTE.
- l) As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno e/ou finais de semana, de acordo com a definição do CONTRATANTE.
- m) Nesta etapa, o CONTRATANTE não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe técnica do CONTRATANTE acompanhará os serviços e a console de administração, bem como a integração com os dispositivos do CONTRATANTE, mantendo sempre o alinhamento com a Política de Informação do Tribunal.
- n) A critério da CONTRATANTE, a CONTRATADA deverá ela própria realizar as alterações necessárias no ambiente, ou instruir e acompanhar o acompanhante na reconfiguração, de forma síncrona (presencialmente ou remotamente, também a critério da CONTRATANTE).
- o) A configuração final deverá contemplar todas as funcionalidades descritas neste Termo de Referência, necessárias para o alcance do nível de segurança adequado à operação em ambiente de nuvem, incluindo, mas não se limitando, o provisionamento de perfis de acesso, contas de usuário, e duplo fator de autenticação.
- p) A solução, deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários ao seu pleno funcionamento.
- q) A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos dispositivos e softwares que compõem a solução.
- r) A instalação, configuração e testes da solução deverá ser feita com o acompanhamento de técnicos da CONTRATANTE, visando o repasse de conhecimento e observação de gerenciamento de manutenção e segurança da CONTRATANTE.
- s) Deverá ser fornecida documentação de toda a implementação e configuração dos produtos adquiridos.

3.7.4. A data do início da realização dos serviços será acordada entre a CONTRATANTE e a CONTRATADA, e deverá estar contida em um período máximo de 15 dias corridos após a assinatura definitiva das licenças de uso do Tenable One.

- 3.7.5. 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, ou em horário noturno, se for o caso.
- 3.7.6. Atividades associadas à implantação com a necessidade eventual de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estar devidamente planejadas e aprovadas previamente pela equipe técnica da CONTRATANTE.
- 3.7.7. A CONTRATADA deverá comunicar a CONTRATANTE à conclusão da instalação e entregar toda documentação técnica (*As Built*) em até 15 (quinze) dias corridos após a conclusão da instalação, bem como de cada ordem de serviço gerada dos serviços técnicos especializados.
- 3.7.7.1. A documentação técnica (*As Built*), deverá ser aprovada pela equipe da CONTRATANTE, e caso necessário, os ajustes solicitados deverão ser realizados pela CONTRATADA em até 05 (cinco) dias após a análise da equipe da CONTRATANTE.
- 3.7.8. O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 30(trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço.
- 3.7.9. As atividades de instalação deverão ser acompanhadas pela equipe técnica da CONTRATANTE, devendo a CONTRATADA:
- a) Efetuar o repasse técnico através de reunião referente à instalação, implementação e operacionalização da solução, com transferência dos procedimentos básicos de operação utilizados;
 - b) O repasse técnico, procedimentos e operacionalização deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas e utilização da solução.
- 3.7.10. A equipe técnica da CONTRATANTE deverá disponibilizar analistas ou técnicos para o acompanhamento das atividades definidas nos itens acima.
- 3.7.10.1. O serviço deverá ser executado por profissional especializado, que detenha no mínimo a certificação "Tenable Certified Delivery Engineer" referente ao Tenable.sc emitida pelo fabricante Tenable.
- 3.7.11. As atividades de instalação, implementação e operacionalização da solução, que serão acompanhadas pela equipe técnica da CONTRATANTE, e realizadas pela CC deverão ser previstas no Plano de Projeto, conforme definido no item 3.7.2.1, e estas deverão ser distribuídas ou organizadas da melhor maneira possível durante as atividades previstas, para não impactar ou comprometer o prazo de entrega deste item pela CONTRATADA, conforme previsto neste TR.
- 3.7.12. As atividades de instalação, implementação e operacionalização da solução, que serão acompanhadas pela equipe técnica da CONTRATANTE, e realizadas pela CC deverão ser realizadas por profissionais que sejam aptos a demonstrar na prática as principais funcionalidades da solução, particularmente, aquelas relacionadas à mudança de configuração e monitoração da solução.
- 3.7.13. O serviço de instalação, implantação, parametrização e operacionalização somente será considerado entregue:
- 3.7.13.1. Após a aprovação da documentação técnica (*As Built*) pela equipe técnica da CONTRATANTE;
 - 3.7.13.2. Comprovação do pleno funcionamento da solução conforme definido no Plano de Projeto estabelecido no item 3.7.2.1, e;
 - 3.7.13.3. Após de acordo da equipe técnica da CONTRATANTE quanto ao repasse técnico realizado pela CONTRATADA.

ITEM	DESCRIÇÃO	UNID D/ MED
8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	TURM

Especificação técnica mínima

- 3.8.1. Trata-se do serviço de treinamento da solução, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução gestão de todos os componentes da solução de forma que o(s) servidor(es) e/ou colaboradores capacitado(s) possam colocar a solução em produção, bem como planejar configuração no ambiente.
- 3.8.2. O TREINAMENTO, deverá possuir carga horária mínima de 20 (vinte) horas, e deverá ser realizado preferencialmente na forma remota (ao vivo), com emissão de participação, sendo que, a critério do CONTRATANTE, poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação (limitando-se a 4 participantes adicionais do tipo “ouvintes”).
- 3.8.3. O CONTRATANTE solicitará a realização do treinamento à CONTRATADA mediante Abertura - ORDEM DE SERVIÇO (ANEXO I-III), sendo que este deverá ser iniciado (quarenta e cinco) dias corridos após o recebimento da Abertura da ORDEM DE SERVIÇO pela CONTRATADA.
- 3.8.4. A CONTRATADA deverá comprovar, previamente à realização do Treinamento, que o(s) INSTRUTOR(ES) selecionado(s) para ministrar o treinamento possua condizente com o conteúdo programático a ser ministrado, incluindo certificados ou declaração do fabricante da solução.
- 3.8.5. O CONTRATANTE poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca do instrutor. Caso a deficiência sanada sem prejuízo para o andamento do curso, esse será suspenso devendo a CONTRATADA agendar novo curso, sem ônus adicional ao CONTRATANTE.
- 3.8.6. O treinamento deverá, ainda, observar o seguinte:
- a) Deverá oferecer carga horária total de no mínimo 20 (vinte) horas.
 - b) Serão aceitos apenas treinamento online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.
 - c) A CONTRATADA deve prover capacitação técnica em turma com no máximo 10 (dez) participantes.
 - d) Se o treinamento na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.
 - e) Possuir o conteúdo organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos para fixação;
 - f) Incluir apostilas e manuais dos equipamentos e softwares necessários para a prática dos exercícios propostos no material do treinamento;
 - g) Prover os acessos que irão compor o laboratório do treinamento que deverão ser iguais aos adquiridos pelo ou, quando não for possível, por ambientes similares e funcionalidades;
 - h) Abranger todas as funcionalidades especificadas nesta especificação técnica;
 - i) Serem fornecidos certificados de participação para cada participante (exceto para aqueles na condição de ouvintes);
 - j) Todos os manuais, apostilas e demais documentos devem estar nos idiomas Português (ou Inglês, quando não disponíveis em Português); e
 - k) Os cursos devem ser ministrados no idioma Português.
- 3.8.7. Após realização do curso será feita uma avaliação de satisfação junto aos participantes, cujo resultado deverá alcançar a média de, pelo menos, 70% (setenta por cento) dentre os critérios avaliados, para validação e emissão do Termo de Aceite Definitivo. Caso não alcance o resultado esperado, o treinamento deverá ser ministrado novamente.
- 3.8.8. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão responsabilidade da CONTRATADA.
- 3.8.9. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.
- 3.8.9.1. A licitante proponente deverá entregar, na fase de habilitação, uma declaração afirmando que oferta o treinamento da solução e que a ementa e todo o material oferecido pelo fabricante da solução, bem como, indicar na proposta o calendário contendo as datas e as localidades de realização do Treinamento.
- 3.8.9.2. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o treinamento ofertado atende os requisitos indicados.
- 3.8.9.3. É facultado ao Tribunal a realização de diligências e verificação da autenticidade da declaração e demais documentos comprobatórios.
- 3.8.10. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de vigência do Contrato, a contar da entrega do calendário.
- 3.8.11. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação da solução, ficando a critério da administração e calendário a ser fornecido pela contratada.
- 3.8.12. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato.
- 3.8.13. A contratada deverá fornecer material didático individual que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização deverá ser atualizado e poderá estar em inglês ou português.
- 3.8.15. A pedido do Contratante, o treinamento poderá ser gravado e disponibilizado ao Fiscal da CONTRATANTE;
- 3.8.16. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 5 (cinco) dias úteis após o término do treinamento, a conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia desse certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.
- 3.8.16.1. O certificado de conclusão do curso deverá ser emitido pelo fabricante ou pela empresa a ser contratada.
- 3.8.17. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor.
- 3.8.18. O treinamento ofertado deve seguir os modelos padrão de capacitação disponíveis no mercado naquilo que couber.
- 3.8.19. Não serão aceitos treinamentos não oficiais ou cujo conteúdo ministrado não abranja a utilização da solução para o fim a que se destina, bem ainda, aqueles cujos resultados forem emitidos no prazo máximo de 5 dias contados da conclusão da capacitação.
- a) A não aceitação da capacitação implicará no não pagamento dos serviços realizados.
 - b) A empresa a ser contratada deverá emitir certificados de participação contendo a exata carga horária do treinamento e a participação do treinando.
- 3.8.20. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo constante no Anexo deste Termo de Referência (Anexo I-VII - Formulário de avaliação - Treinamento da solução).
- a) No Formulário, será utilizada escala de até 5 (cinco) pontos para cada quesito. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para ser considerado proveitoso.
 - b) O resultado da Avaliação de Instrutor/Tutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como “provavelmente satisfatório” (6 ou mais) dos 10 (dez) itens avaliados;
 - c) Caso o resultado da Avaliação de Instrutor/Tutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito;
 - d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE;
 - e) Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

ITEM	DESCRIÇÃO	UNID D/ MED
9	Serviço de Suporte Técnico com Operação Assistida, pelo período de 60 (sessenta) meses.	SERVI

Especificação técnica mínima

3.9.1. Definição e Objetivo: O serviço de Operação Assistida consiste no acompanhamento e suporte técnico especializado, prestado por profissional da CONTRATADA, com o objetivo de assegurar a correta utilização, otimização e a transferência de conhecimento da solução de Gerenciamento de Exposição Cibernética para a equipe técnica da CONTRATANTE.

incluem:

- a) Esclarecimento de dúvidas técnicas avançadas sobre a operação da plataforma;
- b) Auxílio na análise e ajuste fino de configurações para otimizar o desempenho e a precisão dos resultados;
- c) Apoio na interpretação de dados e na elaboração de estratégias de correção para vulnerabilidades identificadas;
- d) Orientação sobre as melhores práticas para a integração contínua de novos ativos do Tribunal à solução.

3.9.2. Distinção de Outros Serviços: Este serviço é de natureza consultiva e complementar, não se confundindo com:

- a) **Serviços de Implantação:** Atividades relacionadas à instalação e configuração inicial da solução.
- b) **Serviços de Suporte Técnico e Garantia do Fabricante:** Atendimento para correção de falhas, bugs e defeitos da solução, já contemplado na garantia do produto.

3.9.3. Execução e Agendamento

- a) O serviço de Operação Assistida estará disponível à CONTRATANTE a partir da assinatura do contrato e durante toda a sua vigência.
- b) A CONTRATANTE poderá solicitar, mensalmente, no mínimo, 2 (duas) até 4 (quatro) sessões de Operação Assistida, que poderão ser utilizadas em sessões de, no mínimo, duração cada.
- c) As sessões deverão ser agendadas com antecedência mínima de **5 (cinco) dias úteis**, em comum acordo entre as partes, e realizadas remotamente (por videoconferência dentro do horário de expediente do Tribunal.
- d) A primeira sessão deverá ser realizada em até **10 (dez) dias úteis** após a conclusão do serviço de implantação, com foco na validação das integrações e no acompanhamento inicial de varredura e análise.

3.9.3.1. Regras da Franquia de Horas: A franquia de horas mensais de Operação Assistida não é cumulativa. As horas não utilizadas dentro de um determinado mês não são transferidas para os meses subsequentes.

3.9.4. Atendimento a Chamados Técnicos (Suporte e Garantia): Para demandas relacionadas a defeitos, falhas de funcionamento ou indisponibilidade da solução (Suporte e Garantia), o atendimento deverá ser realizado por telefone e/ou portal web da CONTRATADA. A cobertura mínima para este serviço será de 8 (oito) horas por dia, 5 (cinco) dias úteis (8x5), em horário comercial (08:00 às 18:00, horário de Brasília), com tempos de resposta e solução definidos no Acordo de Nível de Serviço (ANS) deste Termo de Referência.

3.9.4.1. O atendimento deve ser realizado por um profissional especializado da CONTRATADA, que possua, pelo menos, uma das seguintes certificações:

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

3.9.5. O suporte direto do fabricante da solução deverá ser fornecido para atualizações de versão e resolução de problemas, além do suporte técnico com operação assistida pela CONTRATADA e previsto neste Termo de Referência e seus Apêndices. O suporte do fabricante, quando necessário, será realizado em conjunto com a CONTRATADA e fora do horário de vigência contratual.

3.9.6. Escopo de Atividades da Operação Assistida: No âmbito do serviço de Operação Assistida, a CONTRATADA deverá, mediante solicitação da CONTRATANTE, executar as seguintes atividades e fornecer os entregáveis correspondentes, utilizando a franquia de horas contratada.

3.9.6.1. Configuração, Integração e Otimização da Solução:

- a) **Orientação e Transferência de Conhecimento:** Instruir a equipe técnica da CONTRATANTE sobre a instalação, configuração e utilização de todos os componentes da solução, incluindo console de gerenciamento, agentes e sensores.
- b) **Parametrização Avançada:** Definir e executar políticas de varredura (scans) avançadas e customizadas, de acordo com as necessidades e os ativos de TIC do Tribunal.
- c) **Integração de Sistemas:** Executar a implementação de novas integrações da solução com outras ferramentas do ambiente da CONTRATANTE que se mostrarem necessárias para o funcionamento da solução.
- d) **Manutenção da Estabilidade:** Diagnosticar e corrigir comportamentos instáveis ou inadequados da plataforma, garantindo seu pleno funcionamento.
- e) **Atualização e Evolução:** Planejar e executar os procedimentos de atualização para novas versões da solução, avaliando e mitigando o impacto nos agentes e sensores instalados.

3.9.6.2. Gestão de Vulnerabilidades e Remediação:

- a) **Análise Qualificada:** Realizar análises técnicas aprofundadas sobre as vulnerabilidades identificadas, provendo orientação para a aplicação de correções e patches.
- b) **Priorização Estratégica:** Propor a priorização para tratamento de vulnerabilidades com base em critérios técnicos, como o *Vulnerability Priority Rating (VPR)* do ambiente do Tribunal, com ênfase especial naquelas com VPR superior a 9.0.
- c) **Planos de Ação:** Elaborar, em conjunto com a equipe da CONTRATANTE, planos de ação detalhados para a mitigação e correção das vulnerabilidades críticas identificadas.
- d) **Acompanhamento do Ciclo de Vida:** Apoiar o monitoramento do ciclo de vida das vulnerabilidades, desde a identificação até o fechamento, utilizando as ferramentas e projetos de remediação.
- e) **Correção na Própria Solução:** Executar a correção de eventuais vulnerabilidades identificadas nos próprios servidores que hospedam a solução de gerenciamento.

3.9.6.3. Inteligência, Relatórios e Documentação:

- a) **Dashboards e Relatórios:** Configurar e parametrizar painéis (*dashboards*) e relatórios para o monitoramento contínuo da exposição cibernética, adequados aos requisitos operacionais.
- b) **Documentação Técnica:** Elaborar e manter atualizada a documentação de todas as configurações, políticas e integrações implementadas na solução durante as atividades de operação assistida.
- c) **Transferência de Conhecimento:** Formalizar e repassar o conhecimento sobre as atividades técnicas executadas sempre que solicitado pela CONTRATANTE para a autonomia da equipe interna.

3.9.6.4. Suporte Estratégico:

- a) **Melhoria Contínua:** Realizar estudos proativos do ambiente e propor melhorias contínuas nas políticas de segurança, configurações e processos de gestão de vulnerabilidades.
- b) **Planejamento e Migração:** Fornecer suporte consultivo para o planejamento de migrações, adequações e expansão do uso de agentes e sensores no parque tecnológico da CONTRATANTE.
- c) **Diagnóstico Avançado:** Atuar como um ponto de escalonamento para o diagnóstico de problemas técnicos complexos e análise de tendências relacionadas ao uso da solução.

3.9.7. Os relatórios e indicadores da solução devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados. Esse profissional deve apresentá-lo de forma presencial nas dependências da CONTRATADA ou de forma virtual, por meio de solução de videoconferência.

3.9.8. Não estão contemplados problemas relacionados a hardware e/ou Internet para acesso à plataforma/ambiente da solução SaaS, uma vez que os recursos físicos serão de responsabilidade da CONTRATANTE.

3.9.9. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração com

do CONTRATANTE, configuração de novas funcionalidades, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

3.9.10. Para os casos em que houver alguma mudança significativa de atualização de versão, que reflita na operação da solução, a CONTRATADA deverá ocorrer a atualização de conhecimento para equipe interna do CONTRATANTE sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4” (Conforme Item 3.9.12).

3.9.11. A CONTRATADA deverá fornecer um sistema para monitorar e controlar chamados, permitindo o acesso apenas aos membros autorizados da equipe técnica do CONTRATANTE.

3.9.11.1. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe do CONTRATANTE.

3.9.11.2. A CONTRATADA deverá disponibilizar o acesso à Central de Atendimento através de plataforma online, e-mail, número de telefone local ou DDG (número de abertura de chamados de suporte técnico, conforme períodos, horários e condições estabelecidas neste TR).

3.9.12. Os serviços serão prestados de forma remota observando as seguintes condições:

- O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.
- As sessões remotas, a critério do CONTRATANTE, poderão ser gravadas, seguindo todas as diretrizes de segurança pré-estabelecidas, possibilitando a documentação posterior consulta pelo Tribunal.
- A CONTRATADA deverá, para cada vulnerabilidade encontrada no ambiente do CONTRATANTE, propor solução documentada no escopo do chamado; disponibilizar o especialista (AD, LINUX, Firewall, etc) para orientar quanto à aplicação da solução, quando for o caso.
- Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

NÍVEL DE SEVERIDADE	DESCRIÇÃO	PRAZO MÁXIMO DE INÍCIO DE ATENDIMENTO	PRAZO MÁXIMO PARA PROPOSTA DE SOLUÇÃO
Urgente / Crítica Severidade 1	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente. Normalmente associado à vulnerabilidade(s) onde pessoas mal intencionadas podem facilmente obter o controle do ativo ou <i>host</i> . As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e <i>backdoors</i> .	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 1 (um) dia após abertura do chamado remoto.
Alta Severidade 2	Impacto de alta significância relacionado à utilização do ambiente: vulnerabilidade que, se explorada, pode ocasionar indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 3 (três) dias após abertura do chamado remoto.
Média Severidade 3	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto	Até 8 (oito) dias após abertura do chamado remoto.
Baixa Severidade 4	Consulta e/ou dúvida técnica e/ou transferência de conhecimento	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 10 (dez) dias após a abertura do chamado remoto.
Informação Severidade 5	Exposição ou vulnerabilidade que, se explorada, poderá possibilitar a coleta de informações sobre o <i>host</i> por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias após a abertura do chamado remoto.

3.9.12.1. O nível de severidade será atribuído pela equipe autorizada do CONTRATANTE no momento da abertura do chamado e poderá ser reclassificado pela equipe da contratada caso necessário.

3.9.12.2. Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que o CONTRATANTE responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que esteja fora do escopo de atuação da CONTRATADA.

3.9.12.3. Durante o período de vigência do contrato a CONTRATADA deverá apresentar mensalmente relatório em formato eletrônico, contendo todos os chamados ocorridos no período, contendo informações analíticas e sintéticas de cada chamado, contendo a lista e total de chamados concluídos dentro e fora do prazo de SLA estabelecido.

3.9.12.4. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

3.9.12.5. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorreu o incidente até a mesma hora do último dia, conforme os prazos.

Manutenção de Sigilo e Normas de Segurança

3.9.13. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer utilização ou divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

- Todas as informações, imagens, aplicativos e documentos providos pela CONTRATANTE ou oriundos das informações que forem propriedade da CONTRATADA, manuseados e utilizados, são de propriedade da CONTRATANTE, não podendo ser repassadas, copiadas, alteradas ou absorvidas na relação de bens da CONTRATADA, como, de seus executores, sem expressa autorização da CONTRATANTE.
- Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).
- Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da CONTRATANTE.
- Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.
- A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

3.9.14. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante da Contratada e Profissional responsável pela execução dos serviços.

3.9.15. A prestação de serviços de que trata este Termo de Referência não gera vínculo empregatício entre os empregados da contratada e o CONTRATANTE, vedando a contratação de terceiros para substituição direta.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Os requisitos necessários e suficientes à escolha da solução de TIC, encontram-se pormenorizada no tópico 2 do Estudo Técnico Preliminar, destacando-se os seguintes tópicos atualizados:

4.2. Indicação e/ou vedação de marcas ou modelos (Art. 41, incisos I e III, da Lei nº 14.133, de 2021)

4.2.1. Há indicação na especificação do objeto de marca e/ou modelo, em razão da necessidade de manter padronização, continuidade e compatibilidade com as soluções já existentes nos órgãos participantes, entre outros motivos, conforme justificativas detalhadas no item 2.23 do ETP.

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

4.3. Da exigência de carta de solidariedade

4.3.1. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

4.4. Da possibilidade de subcontratação

4.4.1. Não será admitida a subcontratação para a contratação.

4.5. Exigência de amostra e/ou prova de conceito

4.5.1. Não será exigido amostra ou prova de conceito, tendo em vista as características da solução e os requisitos e informações exigidos na apresentação da proposta e aceitação do objeto.

4.6. Garantia, manutenção e assistência técnica

4.6.1. A contratada deverá ofertar garantia do fabricante, por no mínimo 60 (sessenta) meses. A garantia deve cobrir o prazo de vigência das licenças, sendo prorrogada em caso de renovação contratual.

4.6.2. 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.

4.6.3. 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.

4.6.4. 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.

4.6.5. 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.

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

4.6.7. 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.

4.6.8. 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.

4.6.9. 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.

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

4.6.11. 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.

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

4.7. Requisitos legais

4.7.1. O presente 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 - SISF 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 - SISF 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/IEC27017 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.

4.7.2. 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.

4.8. Critérios e práticas de sustentabilidade

4.8.1 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.

4.9. Requisitos sociais, ambientais e culturais

4.9.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PTBR e fornecidos em meio digital.

4.9.2. O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.

4.9.3. 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.

4.9.4. 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;

4.9.5. No que se refere aos aspectos culturais e sociais, os funcionários e colaboradores deverão atender somente demandas relacionadas com o objeto a ser contratado;

4.9.6. 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;

4.9.7. 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;

4.10. Garantia da Contratação

4.10.1. Será exigida a garantia contratual da execução, nos termos do art. 96 da Lei 14.133/2021, no percentual de **5%** do valor contratado, tendo em vista o vulto da contratação e os riscos inerentes à execução de uma contratação compartilhada.

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

4.11. Requisitos de Segurança e Privacidade

4.11.1 A Contratada deverá atender aos requisitos de segurança e privacidade, conforme a seguir:

4.11.2. 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).

4.11.3. 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.

4.11.4. 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).

4.11.5. 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 Nº 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;

4.12. Requisitos de capacitação

4.12.1. Haverá a necessidade de treinamento, conforme especificação e descrição da solução dos itens 3 e 8 deste TR.

4.12.2. 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.

4.12.3. 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.

4.13. Requisitos de experiência profissional

4.13.1. 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.

4.13.2. 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

4.14. Requisitos da Arquitetura Tecnológica

4.14.1. 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.

4.14.2. 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.

4.14.3. A arquitetura da Solução de Segurança Cibernética 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.

4.14.4. 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.

4.14.5. 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.

4.15. Requisitos de Projeto e Implementação

4.15.1. 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 requisição 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.

4.16. Requisitos de implantação

4.16.1. 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.

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

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

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

4.16.5. 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.

4.17. Requisitos de formação da equipe

4.17.1. 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.

4.17.2. 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.

4.17.3. 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.

4.17.4. 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.

4.18. Requisitos de segurança da informação

4.18.1 A CONTRATADA deverá manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE, ou de terceiros, de que tomar conhecimento.

4.18.2. As informações sob custódia do fornecedor deverão ser tratadas como informações sigilosas, não podendo ser usadas por este fornecedor ou fornecidas sem autorização formal da CONTRATANTE.

4.18.3. A solução contratada deverá possuir recursos que possibilitem a definição de regras e configurações aderentes à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

4.18.4. A quebra do sigilo das informações restritas, devidamente comprovada, sem autorização expressa do CONTRATANTE, possibilitará a imediata rescisão de contrato, sem qualquer ônus para o CONTRATANTE, ensejando a reparação por perdas e danos sofridos pela CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas.

4.19 Requisitos de Metodologia de Trabalho

4.19.1. A dinâmica de execução do objeto, a forma de encaminhamento das demandas, os prazos, locais e mecanismos de comunicação, entre outros, estão descritos no tópico 6 (modelo de execução do contrato).

4.20. Vistoria

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

4.21. Da participação de consórcios

4.21.1. Não será permitida a participação de empresas em consórcio, conforme justificativas constantes do ETP.

4.22. Da participação de cooperativas

4.22.1. 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.

4.23. Da participação de pessoa física

4.23.1. Não será permitida a participação de pessoas físicas, pois a presente contratação exige estrutura mínima da contratada, com equipamentos, instalações e equipe de profissionais ou corpo técnico para a execução do objeto incompatíveis com a natureza profissional da pessoa física (art. 4º da IN SEGES /ME nº 116/2021).

4.24. Necessidade de transição contratual

4.24.1. Durante a instalação e configuração da solução, a contratada deverá realizar transferência de conhecimentos do tipo “hands on” relativos às funções disponíveis nos equipamentos, sua operação e manutenção.

4.24.2. Os procedimentos de transição e finalização do contrato estão descritos no item 6.6 deste TR.

4.24.3. A contratada obriga-se a fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

4.25.4. O ETP, no tópico 2.25, descreve com detalhes as estratégias de continuidade da solução, de independência do TRE-PA em relação à Contratada, as ações de encerramento e transição contratual e os direitos de propriedade intelectual sobre os ativos gerados/manuseados e documentação técnica.

4.25. Margem de Preferência

4.25.1. Não será aplicada em razão da ausência de regulamentação da norma de eficácia limitada (art. 26, incisos I e II, da Lei nº 14.133, de 2021).

5. PAPÉIS E RESPONSABILIDADES

Obrigações do contratante e do contratado

5.1. São obrigações da CONTRATANTE

5.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com o contrato e seus anexos.

5.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

5.1.3. Notificar o CONTRATADO, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas.

5.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo CONTRATADO.

5.1.5. Comunicar o CONTRATADO para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.

5.1.6. Efetuar o pagamento ao CONTRATADO do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente contrato.

5.1.7. Aplicar ao CONTRATADO as sanções previstas na lei e neste contrato.

5.1.8. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo CONTRATADO, quando for o caso.

5.1.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

5.1.9.1. A Administração terá o prazo de **1 (um) mês**, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

5.1.9.2. A decisão será tomada pelo fiscal do contrato, pelo gestor do contrato ou pela autoridade superior, nos limites de suas competências.

5.1.10. Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pelo CONTRATADO no prazo máximo de 1 (um) mês.

5.1.11. Quando exigida garantia contratual, notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

5.1.12. A Administração não responderá por quaisquer compromissos assumidos pelo CONTRATADO com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do CONTRATADO, de seus empregados, prepostos ou subordinados.

5.1.13. Quando solicitado, o gestor do contrato deverá fornecer o e-mail para o qual deverão ser encaminhadas os registros de licenças referentes ao objeto do Contrato.

5.1.14. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

5.1.15. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.1.16 Não praticar atos de ingerência na administração da Contratada, tais como:

1. exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário (estabelecer vínculo de subordinação com funcionários da contratada);

2. direcionar a contratação de pessoas para trabalhar nas empresas Contratadas (indicar pessoas para compor o quadro funcional da contratada);

3. promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado (demandar a execução de serviços ou tarefas estranhas ao objeto da contratação, mesmo que haja anuência do preposto ou da própria contratada);
4. considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens (reembolsar despesas com transporte, hospedagem e outros custos operacionais, que devem ser de exclusiva responsabilidade da contratada);
5. Prever em edital a remuneração dos funcionários da contratada;
6. Prever em edital exigências que constituam intervenção indevida da Administração na gestão interna dos fornecedores;
7. Prever em edital exigência que os fornecedores apresentem, em seus quadros, funcionários capacitados ou certificados para o fornecimento da solução, antes da contratação;
8. Adotar a métrica homem-hora ou equivalente para aferição de esforço, salvo mediante justificativa e sempre vinculada à entrega de produtos de acordo com prazos e qualidade previamente definidos;
9. Contratar por postos de trabalho alocados, salvo os casos justificados mediante a comprovação obrigatória de resultados compatíveis com o posto previamente definido;
10. Fazer referências, em edital ou em contrato, a regras externas de fabricantes, fornecedores ou prestadores de serviços que possam acarretar na alteração unilateral do contrato por parte da contratada.

5.2. São obrigações do CONTRATADO

5.2.1. O CONTRATADO deve cumprir todas as obrigações constantes deste Termo de Referência e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

- 5.2.1.1. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078/1990).
- 5.2.1.2. Comunicar ao CONTRATANTE, no prazo máximo de **10 (dez) dias úteis** que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
- 5.2.1.3. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei nº 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados.
- 5.2.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.
- 5.2.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo CONTRATANTE, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos.
- 5.2.1.6. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT.
- 5.2.1.7. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE e não poderá onerar o objeto do contrato.
- 5.2.1.8. Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.
- 5.2.1.8.1. Comunicar imediatamente ao fiscal do contrato qualquer a ocorrência de falha crítica ao sistema, que possa comprometer a integridade de todo o sistema.
- 5.2.1.9. Paralisar, por determinação do CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 5.2.1.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.
- 5.2.1.11. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (**caput do art. 116 da Lei nº 14.133, de 2021**).
- 5.2.1.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei nº 14.133, de 2021).
- 5.2.1.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.
- 5.2.1.14. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE.
- 5.2.1.15. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.
- 5.2.1.16. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709/2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato.
- 5.2.1.17. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.
- 5.2.1.18. Submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congêner.
- 5.2.1.19. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.
- 5.2.1.20. Obriga-se a fornecer à CONTRATANTE, ao final do serviço de instalação (ITEM 4) o As-Built, com relatório de implementação com todas as atividades e ações realizadas, devidamente registradas e com evidências, condicionado à aprovação pela equipe da CONTRATANTE; de forma que a equipe técnica do Tribunal possa entender e realizar, quando necessário, o procedimento de instalação/configuração.
- 5.2.1.21. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.
- 5.2.1.22. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.
- 5.2.1.23. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, Logs do Sistema, os modelos de dados e as bases de dados à Administração.
- 5.2.1.24. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

5.3. São obrigações do órgão gerenciador do registro de preços

- 5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- 5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

- 5.3.3.1. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- 5.3.3.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
- 5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
- 5.3.4.1. A definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- 5.3.4.2. As regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo Contratado; e
- 5.3.4.3. As regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

Obrigações pertinentes à LGPD

- 5.4. A presente contratação envolve o tratamento de dados pessoais, motivo pelo qual deverão ser incluídas no termo de contrato as condições de cumprimento da [Lei nº 13.709, de 14 de agosto de 2018 \(LGPD\)](#).
- 5.4.1. As partes deverão cumprir o disposto na **Lei nº 13.709, de 14 de agosto de 2018 (LGPD)**, na **Resolução TRE/PA nº 5.699/2021** (Política Geral de Privacidade e Proteção de Dados Pessoais (PGPD) no âmbito do TRE-PA) e na Resolução/TSE nº 23.644/2021 (Dispõe sobre a Política de Segurança da Informação - PSI, no âmbito da Justiça Eleitoral) quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
- 5.4.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.
- 5.4.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.
- 5.4.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.
- 5.4.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.
- 5.4.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
- 5.4.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.
- 5.4.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.
- 5.4.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.
- 5.4.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.
- 5.4.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.
- 5.4.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.
- 5.4.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Forma/regime de execução: empreitada por preço global.

Condições de execução

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

ETA PA	DESCRIÇÃO	PRODUTOS FINAIS A SEREM ENTREGUES	PRAZO MÁXIMO DA ENTREGA
1	Disponibilização das Licenças e Planejamento Inicial	1. Chaves de licença/subscrição ativadas e disponíveis para o CONTRATANTE. 2. Ata da Reunião Inicial (Kick-off) realizada. 3. Plano de Projeto detalhado, contendo o cronograma de implantação (quando houver), migração (para os itens 4 e 5), e configuração, submetido para aprovação.	Até 15 (quinze) dias corridos, contados do recebimento da Ordem de Serviço.
2	Execução dos Serviços de Implantação, Migração (Upgrade) e Configuração	1. Para os Itens 4 e 5 (Upgrade): Ambiente legado migrado para a plataforma Tenable One, com dados e configurações preservados. 2. Para o Item 6 (Novas Licenças): Ambiente Tenable One instalado e configurado. 3. Solução integrada aos ativos do CONTRATANTE, em pleno funcionamento e com todos os testes operacionais concluídos. 4. Documentação técnica da implantação ("As Built") entregue.	Até 30 (trinta) dias corridos, contados da aprovação do Plano de Projeto pelo CONTRATANTE.
3	Capacitação Técnica (Treinamento)	1. Treinamento realizado conforme o conteúdo programático 2. Material didático entregue aos participantes. 3. Certificados de participação emitidos.	A ser realizado conforme agendamento, em até 45 (quarenta e cinco) dias corridos após a solicitação específica via Ordem de Serviço.

4	Início dos Serviços Contínuos (Operação Assistida e Suporte)	1. Canais de suporte técnico plenamente operacionais. 2. Primeira sessão mensal de Operação Assistida agendada e/ou realizada. <i>(Este serviço será prestado continuamente ao longo dos 60 meses de vigência contratual)</i>	Início da disponibilização em até 5 (cinco) dias úteis após a emissão do Termo de Recebimento Provisório da Etapa 2.
---	---	---	--

Do Encaminhamento Formal de Demandas

- 1) O gestor do contrato emitirá a Ordem de Serviço para a entrega/execução dos itens da solução, conforme ANEXO III AO TERMO DE REFERÊNCIA.
- 2) O Contratado deverá fornecer os itens com as mesmas configurações e quantidades definidas na Ordem de Serviço.

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 Serviço.

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 Serviço 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

- 6.3. 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 Serviço (OS)
- 6.3.1. Os serviços de garantia, manutenção, suporte e assistência técnica serão prestados 24h/dia, 7 dias na semana.
- 6.3.2. A demanda de serviços será encaminhada à CONTRATADA por meio de documentos oficiais de comunicação definidos neste Instrumento.
- 6.3.3. Fica a critério do CONTRATANTE, definir o horário de instalação e configuração da solução.
- 6.3.4. 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.

Informações relevantes para o dimensionamento da proposta

- 6.3. De acordo com o art. 12, §4º da Instrução Normativa SGD/ME nº 94, de 2022, nas licitações por preço global, cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 26 da Lei nº 14.133, de 2021.
- 6.4. Estimativa de demanda dos Tribunais Regionais Eleitorais interessados na contratação.
- 6.4.1. Para a contratação que trata este TR, optou-se por utilizar o procedimento de contratação conjunta comumente utilizada na Estratégia Nacional de Cibersegurança TSE e TREs, o qual permite a modalidade de compra por mais de um Tribunal interessado na solução em razão da necessidade de padronização de tecnologias, visando atender a arquitetura proposta na [Estratégia Nacional de Segurança Cibernética do Poder Judiciário \(ENSEC-PJ\)](#).
- 6.4.3. Visando a compilação 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	SERV
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

6.4.4. O quadro a seguir consolida as respostas recebidas dos TREs e TSE, partícipes desta Contratação, quanto à concordância 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):

REGIONAL	OFÍCIO	EVENTO
TRE-AM	Ofício nº 78/2025 TRE-AM/GAB-DG	2812460
TRE-ES	Ofício nº 2909 - TRE-ES/PRE/DG/STI	2818229
TRE-AL	Ofício nº 2704 TRE-AL/PRE/DG/GDG	2807575
TRE-DF	Ofício nº 1174 - TRE-DF/PR/DG/GDG	2807576
TRE-GO	Ofício nº 215/2025 - TRE-GO/DG	2807577
TRE-TO	Ofício nº 3776/2025 - TRE-TO/PRES/DG/STI/ASCIBER	2807578
TRE-MG	Ofício nº 1955 TRE-MG 1955/2025 - DG	2807579
TRE-MT	Ofício nº 86/2025 - TRE-MT/GAB/DG	2807580
TRE-AP	Ofício nº 1698/2025 TRE-AP/PRE/DG/GAB-DG	2807582
TRE-MA	Ofício nº 6746/2025 - TRE-MA/PRES/DG	2804530

TRE-BA	Ofício nº 1777/2025 - TRE-BA/PRE/DG/ASSED	2807583
TRE-CE	Ofício N ° 1647/2025 TRE-CE	2807584
TRE-MS	Ofício nº 3426 TRE-MS/PRE/DG/GABDG	2808902
TRE-PB	Ofício N ° 90/2025 - TRE-PB/PRE/DG	2807585
TRE-PI	Ofício N ° 67/2025 - TRE-PI/PRE/DG	2807586
TRE-PR	Ofício nº 838/2025 TRE-PR/DG	2807587
TRE-RJ	Ofício nº 157/2025 - TRE-RJ/DG	2807588
TRE-RN	Ofício nº 191/2025 - TRE-RN/DG	2808615
TRE-RO	Ofício nº 170 / 2025 - PRES/DG/GABDG	2811462
TRE-SE	Ofício nº 2697/2025 - TRE-SE/DG	2808925
TRE-SP	Ofício nº 1909/2025 - TRE-SP/DG	2807589
TSE	Ofício nº 852/2025 - TSE/GAB-DG	2808774

Formas de transferência de conhecimento

6.5. A Contratada deverá promover a contínua transferência de conhecimento sobre a solução implantada para a equipe técnica designada pelo CONTRATANTE, visando a sua autonomia operacional e a garantia de uma transição contratual eficiente ao final do contrato.

Distingue-se a **capacitação** (treinamento formal sobre as funcionalidades da ferramenta) da **transferência de conhecimento**, que consiste no repasse de informações e experiências específicas sobre a implantação, configuração, operação e manutenção da solução no ambiente particular do CONTRATANTE.

Essa transferência ocorrerá por meio dos seguintes mecanismos:

a) Repasse Técnico Durante a Execução: Durante os serviços de implantação, configuração e migração (Item 7 do Grupo 2) , e ao longo de todo o serviço de Operação Assistida (Item 9 do Grupo 2), a equipe da Contratada deverá detalhar e explicar todos os procedimentos executados, as configurações aplicadas e as lógicas adotadas, sanando dúvidas da equipe do CONTRATANTE.

b) Documentação Técnica Completa e Atualizada: A Contratada deverá elaborar e entregar a documentação "As Built" de toda a implementação, detalhando a arquitetura, as integrações, as políticas e as customizações realizadas. Este documento, de propriedade do CONTRATANTE, deverá ser mantido atualizado sempre que ocorrerem alterações significativas no ambiente.

c) Reuniões de Acompanhamento Técnico: Realização de reuniões periódicas, a critério do fiscal do contrato, para discutir a evolução do ambiente, os incidentes tratados, as otimizações realizadas e outras informações técnicas relevantes para a gestão da solução.

d) Plano e Execução de Transição Contratual: Conforme previsto no ETP, ao término do contrato ou quando solicitado, a Contratada obriga-se a colaborar ativamente no processo de transição para uma nova empresa ou para a equipe interna do Tribunal, garantindo o repasse integral de todas as informações e conhecimentos necessários para a continuidade das operações sem perda de informações.

Procedimentos de transição e finalização do contrato

6.6. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

- a) entrega de versões finais dos produtos alvos da contratação como, por exemplo, arquivos de configuração;
- b) transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação;
- d) revogação de perfis de acesso.

Quantidade mínima de serviços para comparação e controle

6.7. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no ANEXO III.

Formas de Pagamento

6.8. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio no item "8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO".

Manutenção de Sigilo e Normas de Segurança

6.9. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.10. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXO I - I e ANEXO I - II.

6.11. É vedada a veiculação de publicidade acerca do contrato;

6.12. Os requisitos de segurança estão descritos na Resolução TSE Nº 23.644, de 1º de julho de 2021, que Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

7.6. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

Reunião Inicial

7.7. Em consonância ao Art. 31 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, após a assinatura do Contrato, a CONTRATANTE convocará reunião, a ser registrada em ata, podendo ser prorrogada a critério da Contratante.

7.7.1. As reuniões poderão ser presenciais ou virtuais. Quando virtuais, será utilizada a plataforma designada pela CONTRATANTE ou pela CONTRATADA.

7.7.2. A reunião será convocada pelo Gestor do Contrato com a participação da Equipe de Fiscalização do Contrato, da Contratada e dos demais interessados por ele identificados, cuja pauta observará, pelo menos:

- a) presença do representante legal da contratada, que apresentará o seu preposto;
- b) entrega, por parte da contratada, do Termo de Compromisso e dos Termos de Ciência; e
- c) esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.3. O Gestor do Contrato deverá apresentar o plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

7.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)), nos termos dos arts. 21 a 26 da Res. CNJ 468, de 2022, do art. 33 da IN SGD nº 94, de 2022, no que couber, observando-se, em especial, as orientações do Guia de Contratações de STIC do Poder Judiciário (Anexo I da Resolução CNJ 468/22) e as as rotinas a seguir.

Fiscalização Técnica

7.9. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da [IN SGD nº 94, de 2022](#), acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. ([Decreto nº 11.246, de 2022, art. 22, VI](#));

7.9.1. O fiscal técnico do contrato anotarà no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#), e [Decreto nº 11.246, de 2022, art. 22, II](#));

7.9.2. Identificada qualquer inexistência ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#));

7.9.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. ([Decreto nº 11.246, de 2022, art. 22, IV](#)).

7.9.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas apazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. ([Decreto nº 11.246, de 2022, art. 22, V](#)).

7.9.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual. ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

Fiscalização Administrativa

7.10. O fiscal administrativo do contrato, além de exercer as atribuições previstas no [art. 33, IV, da IN SGD nº 94, de 2022](#), verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário ([Art. 23, I e II, do Decreto nº 11.246, de 2022](#)).

7.10.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; ([Decreto nº 11.246, de 2022, art. 23, IV](#)).

Gestor do Contrato

7.11. O gestor do contrato, além de exercer as atribuições previstas no [art. 33, I, da IN SGD nº 94, de 2022](#), coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. ([Decreto nº 11.246, de 2022, art. 21, IV](#)).

7.12. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotarà os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. ([Decreto nº 11.246, de 2022, art. 21, III](#)).

7.13. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. ([Decreto nº 11.246, de 2022, art. 21, II](#)).

7.14. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. ([Decreto nº 11.246, de 2022, art. 21, VIII](#)).

7.15. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o [art. 158 da Lei nº 14.133, de 2021](#), ou pelo agente ou pelo setor com competência para tal, conforme o caso. ([Decreto nº 11.246, de 2022, art. 21, X](#)).

7.16. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. ([Decreto nº 11.246, de 2022, art. 21, VI](#)).

7.17. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

Níveis Mínimos de Serviço Exigidos

8.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação.

8.1.1. A verificação da qualidade constitui-se em procedimento indispensável para a fiscalização e a gestão de contratos de serviços da Administração Pública. Proporciona a devida verificação na medida em que o que está sendo entregue ao longo do ciclo de vida da solução efetivamente corresponde ao resultado esperado (ou planejado). Nesse sentido, indicadores de níveis de serviços deve ser estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação, observando-se o conjunto mínimo de indicadores capaz de assegurar a efetiva prestação de serviço com a qualidade esperada para contratação de software e de serviços relacionados ao objeto.

8.1.2. O gerenciamento dos níveis mínimos de serviço consiste no monitoramento e controle da qualidade na execução dos serviços em função dos resultados pretendidos, por meio de um conjunto de procedimentos preestabelecidos pelo órgão ou entidade.

8.1.3. Para a contratação não será admitida a aferição de indicadores de níveis de serviço baseada exclusivamente em dados fornecidos pela própria contratada.

8.1.4. Os indicadores de níveis adotados neste Instrumento foram propostos com base na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, considerando apenas aqueles relacionados diretamente às necessidades de negócio, os benefícios esperados, os riscos associados ao processo e a criticidade dos serviços.

8.1.5. A contratada poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador, conforme item 3.2 do Anexo VIII-A da

8.2. O suporte técnico relacionado à contratação deverá estar disponível em caso de qualquer falha da solução, se requerido pelo CONTRATANTE, garantindo um atendimento conforme os índices de severidade definidos no **item 3.9.12.d**.

8.3. Além disso, devem ser considerados para a presente contratação o seguinte indicador:

Tabela - Indicador de atraso na Entrega - IAE

IAF – INDICADOR DE ATRASO NO FORNECIMENTO DA SOLUÇÃO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos ou serviços constantes na Ordem de Serviço (OS).	
Meta a cumprir	IAE <= 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento (OFB) dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.	
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	IAE = TEX – TEST Onde: IAE – Indicador de Atraso de Entrega da OFB; TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB. A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB. A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.	
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.	
Início de Vigência	A partir da emissão da Ordem de Fornecimento de Bens.	
Faixas de ajuste no pagamento e Sanções	IAE <= 0: Pagamento integral da OS; IAE >= 1 e < 30: Aplicar-se-á glosa de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso; IAE >= 30: Aplicar-se-á glosa de 10% sobre o valor da OS ou fração em atraso acrescido de 0,5% por dia de atraso sobre o valor da OS ou fração em atraso limitado em 30% sobre o valor da OS, bem como multa de 2% sobre o valor do contrato.	

Tabela - Indicador de Chamados Atendidos no Prazo – ICAP, referente ao ITEM 9.

ICAP – INDICADOR DE CHAMADOS ATENDIDOS NO PRAZO	
TÓPICO	DESCRIÇÃO
Finalidade	Aferir a quantidade de chamados atendidos para todos os produtos/serviços contratados dentro do prazo estabelecido na Tabela do item 3.9.12.d, do ITEM 9.
Meta a cumprir	≥ 80% de chamados atendidos dentro do prazo. A meta definida visa garantir que os chamados sejam atendidos dentro do prazo.
Instrumento de medição	Por meio de relatório de chamados abertos pela CONTRATANTE, extraído pela CONTRATADA, podendo ser utilizado Excel ou ferramenta específica, contendo, pelo menos, os seguintes campos: Protocolo, Nível de Severidade (Tabela do item 3.9.12.d), Data de Abertura, Data de Fechamento, Hora de Fechamento, Tempo total de atendimento, Técnico responsável, Descrição do chamado, Motivo do fechamento e outros itens pertinentes.
Forma de acompanhamento	O fiscal técnico deve atestar o relatório e, se necessário, indicar a glosa da fatura.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	Índice de chamados atendidos. Fórmula: Nível de Serviço = (Total de chamados atendidos dentro do prazo pela empresa CONTRATADA / Total de chamados abertos pelo CONTRATANTE no ambiente de abertura de chamados da empresa contratada) x 100.
Observações	Serão utilizadas duas casas decimais, truncando as demais. Será calculado um único indicador para os chamados, independentemente do tipo do produto/serviço.
Início de Vigência	A partir da emissão do Termo de Recebimento Definitivo do produto/serviço contratado.
Faixas de ajuste no pagamento e Sanções	Para valores do Indicador de Chamados Atendidos no Prazo será aplicada a glosa, se necessário, no faturamento do mês para todos os produtos/serviços, exceto para o item 04 – Carteira de Identidade Profissional (Física): • Igual ou maior que 80,00%= 0% de glosa; • De 79,99% até 70,00%= Glosa de 5% do faturamento do mês; • De 69,99% até 50,00%= Glosa de 10% do faturamento do mês; • Abaixo de 50,00% = 30% de Glosa do faturamento do mês e abertura de processo de apuração e eventual aplicação de penalidade.

8.3.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

8.3.1.1. não produzir os resultados acordados,

8.3.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

- 8.3.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.
- 8.3.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

Recebimento do Objeto

- 8.4. Os serviços serão recebidos provisoriamente, no prazo de **5 (cinco) dias corridos**, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. ([Art. 140, I, a, da Lei nº 14.133](#) e [Arts. 22, X e 23, VII do Decreto nº 11.246, de 2022](#)).
- 8.4.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.
- 8.4.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. ([Art. 22, X, Decreto nº 11.246, de 2022](#)).
- 8.4.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. ([Art. 23, X, Decreto nº 11.246, de 2022](#)).
- 8.4.4. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.
- 8.5. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.
- 8.5.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
- 8.5.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. ([Art. 119 c/c art. 140 da Lei nº 14133, de 2021](#))
- 8.5.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.
- 8.5.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.
- 8.6. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.
- 8.7. Os serviços serão recebidos definitivamente no prazo de **10 (dez) dias corridos**, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:
- 8.7.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento ([art. 21, VIII, Decreto nº 11.246, de 2022](#)).
- 8.7.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;
- 8.7.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
- 8.7.4. Comunicar à empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
- 8.7.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
- 8.8. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do [art. 143 da Lei nº 14.133, de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
- 8.9. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
- 8.10. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

- 8.11. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:
- Verificação da Conformidade Técnica – Análise da aderência da solução entregue às especificações funcionais e tecnológicas estabelecidas no Termo de Referência, incluindo requisitos de desempenho, compatibilidade e segurança;
 - Testes Funcionais e Operacionais – Execução de testes para comprovar o correto funcionamento da solução conforme os requisitos estabelecidos, podendo incluir testes de usabilidade, desempenho e segurança, quando aplicáveis;
 - Inspeção por Amostragem ou Integral – Avaliação do fornecimento das licenças por meio de amostragem estatística ou inspeção total, conforme a complexidade e criticidade da solução;
 - Revisão de Documentação Técnica – Conferência da documentação fornecida, incluindo manuais, relatórios de testes, licenças de software e demais artefatos exigidos contratualmente;
 - Listas de Verificação e Roteiros de Testes – Aplicação de checklists e roteiros previamente definidos para subsidiar a ação dos fiscais do contrato na avaliação da entrega;
 - Registro e Tratamento de Não Conformidades – Formalização de eventuais não conformidades identificadas, com estabelecimento de prazos para correção e reavaliação antes do recebimento definitivo.

Liquidação

- 8.12. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de **10 (dez) dias úteis** para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do [art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022](#).
- 8.10.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#).
- 8.13. Para fins de liquidação, a fiscalização e o setor competente deverão verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:
- o prazo de validade;
 - a data da emissão;
 - os dados do contrato e do órgão Contratante;
 - o período respectivo de execução do contrato;

8.13.5. o valor a pagar; e

8.13.6. eventual destaque do valor de retenções tributárias cabíveis.

8.14. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

8.15. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei nº 14.133, de 2021](#).

8.16. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.17. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

8.18. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.19. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

8.20. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

8.21. **O pagamento será efetuado em parcela única, exceto para o item 9, que será mensal, no prazo de até 10 (dez) dias úteis** contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da [Instrução Normativa SEGES/ME nº 77, de 2022](#).

8.22. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante a seguinte fórmula de atualização:

$$EM = I \times N \times VP$$

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga; e

I = Índice de atualização financeira = 0,0001644, assim apurado:

$$I = (TX/100)$$

$$365$$

$$I = (6/100)$$

$$365$$

$$I = 0,0001644$$

$$TX = \text{Percentual da taxa anual} = 6\%$$

Forma de pagamento

8.23. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.23.1. O pagamento será realizado em **parcela única** após o recebimento definitivo do objeto, **exceto para o item 9, cuja previsão de pagamento será mensal**.

8.24. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

Retenções tributárias

8.25. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável e indicadas a seguir de acordo com as orientações da Coordenadoria de Contabilidade e Finanças:

I. Na ocasião do pagamento, serão efetuadas as seguintes retenções:

I.1. *Tributos federais (IR, CSLL, PIS e COFINS) previstos no artigo 64 da Lei nº 9.430, de 27.12.96, e Instrução Normativa RFB nº 1.234, de 11.01.12, enquadrando o serviço no código 6190 (Demais serviços) da Tabela de Retenção do Anexo I da referida Instrução Normativa, exceto quando se tratar de empresa optante pelo simples nacional, hipótese em que deverá ser apresentada, no ato da assinatura do contrato, a declaração prevista no Anexo IV da mesma Instrução Normativa; e*

I.2. *Imposto Sobre Serviços (ISS) previsto na [Lei Complementar nº 116](#), de 31.07.03, enquadrando os serviços nos itens 1.05 (atualização e subscrição de licenças), 1.07 (instalação e suporte técnico) 8.02 (treinamento) da Lista de Serviços anexa à referida Lei. Para efeito do disposto neste tópico será observado o contido nos artigos 3º e 4º da Lei Complementar nº 116/03 (local do estabelecimento prestador). Em se tratando de empresa optante pelo simples nacional, a retenção se dará conforme enquadramento no respectivo Anexo da Lei Complementar nº 123/2006.*

II. *Para efeito do disposto no tópico I, a empresa deverá destacar no documento fiscal as alíquotas dos tributos e os correspondentes valores, nos termos das respectivas legislações. Em caso de descumprimento desta determinação, a empresa sofrerá a retenção pelas alíquotas máximas previstas.*

III. *Na hipótese de ocorrer alteração em alguma das normas referenciadas no tópico I, será aplicada a retenção correspondente prevista na legislação em vigor.*

8.26. O Contratado regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.26.1. Para os fins de comprovação de que trata o item anterior, deverá ser apresentada a declaração de que trata o art. 6º da Instrução Normativa nº 1234/2012, em meio físico ou eletrônico assinado por certificação digital (não será aceito simples cópia digitalizada).

Antecipação de pagamento

8.27. A presente contratação não permite a antecipação de pagamento.

9. DO REAJUSTE

- 9.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em **08/09/2025**.
- 9.2. **Quando aplicável**, após o interregno de um ano, e independentemente de pedido do CONTRATADO, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
- 9.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 9.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.
- 9.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
- 9.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 9.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 9.8. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

- 10.1. 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.

Apresentação da proposta

- 10.1.1. Somente serão classificadas as propostas cujos produtos/serviços atendam às especificações mínimas descritas neste Termo de Referência.
- I. A proposta deverá discriminar cada serviço ou produto que compõe o respectivo lote, separadamente, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 26 da Lei nº 14.133, de 2021.
- II. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento de todos os requisitos deste termo de referência. Para tal, deverá ser indicado na proposta comercial abrangendo, no mínimo, os seguintes elementos, de forma a deixar claro o atendimento de acordo com o exigido no edital: a) nome específico, nome oficial e/ou descrição; b) categoria ou linha do software, serviço ou produto; c) código de identificação unívoca do fabricante (part number, SKU etc.); d) modelo de licenciamento; e) métrica ou unidade; f) tipo de software, serviço ou produto; e g) quantidade.
- III. A omissão dessas informações acarretará na desclassificação da proposta. A solução ofertada deve estar em linha de produção, na data de entrega da proposta.
- IV. Os Part Numbers/nome dos produtos podem sofrer modificações de acordo com as últimas atualizações do fabricante, por isso, aqueles informados neste TR são apenas uma referência. Serão aceitos outros part-numbers, já que a aceitação de Part Numbers alternativos não configura mudança de objeto, desde que atendam aos requisitos, especificações e quantitativos definidos neste termo de referência.
- V. Nos preços propostos deverão estar incluídos todas as despesas e custos para seu fornecimento, como transportes, tributos, encargos trabalhistas, previdenciários, fiscais, seguros e quais quer outros que incidam direta ou indiretamente.
- VI. A LICITANTE deverá indicar em sua proposta os fabricantes, modelos e versões de todos os componentes das soluções, incluindo componentes do software, realizando a indicação de todos os Códigos de Produto. Devem ser entregues prospectos/folders/folhetos com as características técnicas dos softwares e licenças. Devem ser apresentadas, de forma clara e detalhada, as descrições das soluções com todos os seus componentes, podendo ser complementadas por documentações integrantes da proposta, tais como: brochuras, catálogos, manuais técnicos, manuais de operação, etc. Na especificação técnica devem ser destacados e referenciados pelo licitante os requisitos mínimos exigidos no Termo de Referência, com a indicação do documento e página onde se encontra grifada a comprovação, sob pena de desclassificação.
- VII. A proposta deverá possuir validade mínima de 60 (sessenta) dias.

Regime de execução

- 10.2. O regime de execução do contrato será por empreitado por preço global, uma vez que se tem certeza da qualidade e especificação do objeto a ser adquirido e também certeza, previamente, dos quantitativos a serem adquiridos para a execução contratual.

Margem de Preferência

- 10.3. Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

- 10.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

- 10.5. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;
- 10.6. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
- 10.7. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pi-br/empreendedor>;
- 10.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;
- 10.9. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução [Normativa DREI/ME n.º 77, de 18 de março de 2020](#).
- 10.10. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;
- 10.11. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz
- 10.12. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o [art. 107 da Lei nº 5.764, de 16 de dezembro 1971](#).
- 10.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

- 10.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
- 10.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
- 10.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 10.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do [Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943](#);
- 10.18. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 10.19. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 10.20. Caso o fornecedor seja considerado isento dos tributos Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
- 10.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na [Lei Complementar n. 123, de 2006](#), estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

- 10.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - [Lei nº 14.133, de 2021, art. 69, caput, inciso II](#));
- 10.23. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando:
- 10.23.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:
- $$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$
- $$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$
- $$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$
- 10.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo de até 10% do valor total estimado da contratação.
- 10.25. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;
- 10.26. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;
- 10.23.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.
- 10.25. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. ([Lei nº 14.133, de 2021, art. 65, §1º](#)).
- 10.26. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.
- 10.23.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

Qualificação Técnica

- 10.27. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.
- 10.27.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:
- 10.27.1.1. que demonstre(m) a execução de forma satisfatória dos serviços de fornecimento de licenciamento(s) de PLATAFORMA DE GERENCIAMENTO DE EXPOSIÇÃO CIBERNÉTICA, incluindo SERVIÇO DE IMPLANTAÇÃO E GARANTIA DOS EQUIPAMENTOS E/OU SOFTWARES, com experiência no mínima de **36 (trinta e seis) meses** e com o quantitativo mínimo de **1.200 (mil e duzentas) renovações de licenças, para o grupo 1, e de 14.046 (quatorze mil e quarenta e seis) licenças, para o grupo 2**;
- 10.27.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 10.27.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.
- 10.27.4. Os atestados deverão conter as seguintes informações mínimas: a data da emissão, a identificação clara do contratante e da contratada, nome e cargo da pessoa que os assina, datas de início e conclusão do serviço, declaração expressa da prestação satisfatória do serviço.
- 10.27.5. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 10.27.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 10.27.7. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.
- 10.27.8. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.
- 10.27.9. A apresentação de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitido, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.
- 10.27.10. **O fornecedor deverá apresentar Declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na disposto no item 1.7 do Anexo I da Instrução Normativa SGD/ME nº 94/2022 e no art. 5º da Lei nº 14.133, de 2021.**

Disposições gerais sobre habilitação

- 10.28. Quando permitida a participação na licitação/contratação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.
- 10.29. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto

nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.30. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.31. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.32. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de **R\$ 74.336.590,54** (setenta e quatro milhões trezentos e trinta e seis mil quinhentos e noventa reais e cinquenta e quatro centavos), conforme custos unitários apostos na tabela a seguir:

	ITE M	DESCRIÇÃO	CATSER	PART NUMBER	UNIDA DE	QTD E	VALOR UNITÁRI O	TOTAL
GRUP 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	TIO-WAS	LICENÇ A	39	R\$ 2.092,07	81.590,73
	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	TSCCV-M	LICENÇ A	2400	R\$ 1.942,72	4.662.528,0 0
	3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	N/A	TURMA	4	R\$ 25.792,11	103.168,44
TOTAL GERAL (GRUPO 1)								R\$ 4.847.287,1 7

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

	ITE M	DESCRIÇÃO	CATSER	PART NUMBER	UNIDA DE	QTD E	VALOR UNITÁRIO	TOTAL
GRUP O 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)	T-ONE	LICENÇ A	30	R\$ 1.648,90	49.467,00
	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)	T-ONE	LICENÇ A	11.90 0	R\$ 1.650,10	19.636.190,00
	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)	T-ONE	LICENÇ A	21.99 5	R\$ 1.722,24	37.880.668,80
	7	Serviço de Instalação, configuração e migração do ambiente atual.	26972 - Serviços de instalação, transição e configuração / parametrização de software	N/A	SERVIÇ O	21	R\$ 33.793,09	709.654,89
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	N/A	TURMA	22	R\$ 31.202,80	686.461,60
	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)	N/A	SERVIÇ O	19	R\$ 554.045,32	10.526.861,08
TOTAL GERAL (GRUPO 2)								R\$ 69.489.303,37

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

11.2. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

11.2.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

11.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

11.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

11.2.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento ordinário e/ou pleitos da Justiça Eleitoral.

12.1.1. A contratação será atendida pela seguinte dotação:

- I) Gestão/Unidade: UGR 070.272 - STI;
- II) Fonte de Recursos: 21EE - Gestão da Política de Segurança da Informação;
- III) Programa de Trabalho: AQUISICAO E DESENV. SOFTWARE - SEG. INFORM.;
- IV) Elemento de Despesa: 4.4.90.40/3.3.90.40;
- V) Plano Interno: SIN SFTWR.

12.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

13. DO DESCUMPRIMENTO CONTRATUAL E PENALIDADES

13.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

13.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

I. advertência, exclusivamente pela infração prevista no subitem 13.1, alínea “a”, quando não se justificar a imposição de penalidade mais grave;

II. impedimento de licitar e contratar no âmbito da Administração Pública Federal direta e indireta, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave, pelas infrações previstas nas alíneas “b”, “c” e “d” do subitem 13.1;

III. declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, pelas infrações previstas nas alíneas “e”, “f”, “g” e “h” do subitem 13.1, bem como nas alíneas “b”, “c” e “d” do referido subitem, quando as respectivas infrações justificarem a imposição de penalidade mais grave que a sanção referida na alínea anterior.

IV. Multa:

- 1. moratória de **0,5%** (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida (valor do item), até o limite de 10% (dez por cento) do valor global do contrato;
- 2. moratória de **0,07%** (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
- 3. moratória de **1%** (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o máximo de 10% (dez por cento) do valor global do item, pela inobservância do prazo fixado para substituição do bem rejeitado (item 8.2) ou em garantia (item 5.6.1.1).
- 4. compensatória de até 30% (trinta por cento) sobre o valor total do contrato, no caso de inexecução total ou parcial do objeto que resulte na extinção do contrato.
- 5. multa em decorrência de outras infrações abaixo descritas, considerando os graus, percentuais e formas de incidência descritos nas tabelas 1 e 2 abaixo, até o limite de 10% do valor do contrato:

Tabela 1

GRAU	PERCENTUAL CORRESPONDENTE
1	0,5% do valor do contrato
2	0,7% do valor do contrato
3	1% do valor do item/OS
4	2% do valor do contrato

Tabela 2

Item	Hipóteses	Grau	Incidência
01	suspender ou interromper, salvo motivo justificado por força maior ou caso fortuito, os serviços contratados.	3	por dia
02	permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequência letais.	4	por ocorrência sobre o valor do contrato
04	manter empregado sem qualificação para executar os serviços contratados.	3	por ocorrência
05	deixar de atender aos requisitos de sustentabilidade, segurança da informação e de segurança e privacidade.	1	por ocorrência
06	deixar de atender os prazos definidos no item 6.2 deste TR.	1	por ocorrência
06	deixar de cumprir determinação formal, instrução complementar do fiscalizador ou demais obrigações previstas neste Termo e não elencadas neste item 13.	1	por ocorrência
07	Reincidir no descumprimento da mesma obrigação anteriormente punida com multa de grau 1.	2	por ocorrência

- 13.3. Para os subitens 1, 2 e 3 do item IV acima, o atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
- 13.4. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante ([art. 156, §9º, da Lei nº 14.133, de 2021](#)).
- 13.5. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa ([art. 156, §7º, da Lei nº 14.133, de 2021](#)).
- 13.5.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação ([art. 157, da Lei nº 14.133, de 2021](#)).
- 13.5.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente ([art. 156, §8º, da Lei nº 14.133, de 2021](#)).
- 13.5.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.
- 13.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do [art. 158 da Lei nº 14.133, de 2021](#), para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.
- 13.7. Na aplicação das sanções serão considerados ([art. 156, §1º, da Lei nº 14.133, de 2021](#)):
1. a natureza e a gravidade da infração cometida;
 2. as peculiaridades do caso concreto;
 3. as circunstâncias agravantes ou atenuantes;
 4. os danos que dela provierem para o Contratante;
 5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 13.8. Os atos previstos como infrações administrativas na [Lei nº 14.133, de 2021](#), ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na [Lei nº 12.846, de 2013](#), serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei ([art. 159](#)).
- 13.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia ([art. 160, da Lei nº 14.133, de 2021](#)).
- 13.10. A sanção de **declaração de inidoneidade** é de competência do Presidente do TRE-PA.
- 13.11. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. ([Art. 161, da Lei nº 14.133, de 2021](#)).
- 13.12. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do [art. 163 da Lei nº 14.133/21](#).
- 13.13. Da aplicação das sanções de advertência, multa e impedimento licitar e contratar caberá recurso no prazo de 15 (quinze) dias úteis, contado da data da intimação.
- 13.13.1. O recurso de que trata o subitem acima será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.
- 13.14. Da aplicação da sanção de declaração de inidoneidade caberá apenas pedido de reconsideração, que deverá ser apresentado no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.
- 13.15. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

14.1. 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.

15. RELAÇÃO DE APÊNDICES E ANEXOS

- ⇨ Apêndice I - Estudos Técnicos Preliminares (ETP);
- ⇨ Anexo I - Termo de Compromisso e Manutenção de Sigilo;
- ⇨ Anexo II - Termo de ciência;
- ⇨ Anexo III - Modelo de Ordem de Serviço.
- ⇨ Anexo IV - Minuta de Termo de Recebimento Provisório;
- ⇨ Anexo V - Minuta de Termo de Recebimento Definitivo.
- ⇨ Anexo VI - Modelo de Declaração de não ocorrência do registro de oportunidade.
- ⇨ Anexo VII - Formulário de avaliação - Treinamento da solução

ANEXO I - I
TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A Sociedade Empresária _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____, CPF _____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) relacionadas à **“contratação de solução de gerenciamento de exposição cibernética, composta por disponibilização e renovação de licenças, implantação, repasse técnico, treinamento, garantia e manutenção dos equipamento e/ou softwares por 60 meses”**, contratada pelo Tribunal Regional Eleitoral do Pará, CNPJ nº 05.703.755/0001-76, doravante designado TRE-PA, em conformidade com as seguintes cláusulas e condições:

- 1) Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico do TRE-PA, comprometendo-se a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pelo TRE-PA ou quaisquer de seus representantes;
- 2) As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
- 3) As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
- 4) A CONTRATADA obriga-se a informar imediatamente o TRE-PA qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço;
- 5) A CONTRATADA deverá prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato;
- 6) A não observância de quaisquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao TRE-PA e aos seus usuários;
- 7) O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato do TRE-PA: _____

Representante da Contratada: _____

Local, UF, de de

ANEXO I - II TERMO DE CIÊNCIA

IDENTIFICAÇÃO DO CONTRATO

CONTRATO Nº:

OBJETO: **“Registro de preços para eventual e futura contratação de solução de gerenciamento de exposição cibernética, composta por disponibilização e renovação de licenças, implantação, repasse técnico, treinamento, garantia e manutenção dos equipamento e/ou softwares por 60 meses, conforme condições, quantidades e exigências estabelecidas neste Instrumento e seus anexos.”**

Contratada:

CNPJ:

Representante da Contratada:

CPF:

Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) declara(m):

- Ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA;
- Ter conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deverá ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo;
- Comprometer-se a guardar sigilo necessário sobre todas as informações que eventualmente venha(m) a tomar conhecimento;
- Comprometer-se a prestar obediência às políticas de segurança da informação vigentes no Tribunal Regional Eleitoral do Pará ou que poderão ser instituídas durante a vigência do contrato.

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Nome: CPF: _____

Função/Cargo: _____

Assinatura: _____

Local, UF, de de .

ANEXO I - III ORDEM DE SERVIÇO

IDENTIFICAÇÃO DO CONTRATO

A Sua Senhoria a(o) Senhora(or).

NOME REPRESENTANTE

SOCIEDADE EMPRESÁRIA:	
CNPJ/MF:	
REPRESENTANTE:	
ENDEREÇO:	
TELEFONE:	
E-MAIL	

Na qualidade de fiscal do contrato XX/2025 TRE-PA, conforme previsto na Cláusula XY do referido instrumento contratual, encaminho este documento para solicitar o fornec no quadro a seguir:

GRUPO 1	ITEM	DESCRIÇÃO	CATSER	UNIDAI
	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	
	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	
	3	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	

TOTAL GERAL (GRUPO 1)

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

GRUPO 2	ITEM	DESCRIÇÃO	CATSER	UNIDA
	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	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)	
	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)	
	7	Serviço de Instalação, configuração e migração do ambiente atual.	26972 - Serviços de instalação, transição e configuração / parametrização de software	
	8	Treinamento da solução contratada para até 10 pessoas, com no mínimo 20 horas de duração (EAD).	3840 - Treinamento Informática - Sistema / Software	
	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)	

TOTAL GERAL (GRUPO 2)

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

II - LOCAL DE EXECUÇÃO/ENTREGA:

ANEXO I - IV
MINUTA TERMO DE RECEBIMENTO PROVISÓRIO

A Sua Senhoria a(o) Senhora(or). [NOME REPRESENTANTE]
Representante Legal da Sociedade Empresária [NOME DA CONTRATADA]

Na qualidade de fiscal do CONTRATO N° XX/2025 TRE-PA, por este instrumento, recebo, provisoriamente, em XX/XX/2025, conforme previsto na CLÁUSULA XXXXX, conformidade com a especificação do Termo de Referência do edital XX/2025, entregue por meio do Anexo/Comprovante XXXXX no dia XX/XX/2025.

NOTA DE EMPENHO:
SOCIEDADE EMPRESÁRIA: CNPJ/MF:
OBJETO:

Tabela - Itens que compõe o objeto

Por fim, segue este documento para solicitar o encaminhamento da Nota Fiscal do referido objeto.

ANEXO I - V MINUTA TERMO DE RECEBIMENTO DEFINITIVO	
Nº PROC. SEI DE CONTRATAÇÃO	
CONTRATO	
VIGÊNCIA	
VALOR	
SOCIEDADE EMPRESÁRIA	
FISCAL	
Objeto:	Tabela - Itens que compõe o objeto

Eu, [NOME DO FISCAL], [Técnico Judiciário / Analista Judiciário], declaro que os produtos/serviços objeto do CONTRATO nº XXX/2025, foram fornecidos consoante p motivo pelo qual os recebo de forma definitiva.

ANEXO I - VI DECLARAÇÃO DE NÃO OCORRÊNCIA DO REGISTRO DE OPORTUNIDADE
Edital nº _____ - TRE/PA
OBJETO: “Registro de preços para eventual e futura contratação de solução de gerenciamento de exposição cibernética, composta por disponibilização e renovação de licenças, implantação, repasse técnico, treinamento, garantia e manutenção dos equipamento e/ou softwares por 60 meses, conforme condições, quantidades e exigências estabelecidas neste Instrumento e seus anexos.”
Licitante:
CNPJ:
Pelo presente instrumento, o licitante, por meio de seu representante legal, DECLARA, que para a apresentação de proposta ao referido Edital, NÃO houve ocorrência de “Registro de Oportunidade”, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto no item 1.7 do Anexo I da Instrução Normativa SGD/ME nº 94/2022 e no art. 5º da Lei nº 14.133, de 2021.
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)
Nome: CPF: _____
Função/Cargo: _____
Assinatura: _____
Local, UF, de de .

ANEXO I - VII AO TERMO DE REFERÊNCIA FORMULÁRIO DE AVALIAÇÃO - TREINAMENTO DA SOLUÇÃO
--

AVALIAÇÃO DE REAÇÃO

TREINAMENTO	
PROMOTOR	
PERÍODO	
CARGA HORÁRIA	
INSTRUTOR	
OBJETIVO	

Para que possamos avaliar a qualidade do treinamento, assinala com um (X) na nota que melhor expressa sua opinião de acordo com a escala abaixo:

Grau de satisfação	Não atendeu	Atendeu parcialmente	Atendeu plenamente	Superou
Nota	1	2	3	4

I- PROMOTOR DO EVENTO				
ITEM	NOTA			
1- Quanto à organização do evento				
2- Quanto à adequação das instalações				
3- Quanto à adequação dos recursos audiovisuais				
4- Quanto à qualidade do material didático				
II- CONTEÚDO PROGRAMÁTICO				
ITEM	NOTA			
1- Quanto ao cumprimento do conteúdo programático				
2- Quanto ao detalhamento na abordagem dos tópicos				
3- Quanto à adequação da carga horária				
4- Quanto a adequação do conteúdo a sua necessidade de conhecimento				
III- INSTRUTOR				
ITEM	NOTA			
1- Quanto ao domínio do assunto				
2- Quanto à relevância e atualidade dos conhecimentos difundidos				
3- Quanto à promoção de um ambiente favorável à aprendizagem				
4- Quanto à clareza e objetividade nas exposições				
5- Quanto à objetividade na administração do tempo				
6 – Quanto ao incentivo à participação da turma				
7 – Quanto à disponibilidade para o atendimento e o apoio aos alunos				
IV- APROVEITAMENTO				
ITEM	NOTA			
1- Quanto à assimilação do conteúdo				
2- Quanto à adequação do conteúdo ao objetivo proposto por sua unidade de lotação				
V- COMENTÁRIOS E SUGESTÕES:				

*Tabela - Modelo de formulário - SGP/CODES/Seção de Treinamento e Desenvolvimento



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 **2856633** e o código CRC **F1AA21F6**.