TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS TÉCNICOS PRELIMINARES

1. Necessidade/Demanda a ser Atendida

1.1. Indicação da necessidade, sob a perspectiva do interesse público:

1.1.1. Identificar e tratar as possíveis vulnerabilidades existentes no ambiente de tecnologia da informação do TSE.

1.2. Descrição da necessidade:

1.2.1. Descrição e análise do cenário atual:

1.2.1.1. Com a necessidade de disponibilizar cada vez mais serviços on-line, as organizações, sejam públicas ou privadas, e de por Comunicação - TIC como meio para atingirem seus objetivos. Dessa forma, ocorre um aumento da conectividade dos computado maior quantidade de vulnerabilidades existentes em seu ambiente de TI, contribuindo, em última análise, para o crescimento dos in

1.2.1.2. Segundo a referência do *Gartner* sobre Gerenciamento de Exposição Cibernética (*Exposure Management*), "Até 2026, as nov com base em um programa contínuo de gerenciamento de exposição, terão três vezes menos probabilidade de sofrer uma violaçã *Program, Gartner,* julho de 2022) (https://www.gartner.com/doc/reprints?id=1-2APCAC3H&ct=220729&st=sb)

1.2.1.2.1. O Gerenciamento de Exposição Cibernética é o processo de avaliar e gerenciar riscos e vulnerabilidades (Gestão de V

1.2.1.2.2. Através do Gerenciamento de Exposição o TSE tem uma visão completa de toda a superfície de ataque (vulneral priorização sugerida em termos de probabilidade e impacto da ocorrência de um incidente.

1.2.1.2.3. A análise e a pontuação baseadas em risco de "Ciber Exposição" ponderam as vulnerabilidades, os dados de ame riscos e do impacto positivo das correções sugeridas.

1.2.1.3. De acordo com o *Global Risks Repor*t de 2023, publicado pelo *World Economic Forum* [1] o risco de ciber crimes e insegurai em oitavo lugar tanto na estimativa dos riscos mais relevantes a curto prazo (2 years - 2 anos) quanto a médio prazo (10 years - 10 a

1.2.1.4. O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), por sua vez, provê gráficos anuais podemos observar que de janeiro a junho de 2023, já ocorreram 69% de incidentes em comparação com todos os 12 meses do ano de 202

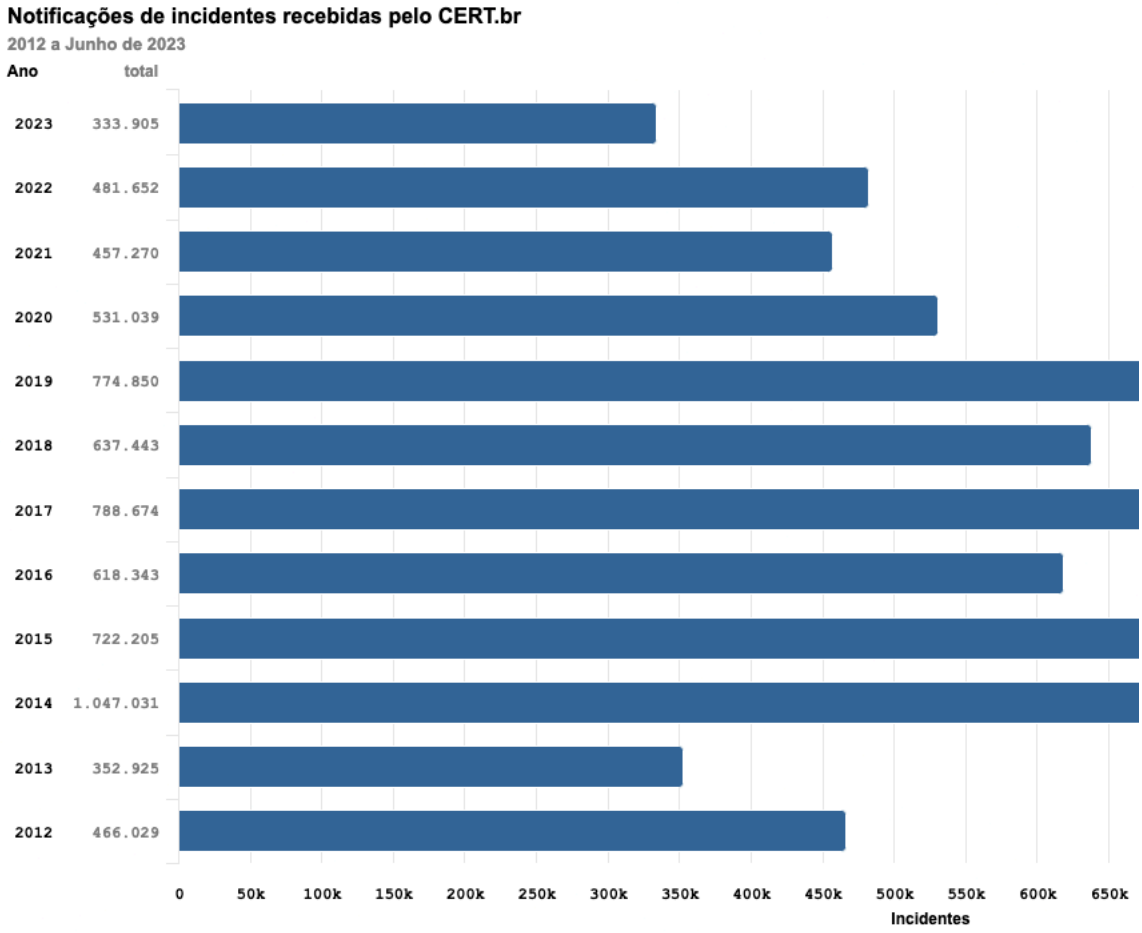


Imagem 01 - Notificações de Incidentes recebidos pelo CERT.BR (Fonte: CERT.BR disponível em https://stats.cert.br/incidentes/ acesso e

1.2.1.5. Grande parte dos incidentes reportados acima poderia ter sido evitada, ou, ao menos, os impactos nas organizações env vulnerabilidades.

1.2.1.6. Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco uma ação interna de segurança da informação (NC 04/IN01/DSIC/GSI/PR).

1.2.1.7. Vulnerabilidade é definida, segundo o CERT.BR, como uma condição que, quando explorada por um atacante, pode resultar e

1.2.1.8. As vulnerabilidades são originadas de falhas, na maioria da vezes não intencionais, e podem ser classificadas como:

1.2.1.8.1. Físicas: Acesso a ativos por pessoas não autorizadas, devido à falta de controle de acesso;

1.2.1.8.2. Hardware: Falhas no hardware, não atualização de firmware, podem provocar indisponibilidades no sistema e perda d

1.2.1.8.3. Naturais: Desastres naturais podem comprometer a segurança dos dados armazenados;

1.2.1.8.4. Humanas: São falhas associadas ao operador de sistema que, de forma intencional ou não, na execução de sua função eventualmente possibilita o sequestro de dados, instalação e ativação de malwares

1.2.1.8.5. Software: falhas na implementação dos requisitos de segurança ou na codificação dos sistemas operacionais, software "brechas" com potenciais pontos de exploração de vulnerabilidades no ambiente interno;

1.2.1.9. Os atacantes se utilizam, como uma das primeiras etapas do planejamento e realização de um ataque, de técnicas de varredura identificar vulnerabilidades ali existentes. Esse processo da varredura é tecnicamente conhecido como "Scan". As estatísticas de incident que os incidentes por "*Scan*" correspondem a 68,67% do total de todas as modalidades mais comuns de incidentes.

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Junho de

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%
jan	59.030	11.827	20,04	2.843	4,82	63	0,11	41.691	70,63	605
fev	47.990	7.503	15,63	2.510	5,23	82	0,17	37.037	77,18	643
mar	53.792	8.258	15,35	2.987	5,55	105	0,20	40.289	74,90	1.230
abr	41.809	6.404	15,32	2.669	6,38	165	0,39	30.195	72,22	1.027
mai	69.974	2.369	3,39	3.631	5,19	143	0,20	44.519	63,62	363
jun	61.310	3.460	5,64	2.814	4,59	100	0,16	35.576	58,03	295
Total	333.905	39.821	11,93	17.454	5,23	658	0,20	229.307	68,67	4.163

Imagem 02 - Notificações de Incidentes recebidos pelo CERT.BR (Fonte: CERT.BR disponível em https://stats.cert.br/incidentes/ acesso e

1.2.1.10. Isso significa que, para a construção de um sistema de defesa cibernética eficaz, o TSE necessita conhecer as vulnerabilic complementado por informações que indiquem como tratar tais vulnerabilidades, de forma que possamos tratá-las antes que sejan de uma solução de Gestão de Vulnerabilidades.

1.2.2. O objetivo a ser alcançado:

1.2.2.1. Manter operacional a ferramenta de Gestão de Vulnerabilidades utilizada pelo TSE, de forma a contribuir para a minimização c afetem o tribunal. Complementação das funcionalidades já existentes na solução adquirida e em utilização pelo tribunal, de forma a também viabiliz implementado no tribunal em passado relativamente recente. Dotar a equipe de cibersegurança do TSE de funcionalidades que facilitem a tarefa de co mais facilmente compreendida sob o ponto de vista negocial.

1.2.3. Público alvo a ser atendido:

1.2.3.1. Equipes de segurança cibernética e de administração do ambiente de TI do TSE de forma geral.

1.2.3.2. De forma indireta, Usuários internos e externos da Justiça Eleitoral que utilizam equipamentos e sistemas de T incidentes cibernéticos que afetem a utilização desses equipamentos e sistemas.

1.2.4. Impactos sobre as atividades do TSE e/ou sobre o público alvo a ser atendido, caso a necessidade apontada não seja sanada:

1.2.4.1. Uma vez que o TSE não tenha conhecimento de novas vulnerabilidades que poderão compromete **cibernética** derivados de vulnerabilidades existentes no ambiente computacional do TSE não poderão ser tratadas assim o ambiente e incrementando a probabilidade da ocorrência de incidentes cibernéticos.

1.2.4.2. Dependendo do tipo de vulnerabilidade, poderá ocorrer indisponibilidade de sistemas, bloqueio e usurpação comprometer inclusive a realização de eleições.

1.2.5. Objetivo(s) estratégico(s) do TSE com os quais necessidade está alinhada, assim como, caso convier, demonstrar a aderência com o

1.2.5.1. A contratação pretendida está alinhada ao Planejamento Estratégico do TSE conforme abaixo:

1.2.5.1.1. Planejamento Estratégico Institucional 2021-2026: Objetivo Estratégico "Aperfeiçoar a Segurança da Inf

1.2.6. Requisitos necessários à composição da necessidade e indispensáveis para a escolha da solução que melhor atenderá essa necessida

1.2.6.1. A solução deve ser capaz de identificar, no parque de tecnologia da informação do TSE, vulnerabilidades já catalogadas e di mundial, além de possuir funcionalidades que permitam a identificação de quais vulnerabilidades são mais críticas considerado o a relatórios que possam suportar decisões referentes à priorização do tratamento dessas vulnerabilidades.

2. Análise do Processo de Contratação e Execução Contratual Anterior no TSE:

2.1. Processo SEI, Contrato ou Nota de Empenho e Contratada:

2.1.1. Contrato TSE nº 128/2022 - Processo SEI nº 2022.00.000003508-0:

2.1.1.1. O processo licitatório foi conduzido pelo TSE, com objetivo de ampliar o licenciamento contratado anteriormente através d
6);

2.2. Fase Interna da Licitação (Exigências e sugestões exaradas pela Assessoria Jurídica (Pareceres Asjur) e Controle Interno/Secretari

2.2.1. De acordo com o Parecer da ASJUR, 2273740, a exigência de ampliação da cota para participação de ME/EPP, foi inviável uma vez que a

2.3. Fase Externa da Licitação (Questionamentos, Pedidos de impugnação, Diligências, Inabilitações, Recursos e etc):

2.3.1. Conforme a Ata do Pregão Eletrônico TSE nº 086/2022, SEI 2309381, não houve questionamentos, pedidos de impugnação, diligênc

2.4. Execução Contratual (Dificuldades e Problemas Identificados):

2.4.1. A execução do contrato vem ocorrendo de forma satisfatória.

2.4.2. As licenças foram fornecidas nas quantidades contratadas e em conformidade com as quantidades e prazos previstos em contrato.

2.5. Necessidade de Transição Contratual:

2.5.1. Não aplicável, uma vez que trata-se de contratação para renovação de licenciamento de produto já adquirido e instalado pelo tribu
anteriores, à exceção da prestação eventual de serviços de suporte.

3. Diferentes Soluções de Mercado que possam Atender à Necessidade

3.1. - 1ª Solução:

3.1.1. Substituição da solução de Gestão de Vulnerabilidades já adquirida por outra disponível no Portal do Software Público Brasileiro:
3.1.1.1. O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da admin
Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro (www.softwarepublico.gov.b
3.1.1.2. O principal objetivo do Portal é promover o desenvolvimento de uma ambiente colaborativo que não só reduz os custos
tecnológicos. O conceito de utilização livre de código fonte, é central para o Portal do Software Público Brasileiro.
3.1.1.3. Já são 81 softwares catalogados para compartilhamento. Não foi encontrada solução de gestão de
(https://softwarepublico.gov.br/social/search/software_infos).
3.1.2. Vantagens:
3.1.2.1. A iniciativa, se estivesse disponível, resultaria na economia de recursos públicos.
3.1.3. Desvantagens:
3.1.3.1.Necessidade de manter equipe exclusiva para manutenções preventivas, reativas e adaptativas (customizações);
3.1.3.2. Dificuldade de atualizações para detecção de novas vulnerabilidades.
3.1.4. Órgãos públicos e/ou entidades que adotaram solução similar:
3.1.4.1. Não foram encontradas.

3.2. - 2ª Solução:

3.2.1. Desenvolvimento interno de uma solução de Gerenciamento de Vulnerabilidades:
3.2.1.1. Para viabilizar essa solução seria necessário necessário que a STI/TSE desenvolvesse uma solução (hardware e software) qu
internacional confiável, realizasse rotinas de varreduras (scans) de vulnerabilidades sobre o ambiente de TI do tribunal, considera
aplicações, servidores de bancos de dados, estações de trabalho, etc.), capaz de gerar relatórios e análises de riscos e impactos dess
3.2.1.2. Este tipo de desenvolvimento demandaria da equipe de TI do TSE uma expertise que esta não possui, além de representar o
módulos, o que demandaria tempo considerável para sua execução;
3.2.1.3. Não foram encontrados órgãos/instituições que possuem software de gerenciamento de vulnerabilidades desenvolvidos pel
3.2.2. Vantagens:
3.2.2.1.Todo conhecimento seria interno ao TSE;
3.2.3. Desvantagens:
3.2.3.1.Necessidade de manter equipe exclusiva para manutenções preventivas, reativas e adaptativas;
3.2.3.2. Dificuldade de atualizações para detecção de novas vulnerabilidades;
3.2.3.3. Dificuldade de manter equipe qualificada e especialistas técnicos nas várias áreas da Tecnologia da Informação (colaborado
3.2.4. Órgãos públicos e/ou entidades que adotaram solução similar:
3.2.4.1. Não foram encontradas.

3.3. - 3ª Solução:

3.3.1. Renovar o licenciamento da solução de Gestão de Vulnerabilidades atualmente utilizada pelo TSE (*Tenable.sc+*) e adquirir m
vulnerabilidades em ambiente de *containers*, e façam a Gestão da Exposição cibernética do Tribunal, conforme módulos abaixo:

3.3.1.1. Renovação das licenças do produto *Tenable.sc* (o atual licenciamento dos direitos de atualização de versões e suporte pe
3.3.1.1.1. Rastreamento automatizado de ativos, vulnerabilidades e progresso de SLA com base em uma variedade de filtr
3.3.1.1.2. Gerenciamento de vulnerabilidades para visibilidade contínua dos ativos e vulnerabilidades do TSE.

3.3.1.2. *Cloud Security*:

3.3.1.2.1. Visibilidade e correção contínua de riscos em recursos e ativos em *cloud;*

3.3.1.2.2. Proteção específica para *Kubernetes, containers*, ambiente *serverless;*

3.3.1.2.3. Integração nativa com *AWS, Azure, GCP* e plataformas *cloud;*

3.3.1.3. *Lumin*:

3.3.1.3.1. Visualização dos riscos cibernéticos;

3.3.1.3.2. Apoio à decisão, fornecendo métodos para a análise e cálculo da eficácia das operações de segurança e faça uma

3.3.1.3.3. Acompanhamento da redução de riscos ao longo do tempo;

3.3.2 Quantidades de licenças que compõem a solução

3.3.2.1 Esses quantitativos observam a memória de cálculo registrada no item 3.6 deste documento.

3.3.3 Potenciais fornecedores e/ou fabricantes.

3.3.3.1 Trata-se de renovação de licenciamento de produto já utilizado no tribunal, o *Tenable.sc,* disponibilizada pelo fabricante
credenciada para comercializar seus produtos.

3.3.4 Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos:

3.3.4.1 Desconhecemos órgãos públicos ou entidades que tenham contratado diferentes módulos da solução de vulner

3.3.5.1 Entretanto, com relação à contratação exclusiva do módulo *Tenable.sc+*, há os seguintes casos: TRE-PB, e todos o
preços nº 101/2020 TRE-PB;

3.3.6.1 Os contratos derivados da ARP TRE-PB nº 101/2020 são idênticos ao contrato hoje vigente para o TSE, e, assim, não tra
às necessidades do Tribunal

3.3.5 Serviços e materiais complementares, não contemplados na solução, mas que devem ser objeto de contratação posteric

3.3.5.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a a

3.3.6 Requisitos de tecnologia da informação presentes na solução

3.3.6.1 Não há requisitos de tecnologia da informação adicionais aos já providos para a solução em utilização no TSE. T
virtualização e executada sobre sistema operacional usualmente utilizados no tribunal.

3.3.7 Custos estimados para fins de análise comparativa

3.3.7.1 O custo estimado, referente à contratação inicial, é de R$ 2.315.100,00, conforme quadro comparativo disponibilizad

3.3.7.1 Para o cálculo do custo inicial estimado, foram considerados os seguintes quantitativos:

3.3.7.1.1 Renovação das licenças do produto *Tenable.sc:* 2.500 licenças;

3.3.7.1.2 *Cloud security:* 300 licenças (quantidade de licenças estimada para iniciarmos o processo de gestão de vul

3.3.7.1.3 *Lumin:* 2.500 licenças (este produto deve ter licenciamento idêntico ao do produto de gerenciamento de vu

3.3.8 Custos indiretos relacionados ao ciclo de vida do objeto.

3.3.8.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a adi

3.3.9 Vantagens

3.3.9.1. A continuidade de utilização da ferramenta de Gestão de Vulnerabilidades já adquirida pelo TSE, aproveitando as
solução, bem como o conhecimento técnico já adquirido pela equipe técnica no tocante à sua operação;

3.3.9.2. Expansão das funcionalidades disponíveis no licenciamento atual, permitindo que o tribunal efetue a gestão de vu
atendidos.;

3.3.10. Desvantagens

3.3.10.1. Maior dificuldade na fiscalização e gestão contratual, pois seriam adquiridos três licenciamentos distintos, refere

3.3.10.2. Maior dificuldade na configuração da console de gerência da solução, pois os três licenciamentos teriam que ser

3.3.10.3. Nesse modelo, a console de gerência permaneceria sendo instalada e operada na infraestrutura do tribunal, dema
tarefas de manutenção e atualização das versões de software dessa console.

3.4. - 4ª Solução:

3.4.1. Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativos de rede (*T*
citados na 3ª Solução por meio de um pacote de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "*Tenable C*

3.4.2 Quantidades de licenças que compõem a solução

3.4.2.1 Esses quantitativos observam a memória de cálculo registrada no item 3.6 deste documento.

3.4.3 Potenciais fornecedores e/ou fabricantes.

3.4.3.1 Trata-se de renovação de licenciamento de produto já utilizado no tribunal, o *Tenable.sc*, disponibilizada pelo fabricante
credenciada para comercializar seus produtos.

3.3.4 Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos:

3.3.4.1 Tenable One Standard

3.3.4.1.1. Tribunal Regional do Trabalho da 8ª Região - TRT 8 - Pregão Eletrônico nº 004/2022 (SRP);
3.3.4.1.2. Procuradoria Geral do Estado da Bahia - PGE BA - Pregão Eletrônico nº 007/2022;
3.3.4.1.3. Empresa Mato-Grossense de Tecnologia da Informação - MTI/MT - Pregão Eletrônico nº 023/2022;
3.3.4.1.4. SANEAGO - Pregão nº 94/2021 - Lote 50 - Item 5.1.

3.3.4.2 Análise dos contratos

3.3.4.2.1 - Todos os contratos são referentes apenas a licenciamento de software (no caso, *Tenable One Standard*) e, event
simples, não foram identificadas metodologias, tecnologias ou inovações que possam atender às necessidades do Tribunal.

3.4.5 Serviços e materiais complementares, não contemplados na solução, mas que devem ser objeto de contratação posteric

3.4.5.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a ad

3.4.6 Requisitos de tecnologia da informação presentes na solução

3.4.6.1 Não há requisitos de tecnologia da informação adicionais aos já providos para a solução em utilização no TSE. T
virtualização e executada sobre sistema operacional usualmente utilizados no tribunal.

3.4.7 Custos estimados para fins de análise comparativa

3.4.7.1 O custo estimado é de R$ 2.235.000,00, conforme quadro comparativo disponibilizado na parte final deste tópico.

3.4.8 Custos indiretos relacionados ao ciclo de vida do objeto.

3.3.8.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a adi

3.4.9 Vantagens

3.4.1.1.1. Todos os módulos são licenciados sob um mesmo pacote de licenciamento, facilitando a gestão e fiscalização contratu
3.4.1.1.2. As quantidades de licenças passam a poder flutuar entre os módulos licenciados. Assim, caso, em um determinado mo
Cloud Security e menos licenças para o Tenable.sc+, essa flutuação pode ser feita sem a necessidade de modificação do licencia
3.4.1.1.3. Disponibiliza, sob o mesmo pacote de licenciamento, as funcionalidades adicionais abaixo detalhadas (em comparaçã
3.4.1.1.4. A console de gerenciamento passa a operar em provedor de nuvem do próprio fabricante, desonerando assim o tribuna
console de gerenciamento.

3.4.10. Desvantagens

3.4.1.2.1. Não vislumbramos nenhuma desvantagem dessa opção em comparação à 3ª solução.

- Observações
  - A utilização da console de gerenciamento da solução em ambiente de nuvem do fabricante poderia trazer riscos à seguran
    confidencialidade. Entretanto, esse risco é mitigado pelos controles de segurança implantados pelo fabricante, tais como a
    de acesso à console, o isolamento entre os ambientes de diferentes clientes, e <garantia técnica de não acesso das informa
    comprovado por informações contidas no documento "*Your Data Security and Privacy Requirements Define How We Ope*
    - Outras soluções de segurança adquiridas pelo tribunal já fazem uso do modelo de console instalada em prove
      (conhecida como EDR/XDR, adquirida pelo tribunal por meio do contrato TSE nº 11/2022 - Processo SEI nº
  - O licenciamento da solução de Gestão de Vulnerabilidades para o pacote "*Tenable One Standard"* representa uma mudanç
    (atualmente contratado pelo tribunal, e que é o modelo associado à 3ª Solução), para o modelo de subscrição. Tal mudanç
    esse tipo de solução, mesmo quando licenciada de modo perpétuo, é diretamente dependente dos direitos de atualização d
    de dados de vulnerabilidades conhecidas e suas respectivas formas de mitigação, direitos esses que não compõem as licen
    seja eficaz.
    - É importante observar que as estimativas de preços solicitadas já contemplaram a conversão das licenças perp
      subscrição do pacote "*Tenable One Standard*".

3.5. - 5ª Solução:

3.5.1. Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativos de rede (*T*
citados na 3ª Solução, e ainda dois módulos adicionais, responsáveis pelo Gerenciamento da Superfície de Ataque (*Attack Surface Ma*
ser explorados por eventuais atacantes *(Attack Path Analysis*), por meio de um pacote de Licenciamento integrado disponibilizado pel
3.5.1.1. Todos os módulos são licenciados sob um mesmo pacote de licenciamento
3.5.1.2. As quantidades de licenças passam a poder flutuar entre os módulos licenciados. Assim, caso, em um determinado mom
Cloud Security e menos licenças para o T*enable.sc+*, essa flutuação pode ser feita sem a necessidade de modificação do licencia
3.5.1.3. Disponibiliza, sob o mesmo pacote de licenciamento, as funcionalidades adicionais abaixo detalhadas (em comparação
3.5.1.3.1. A*ttack Surface Management* (Gerenciamento da Superfície de Ataque):
3.5.1.3.1.1. Descoberta contínua de ativos externos (ativos da organização que estejam expostos à Internet) e identif
3.5.1.3.1.2. Visão do ambiente sob a perspectiva de um invasor externo.
3.5.1.3.1.3. Eliminação de pontos cegos e construção de uma linha de base eficiente.

3.5.1.3.2. *Attack Path Analysis* (Análise de Caminhos de Ataque):

3.5.1.3.2.1. Mapeia e prioriza caminhos críticos que invasores podem explorar, tanto no ambiente interno da organi

3.5.1.3.2.2. Baseado no *framework MITRE ATT&CK* para visualizar a viabilidade de técnicas de ataque.

3.5.1.3.2.3. Foco preventivo em disrupção de exploração antes do ataque.

3.5.1.3.3. *Asset Inventory* (Inventário de Ativos):

3.5.1.3.3.1. Visibilidade completa de todos os ativos, independente da fonte (Máquinas Virtuais (VM), WEB, *Active*

3.5.1.3.3.2. Eliminação de pontos cegos e controle granular por *tags* (associação de etiquetas aos ativos).

3.5.1.3.3.3. Fonte confiável e única de informações sobre ativos.

3.5.2 Quantidades de licenças que compõem a solução

3.5.2.1 Esses quantitativos observam a memória de cálculo registrada no item 3.6 deste documento.

3.5.3 Potenciais fornecedores e/ou fabricantes.

3.5.3.1 Trata-se de renovação de licenciamento de produto já utilizado no tribunal, o *Tenable.sc+*, disponibilizada pelo fabricant
credenciada para comercializar seus produtos.

3.5.4 Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos:

3.5.4.1 Não encontramos órgãos públicos que já tenham realizado a contratação de licenciamento do pacote Tenable O

3.5.5 Serviços e materiais complementares, não contemplados na solução, mas que devem ser objeto de contratação posteri

3.4.5.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a ad

3.5.6 Requisitos de tecnologia da informação presentes na solução

3.4.6.1 Não há requisitos de tecnologia da informação adicionais aos já providos para a solução em utilização no TSE. T
virtualização e executada sobre sistema operacional usualmente utilizados no tribunal.

3.5.7 Custos estimados para fins de análise comparativa

3.5.7.1 O custo estimado é de R$ 2.652.500,00, conforme quadro comparativo disponibilizado na parte final deste tópico.

3.5.8 Custos indiretos relacionados ao ciclo de vida do objeto.

3.3.8.1 Não há. Trata-se da renovação de licenciamento de produto já utilizado pelo tribunal, mesmo considerando a adi

3.5.9. Vantagens:

3.5.9.1. Essa opção traz o maior conjunto de funcionalidades relativas ao Gerenciamento de Exposição Cibernética;

3.5.9.1.1. A funcionalidade de Gerenciamento da Superfície de Ataque permite conhecer, em tempo real, os ativos e servi atacantes externos;

3.5.9.1.2. A funcionalidade de Análise de Caminhos de Ataque permite uma melhor visibilidade sobre os caminhos de ata de segurança mais urgentes;

3.5.9.2. A utilização da console de gerenciamento hospedada na nuvem do fabricante elimina os esforços para a manutenção da novas versões;

3.5.9.3. Este modelo permite a flutuação (flexibilização/mobilidade) do licenciamento entre funcionalidades distintas, o que pod de eventuais novas funcionalidades vem a ser disponibilizadas pelo fabricante mediante, apenas, de licenciamento adicional (qu

3.5.10. Desvantagens:

3.5.10.1. Das 3 opções entendidas como viáveis (3ª, 4ª e 5ª solução), é a que apresenta maior custo;

3.5.10.2. As funcionalidades de "A*ttack Surface Management*" e "*Attack Path Analysis*" são ofertas recentes da solução, requere provêem.

- Observações:
  - A exemplo da 4ª solução, A utilização da console de gerenciamento da solução em ambiente de nuvem do fab tratados, mais notadamente com relação à sua confidencialidade. Entretanto, esse risco é mitigado pelos cont utilização de Duplo Fator de Autenticação (2FA) como controle de acesso à console, o isolamento entre os an das informações dos clientes por parte do próprio fabricante>, conforme comprovado por informações contid *Define How We Operate*", acostado ao presente processo sob número 2604878.
    - Outras soluções de segurança adquiridas pelo tribunal já fazem uso do modelo de console instala *antimalware* (conhecida como EDR/XDR, adquirida pelo tribunal por meio do contrato TSE nº 1
  - O licenciamento da solução de Gestão de Vulnerabilidades para o pacote "*Tenable One Enterprise*" represent de software (atualmente contratado pelo tribunal, e que é o modelo associado à 3ª Solução), para o modelo de tribunal, na medida em que esse tipo de solução, mesmo quando licenciada de modo perpétuo, é diretamente o fornecimento de atualizações das bases de dados de vulnerabilidades conhecidas e suas respectivas formas perpétuas, e devem estar sempre vigentes para que a solução seja eficaz.
    - É importante observar que as estimativas de preços solicitadas já contemplaram a conversão das valor da subscrição do pacote "Tenable One". Enterprise".

3.6 - Memória de Cálculo referente às quantidades de licenças

3.6.1 Atualmente o TSE possui o licenciamento do software de gestão de vulnerabilidades com cobertura de 2.500 ativos, cobrindo eq roteadores, *storages*, etc.). Porém não está coberto ainda o ambiente de "containers" (ambiente mais moderno para a disponibilizaçã recente). Assim, as vulnerabilidades existentes no ambiente de *containers* não estão sendo atualmente gerenciadas, e, caso sejam identific sobre o ambiente de TI do tribunal.

3.6.2 A expansão do licenciamento previa uma expansão da quantidade de servidores virtuais para atender às demandas do tribunal, q quantidade de ativos de rede, englobando servidores de rede físicos e virtuais, *switches*, roteadores, *storages, firewalls*, etc, é de 2009 ati COINF e SESOP (2635992), cujo detalhamento segue abaixo:

b.2.1) Servidores virtuais no ambiente VMware: 1700;
b.2.2) Servidores virtuais no ambiente ABIS: 114;
b.2.3) Servidores físicos (bare metal): 20;
b.2.4) Demais ativos de rede: 175.

3.6.3 Conforme citado anteriormente, o tribunal implementou o ambiente de *containers*. Hoje temos cerca de 1200 serviços implementad conteiners.

3.6.4 Atualmente, portanto, temos 3209 ativos que necessitam ser gerenciados quanto a vulnerabilidades.

3.6.5 Segundo informações prestadas pela SESOP, no histórico de e-mails acima citado, a estimativa é de que a quantidade de servidor observada entre 2019 e 2023. Ou seja, potencialmente, em três anos, teríamos 5100 servidores virtuais.

3.6.6 A proposta que trazemos neste ETP é de formalização de uma Ata de Registro de Preços (ARP) que contemple parte do crescimento ARP em quantidade idêntica à atual.

3.6.6.1) Assim, a proposta é de formalização de um Registro de Preços para **3.500 licenças**, porém com adesão inicial de 2.500 l praticamente 500 licenças para a implantação inicial da gerência de vulnerabilidades sobre *containers*. As 1.000 licenças adic gerenciamento de vulnerabilidades referente a este tipo de ativos esteja estabelecido de forma estável, eao eventual crescimento d meses de sua vigência.

3.7 - Quadro Resumo Comparativo de Preços (com base na contratação inicial de 2.500 licenças)

Solução	Descrição	Itens e Quantidades	Custo Estimado (R$)
1ª	Substituição da solução de Gestão de Vulnerabilidades já adquirida por outra disponível no Portal do Software Público Brasileiro	- x -	sem custo de licenciamento
2ª	Desenvolvimento de uma solução própria de Gerenciamento de Vulnerabilidades	- x -	sem custo de licenciamento
3ª	Renovar o licenciamento da solução de Gestão de Vulnerabilidades atualmente utilizada pelo TSE (Tenable.sc+) e adquirir módulos da mesma solução que atendam às funções de gestão de vulnerabilidades em ambiente de containers, e façam a Gestão da Exposição cibernética do Tribunal	Tenable.sc+: 2.500 licenças Tenable Cloud Security: 300 licenças Tenable Lumin: 2.500 licenças	R$ 2.315.100,00
4ª	Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativos de rede (Tenable.sc+) e contratar o licenciamento dos módulos adicionais citados na 3ª Solução por meio de um pacote de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "**Tenable One Standard**"	2.500 licenças	R$ 2.235.000,00
5ª	Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativos de rede (Tenable.sc+), contratar o licenciamento dos módulos adicionais citados na 3ª Solução, e ainda dois módulos adicionais, responsáveis pelo Gerenciamento da Superfície de Ataque (Attack Surface Managemnt) e pela Identificação de Caminhos de Ataque que podem ser explorados por eventuais atacantes (Attack Path Analysis), por meio de um pacote de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "**Tenable One Enterprise**"	2.500 licenças	R$ 2.652.500,00

3.7.1 O "Custo estimado", para cada opção, foi obtido a partir da multiplicação dos quantitativos pelos valores constantes da proposta inferiores aos da empresa Global Sec (2605101).

4. A Solução Escolhida:

4.1. Os motivos ou as justificativas técnicas e econômicas para a escolha da solução, destacando o que a faz mais vantajosa entre todas

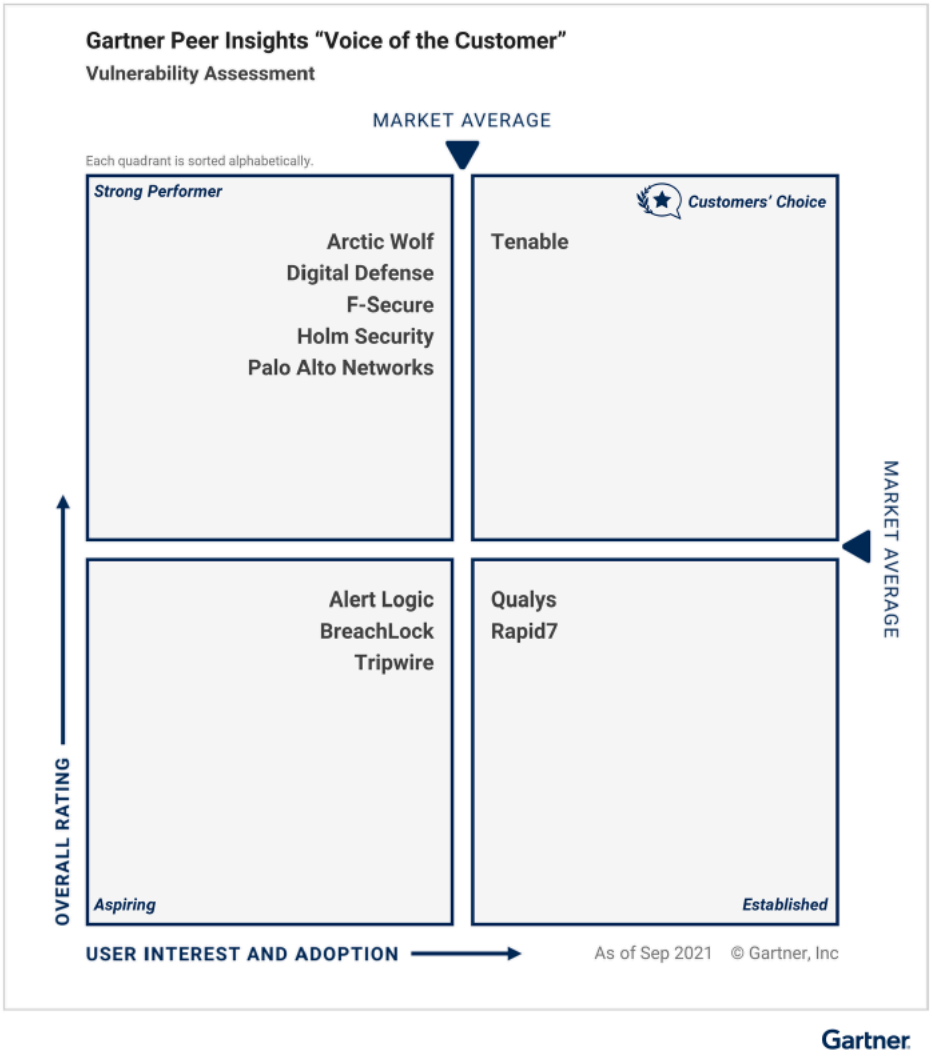
4.1.1. A solução entendida como mais adequada para o TSE é a 4ª Solução - "Renovar o licenciamento do módulo responsável pela funci (*Tenable.sc+*), contratar o licenciamento dos módulos adicionais citados na 3ª Solução, e ainda módulos adicionais, por meio de um p conhecido como "*Tenable One Standard*".

4.1.2. A escolha se justifica pelo fato de a solução contemplar as funcionalidades mínimas necessitadas pelo tribunal, relacionadas notadamente as funcionalidades adicionais fornecidas em função deste modelo de licenciamento, e a desoneração da equipe do TSE c console de gerenciamento, que, por ser instalada em ambiente de nuvem do próprio fabricante, passa a ser de responsabilidade deste.

4.1.2.1. Já a 5ª solução apresenta custo superior ao custo da 4ª solução, por trazer funcionalidades extras ainda não identificadas c a solução indicada para o momento.

4.1.3. A título de informação, destacamos ainda que a solução Tenable continua posicionada como líder do mercado de soluções de G elaborado pelo Gartner, intitulado *Gartner Peer Insights 'Voice of the Customer'*:
Vulnerability Assessment (2604880).

4.1.3.1. O quadro abaixo, extraído do citado documento, evidencia que o produto Tenable encontra-se com em primeiro lugar tanto quanto na quantidade de adoções pelos diversos clientes do mercado de cibersegurança (Eixo X - *User Interest and Adoption*).



4.1.3.2. Essa informação confirma que a continuidade da utilização da solução Tenable, pelo TSE, nos disponibiliza a melhor solução

4.2. Detalhamento da solução:

a) Características básicas do serviço e/ou do material a ser contratado:

a.1) O *Tenable One Standard* é uma solução de software composta pelos seguintes itens:

Módulos	Descrição
Tenable Security Center+	• Avaliação contínua e em tempo real. • Conformidade e segurança com base em riscos para investig forma célere os ativos e as vulnerabilidades mais cruciais.
Nessus	• Avaliação de vulnerabilidades; • Implantação em diversas plataformas. • Mais de 50 modelos pré-configurados que ajudam a entende há vulnerabilidades.
Tenable Lumin	• Visualização dos riscos cibernéticos. • Apoio à decisão, analise e cálculo da eficácia das operações realização de uma análise comparativa com empresas do me • Acompanhamento da redução de riscos ao longo do tempo.
Tenable Cloud Security	• Visibilidade e correção contínua de riscos em recursos e ativos em cloud. • Proteção específica para Kubernetes, containers, ambiente serverless. • Integração nativa com AWS, Azure, GCP e plataformas cloud.
Tenable Web App Scaning	• Gerenciamento da infraestrutura e aplicações WEB. • Verificação de vulnerabilidades abrangente de forma rápida mínimos. • Visibilidade de componentes vulneráveis de aplicações WE vulnerabilidades de código personalizado.

b) Quantidades e as respectivas unidades de medida/fornecimento, com as devidas justificativas, acompanhadas das memórias de cálculo

Grupo	Item	Descrição	Unidade
1	1	Subscrição do licenciamento do software de gestão de vulnerabilidades "*Tenable One Standard*", com garantia por 36 meses	
	2	Serviço de Instalação, configuração e migração da versão atual	
	3	Repasse de conhecimento	
	4	Serviço de suporte técnico, por 36 (trinta e seis) meses.	

b.1) Os quantitativos referentes às licenças (Item 1) são embasados na memória de cálculo contida no item 3.6 deste documento.
b.2) Os quantitativos referentes ao Serviço de Instalação (Item 2) e Repasse de conhecimento (Item 3) são unitários, pois referem-s
fornecimento das licenças;
b.3) O quantitativo referente ao Serviço de suporte técnico é unitário, pois trata-se de um único serviço que deve ser prestado
licenças.

c) Garantia Técnica/Assistência Técnica/ Suporte Técnico:

c.1) A contratação contemplar a Garantia Técnica do software pelo período de 36 (trinta e seis) meses, composto por suporte
atualizações de versões e patches para a correção de problemas identificados pelo fabricante.
c.2) Deverá contar com serviços de suporte por parte da Contratada, complementares ao suporte básico oferecido pelo fabricante d

d) Normas Legais exclusivas:

d.1) Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça - CNJ, que institui a Estratégia Nacional de Segurança
d.2) Estratégia Nacional de Cibersegurança da Justiça Eleitoral (2021 a 2024)

e) Normas Técnicas aplicáveis:

e.1) Não há normas estritamente técnicas que definam como deve ser realizada a Gestão de Vulnerabilidades.
e.2) Entretanto, os principais *frameworks* de segurança atualmente observados pelo mercado recomendam a execução do processo
pelo CNJ como base para a Estratégia Nacional de Segurança Cibernética do Poder Judiciário ENSEC-PJ, pelo TCU, como base para su
Nacional de Segurança da Justiça Eleitoral), bem como da ISO 27001, e outros.
e.3) Res. 23644/2021 que institui a Política de Segurança da Informação da Justiça Eleitoral.
e.4) Portaria 460 de 13 de Julho de 2021, que institui a Norma de Gerenciamento de Vulnerabilidades do TSE.

f) Experiência profissional e formação da equipe técnica de execução do contrato:

f.1) Todo suporte (instalação, configuração, manutenções), deverão ser prestados por pessoa com certificação no software de gestão
f.1.1) A data de validade da certificação deverá estar dentro do período de vigência do contrato.

g) Transição contratual:

g.1) Não aplicável, uma vez que trate-se de renovação de licenciamento do software de gestão de vulnerabilidades atualmente e
licenças existentes.

h) Transferência de conhecimento:

h.1) Será exigida uma atividade de transferência do conhecimento a respeito das diferenças na utilização entre o *Tenable.sc+* (atu
produto que integram esta licitação.

i) Treinamento:

i.1) Não aplicável.

j) Deslocamentos e Reembolso de Diárias e Passagens:

j.1) Não aplicável.

4.3. Outros aspectos relacionados à execução contratual:

a) Prazo de execução e/ou vigência contratual

a.1) A execução do contrato deverá ser iniciada a partir do 1º dia útil após a assinatura do contrato;
a.2) A vigência do contrato será de 36 meses;
a.2.1) A contratação de serviços objeto deste ETP é de natureza continuada, e a fixação de sua vigência em 36 meses é vantajo
1944918.
a.3) De acordo com o art. 84 da Lei nº 14.133/2021, o prazo de vigência da Ata de Registro de Preços será de 1 (um) ano e poderá
vantajoso.

b) Ordem de Serviço Inicial:

b.1) O prazo de fornecimento da solução deverá se iniciar na data da assinatura do contrato, por este motivo, não será necessário a e

c) Itens de controle da execução contratual e verificação para recebimento e pagamento do objeto:

c.1) Recebimento:

c.1.1) Após a assinatura do contrato, a contratada deverá fornecer o licenciamento em até 05 (cinco) dias úteis;
c.1.1.1) No momento da entrega das licenças será emitido o Termo de Recebimento Provisório 01 - TRP01, pelo fiscal d
c.1.1.1.1) A fiscalização deverá emitir o Termo de Recebimento Definitivo 01 - TRD01, após confirmação de que
Referência, no prazo máximo deé 05 (cinco) dias uteis após a emissão do TRP01 e ;
c.1.2) A contratada deverá realizar a instalação conforme as melhores práticas do fabricante e migração do ambiente atual,
emissão do TRD01;
c.1.3) Os fiscais do contrato deverão emitir o Termo de Recebimento Provisório 02 - TRP02, em até 01 (um) dias útil a partir
c.1.4) Após a validação dos serviços previstos no subitem "c.1.2)", a fiscalização deverá emitir o Termo de Recebimento Defini
c.1.4.1) No caso de os fiscais entenderem que a instalação do item "c.1.2)" não esteja em conformidade com o Termo
previstos no referido subitem em até 10 (dez) dias úteis;
c.1.5) A contratada deverá realizar o repasse de conhecimento, com carga horária não inferior a 25h (vinte e cinco), a ser
Referência.
c.1.5.1) Os fiscais de contrato deverão emitir o TRD03 em até 05 (cinco) dias úteis, após o término do repasse de conhe
c.1.6) O serviço de suporte e horas de customizações deverão ser executados sob demanda, dentro da vigência do contrato e c

c.2) Pagamento

c.2.1. O pagamento será efetuado até o 10º (décimo) dia útil, a partir do atesto da nota fiscal/fatura pelo servidor respon
corrente da contratada, observada a ordem cronológica estabelecida na legislação de licitações e contratos.
c.2.2. O atesto de cada item contratado, licenciamento, instalação/configuração/customização, repasse de conhecimento e su
administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA. O fiscal adm
remeter o processo à Coordenadoria de Execução Orçamentária e Financeira - CEOFI, contados do recebimento do docume
documentos exigidos para liquidação e pagamento da despesa.
c.2.3. A contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento após o receb
c.2.4. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta on
nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratação perante a Seguridade Social e Fazen
Trabalhista.

d) Indicadores de Desempenho e Remuneração Variável:

d.1. Os indicadores de desempenho e as respectivas penalidades encontram-se definidos no subitem 8.1.3.

e) Impactos ambientais:

e.1. Não aplicável, uma vez que trata-se de renovação de licenciamento de produto já adquirido e instalado pelo TSE. As funcionali
existente, não gerando qualquer impacto ambiental.

f) Elementos da Matriz de Alocação de Riscos:

f.1) Não se aplica, uma vez que a contratação pretendida não se enquadra nas hipóteses de grande vulto (aqueles cujo valor estimad
integrada (regime de contratação de obras e serviços de engenharia). Adicionalmente, trata-se apenas da renovação do licenciamen
possui e utiliza, de forma que eventuais riscos específicos ao projeto já foram tratados e mitigados anteriormente.

4.4. Diferenças (especificação e quantidades) em relação à última contratação:

4.4.1. Atualmente o TSE detém 2.500 licenças do produto *Tenable.sc+*, tendo sido 1.000 licenças adquiridas originalmente por meio do co
do contrato TSE 128/2022. Conforme citado no item 3.6, a proposta é de renovação dessas 2.500 licenças, com ampliação de funcionalid
de aquisição de até 1.000 licenças adicionais, por meio de uma Ata de Registro de Preços.
4.4.2. O quantitativo adicional previsto neste ETP encontra-se justificado no item 3.6 deste documento.
4.4.3. Os componentes da solução T*enable One Standard* estão descritos no item 4.2, alínea a.1, deste documento.

4.5. Serviços e/ou materiais complementares não contemplados na solução escolhida:

Não aplicável.

5. Valor Estimado da Contratação com Preços Unitários Referenciais e Memória de Cálculo:

5.1. Os valores para a contratação foram estimados a partir de propostas comerciais recebidas de fornecedores dos produtos do fabricante *Te* Sec). Foram adotados como base os valores informados no primeiro documento (Servix), por serem os valores mais baixos entre as duas propost

5.1.1 Aquisição inicial sobre a Ata de Registro de Preços.

5.1.1.1. O valor para a aquisição inicial sobre a Ata de Registro de Preços a ser firmada foi calculado com base no quantitativo de li mesmo quantitativo foi considerado para a funcionalidade *Lumin*, pois as regras de licenciamento do fabricante determinam q gerenciados. A quantidade de licenças para a gerência de vulnerabilidades em *containers* foi estimada inicialmente em 300, embo Tal decisão deveu-se ao fato de que o gerenciamento de vulnerabilidades em containers é uma disciplina que será iniciada a part práticas que eventualmente mostrem ser necessário o gerenciamento de um sub-conjunto dos containers existentes (por hipó gerenciamento de vulnerabilidades de um determinado ambiente de containers, tal como o ambiente de desenvolvimento).

5.1.1.2. A primeira tabela traz os valores referentes à aquisição de cada um dos módulos por meio de licenciamentos apartados (eq a segunda tabela traz os valores referentes ao licenciamento na modalidade *Tenable One* Standard (equivalente à 4º opção de escolhida).

5.1.1.3. Esclarecemos que, na modalidade de licenciamento *Tenable One Standard*, a quantidade de licenças pode flutuar entre os di que o crescimento previsto desde a última contratação ainda não se materializou, parte das 2500 licenças de que o tribunal já dis vulnerabilidades de conteiners. Em função disso, as 300 licenças para conteiners não estão sendo disponibilizadas no cenário de lic

Tenable - Eventual Aquisição dos módulos apartados

Produto	Qtd.	Prazo	P. unitário	P. total
Tenable.sc+	2500	36 meses	442,00	1.105.000,00
Tenable Cloud Security (CS)	300	36 meses	1.617,00	485.100,00
Tenable Lumin	2500	36 meses	290,00	725.000,00
			2.059,00	**2.315.100,00**

TSE - Tenable One - 2500 licenças - Aquisição inicial sobre a Ata

Produto	Qtd.	Prazo	P. unitário	P. total	Diferenç e upgrad
Aquisição Tenable One Standard	2500	36 meses	1.206,00	3.015.000,00	135%
Upgrade do Tenable.sc+ para Tenable One Standard	2500	36 meses	894,00	**2.235.000,00**	

5.1.1.4. Observa-se que a solução escolhida tem custo ligeiramente inferior ao da 3ª opção, contemplando todas as funcionalidade evidencia que a modalidade escolhida, de upgrade do licenciamento atual para o licenciamento *Tenable One Standard*, é bem infe comprovando que as licenças atualmente detidas pelo tribunal estão sendo consideradas para abatimento no custo de licenciament

5.1.1.5. Assim, temos que o custo para a **aquisição inicial** proposta sobre a Ata de Registro de Preços será de **R$ 2.235.000,00**, cob

5.2 Valor total da Ata de Registro de Preços

5.2.1. Conforme citado anteriormente, neste ETP estamos definindo a formalização de uma Ata de Registro de Preços para um total de 3.5 o crescimento do parque de TI do TSE, tanto em termos da quantidade de ativos de rede, quanto da quantidade de *containers*.

5.2.2. Nesse cenário, o valor total da Ata de Regisro de Preços será o seguinte:

Tenable - Eventual Aquisição dos módulos apartados - 3500 licenças

Produto	Qtd.	Prazo	P. unitário	P. total
Tenable.sc+	2500	36 meses	442,00	1.105.000,00
Tenable Cloud Security (CS)	1000	36 meses	1.617,00	1.617.000,00
Tenable Lumin	3500	36 meses	290,00	1.015.000,00
			2.059,00	**3.737.000,00**

TSE - Tenable One - 3500 licenças - Valor total da Ata

Produto	Qtd.	Prazo	P. unitário	P. total	Diferç aquis
Aquisição Tenable One Standard	3500	36 meses	1.206,00	4.221.000,00	135%
Upgrade do Tenable.sc+ para Tenable One Standard	3500	36 meses	894,00	3.129.000,00	

5.2.3. As tabelas acima evidenciam que, no caso de eventual consumo total da Ata de Registro de Preços, o custo da 4º solução (licenci economia ainda maior em relação ao custo da 3ª solução.

5.2.4. Assim, o **valor total da Ata de Registro de Preços seria de R$ 3.129.000,00**.

5.2.5. Destacamos que são valores estimativos, que devem sofrer diminuição como resultado da eventual realização do Pregão.

6. Divisibilidade da Solução (Avaliação do Parcelamento e/ou Agrupamento):

6.1. A solução de software não é divisível, visto que trata-se de software de gestão de vulnerabilidades integrado, composto por módulos específi
6.2. Os serviços de instalação, repasse de conhecimento e suporte técnico, representados pelos itens 2, 3 e 4 também não podem ser dissoci
ligados a ele, de forma que a eventual adjudicação desses itens a licitantes distintas traz diversos riscos, inclusive o da impossibilidade de p
fornecimento das licenças.

7. Aspectos Relacionados à Escolha do Fornecedor, à Forma de Contratação, e às Regras de Participação no Procedimento de Contratação:

7.1. Critérios de Seleção do Fornecedor:

a) Forma de Adjudicação:

a.1) Modalidade de Licitação ou Justificativas para Inexigibilidade ou Dispensa:

a.1.1) Pregão Eletrônico

a.2) Procedimentos Auxiliares:

a.2.1) Sistema de Registro de Preços.

a.3) Critério de Julgamento das Propostas:

a.3.1) Menor preço.

b) Exigências de Qualificação Técnica Profissional e Operacional:

b.1) A empresa contratada deverá apresentar atestado de capacidade técnica referente a prestação de serviço similar ao objet certificados no software de gestão de vulnerabilidades. Os certificados específicos serão detalhados no Termo de Referência.

c) Apresentação de amostras na fase de licitação e/ou prova de conceito, se for o caso:

c.1) Não há necessidade.

d) Vistoria prévia no local de execução dos serviços, se for o caso:

d.1) Não aplicável.

e) Caráter sigiloso para o orçamento estimado da contratação, se for o caso:

e.1) Não aplicável.

f) Critérios técnicos de julgamento das propostas (somente para as licitações com julgamento por técnica e preço ou maior retorno econôı

f.1) Não aplicável.

7.2. Regras de Participação no Procedimento de Contratação:

a) Subcontratação:

a.1) Não há a necessidade de previsão de subcontratação, em razão da simplicidade do objeto.

b) Tratamento diferenciado e favorecido a Microempresas e Empresas de Pequeno Porte (ME/EPP):

b.1) Não há óbice para a aplicação de tratamento diferenciado para ME/EPPs. A empresa deverá ter ciência de que o objeto nã fabricante do software.

c) Formação de Consórcio:

c.1) É permitida a participação de empresas no processo licitatório em regime de Consórcio.

d) Participação de Cooperativas:

d.1) Não aplicável. A participação de cooperativas no certame não ampliará a competitividade e não proporcionará a obten fornecimento do objeto de modo fracionado.

e) Participação de Empresas Estrangeiras:

e.1) É permitida a participação de empresas estrangeiras no processo licitatório.

f) Participação de Pessoa Física:

f.1) Não se aplica uma vez que trata-se de fornecimento de licença de software, instalação, configuração, customização e suporte.

7.3. Particularidades da Contratação:

a) Índice de reajuste:

a.1) Em consonância com o art. 25, § 7º da Lei 14.133/2021, índice de reajuste, para o item 4 - "Serviço de suporte técnico", po (IPEA).

b) Garantia de Execução Contratual:

b.1) Não é necessária, uma vez que cada item somente será pago após completamente entregue e formalmente aceito.

c) Previsão de Conta-Depósito Vinculada:

c.1) Não há necessidade de conta-depósito uma vez que não haverá mão de obra exclusiva.

7.4. Regras para o Sistema de Registro de Preços (se for o caso):

a) Aceitabilidade de Proposta em quantitativo inferior ao máximo previsto em edital:

a.1) Não se aplica uma vez que a quantidade de licenças solicitadas representa a necessidade atual do TSE, que não pode ser atendic

b) Preços diferentes para o mesmo item:

b.1) Não é possível uma vez que trata-se de licença de software determinada e seu valor é único. Os demais serviços especif especificações técnicas de tal forma que não há a possibilidade de atribuições de preços distintos, especialmente considerando-s especificados em apenas uma unidade.

c) Registro de mais de um fornecedor ou prestador de serviço:

c.1) Não é possível em função da indivisibilidade da solução, conforme justificativa constante do item 6 deste documento.

8. Situações que Possam Ensejar Descumprimento do Contrato (Penalidades):

8.1. Nos termos do art. 155 da Lei 14.133/2021, a contratada será responsabilizada administrativamente pelas seguintes infrações:

8.1.1 dar causa à inexecução parcial do contrato;

8.1.2 dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.1.3 dar causa à inexecução total do contrato;

8.1.4 deixar de entregar a documentação exigida para o certame;

8.1.5 não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

8.1.6 não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

8.1.7 ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

8.1.8 apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

8.1.9 fraudar a licitação ou praticar ato fraudulento na execução do contrato;

8.1.10 comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

8.1.11 praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

8.1.12 praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

8.2. Ao responsável pela prática de quaisquer dos atos tipificados como infração administrativa, será aplicada sanção de:

8.2.1 advertência, na ocorrência de causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.2.2 multa, na ocorrência de quaisquer das infrações administrativas previstas no item 8.1. desta Cláusula.

8.2.3 impedimento de licitar e contratar, na ocorrência das condutas previstas nos itens 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6 e 8.1.7 desta Cláusula, sempre que não

8.2.3.1 nesta hipótese, o responsável será impedido de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que

8.2.4 declaração de inidoneidade para licitar ou contratar, na ocorrência das condutas previstas nos itens 8.1.8 , 8.1.9, 8.1.10, 8.1.11 e 8.1.12, bem como no imposição de penalidade mais grave.

8.2.4.1 nesta hipótese, o responsável será impedido de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes fede

8.3. Para efeito de aplicação de penas de advertência e multa, às infrações são atribuídas graus, conforme as tabelas abaixo:

TABELA GRAU X PERCENTUAL	
GRAU	CORRESPONDÊNCIA
1	Advertência
2	0,5% sobre o valor total contratado
3	1% ao dia sobre o valor total das licenças
4	1% ao dia sobre o valor do serviço demandado

Item	**Descrição**	**Incidência**	**Limite m aplicaçã**
1	Deixar de cumprir quaisquer das obrigações previstas no Edital e não prevista neste tabela de multas	Por ocorrência	1 (uma) o
2	Deixar de cumprir quaisquer obrigações previstas no Edital e não previstas nesta tabela de multas, após reincidência formalmente notificada pelo fiscal do contrato.	Por ocorrência	3 (três) oc
3	Deixar de cumprir o prazo para entrega das licenças.	Por dia	10 (dez) c corridos
4	Deixar de cumprir os prazos previstos para os tempos de atendimento às solicitações de suporte e atualizações da solução ou do repasse de conhecimento.	Por dia	5 (cinco) corridos

8.4. Ultrapassado o limite máximo de aplicação da penalidade previsto na tabela de infração, a Administração poderá optar uma das seguintes hipótese
8.4.1. Presente o interesse público, aceitar o objeto mediante justificativa com aplicação apenas da multa de mora e/ou convencional. A aceitaç que sua recusa causará prejuízo à Administração.
8.4.2. Caso o objeto ainda não tenham sido recebidos pelo Contratante, no todo ou em parte, recusar o objeto e rescindir o contrato, configurar 20% (vinte por cento) do valor total contratado, sem prejuízo das demais consequências previstas em lei e no instrumento contratual.
8.4.3. Caso o todo ou parte do objeto já tenha sido recebidos pelo Contratante, rescindir o contrato e recusar o restante do objeto, se aplicáv compensatória de 15% (quinze por cento) do valor total contratado, sem prejuízo das demais consequências previstas em lei e no instrumento c
8.4.4. As multas de mora ou convencional não serão cumuladas com a multa compensatória proveniente de inexecução contratual pela mesma i poderá ter seu valor abatido do montante apurado da multa compensatória, desde que decorrentes da mesma infração/ocorrência.
8.5. Na aplicação das penalidades, a Autoridade Competente poderá considerar, além das previsões legais, contratuais e dos Princípios da Administraçã
8.5.1. a natureza e a gravidade da infração contratual;
8.5.2. as peculiaridades do caso concreto;
8.5.3. as circunstâncias agravantes ou atenuantes; e
8.5.4. os danos que dela provierem para a Administração Pública;
8.5.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;
8.5.6. a vantagem auferida pela contratada em virtude da infração;
8.5.7. os antecedentes da contratada.
8.6. Os prazos de adimplemento das obrigações contratadas admitem prorrogação, em caráter excepcional, sem efeito suspensivo, devendo a solicit (cinco) dias úteis do seu vencimento, anexando-se documento comprobatório do alegado pela contratada, ficando a aceitação da justificativa a critério
8.7. Se a contratada não recolher o valor da multa que lhe for aplicada, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamer dívida, consoante o art. 156 da Lei nº 14.133/2021, acrescida de juros moratórios de 0,5% (meio por cento) ao mês.

8.8. A recusa da licitante vencedora em assinar o contrato ou aceitar a nota de empenho no prazo estabelecido pela Administração será considerada c
das sanções previstas em lei e no Edital da Licitação e a imediata perda da garantia de proposta em favor do TSE, quando for o caso.
8.9. As sanções serão registradas e publicadas no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas P
prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, nos termos do art. 161 da Lei nº 14.133/2021.
8.10. O período de atraso será contado em dias corridos, salvo disposição em contrário.
8.11. As multas de mora e por inexecução parcial, quando aplicadas em razão de descumprimento contratual, não ultrapassarão o limite de __% (___
cada item como um contrato em apartado, salvo no caso de agrupamento de itens em lote. (OBS: CONFORME PARECERES, ESTE PERCENTUAL DE
LIMITADO A 30% DO VALOR DO CONTRATO, O QUE NÃO IMPEDE DEFINIÇÃO DE PERCENTUAL INFERIOR DESDE QUE LIMITADO A 0,5% (§ 3º do art.
8.12. Antes da aplicação da sanção de multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimaçã
8.13. Antes da aplicação das sanções de impedimento de licitar e contratar ou declaração de inidoneidade para licitar ou contratar, a comissão
CONTRATADA para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda pr
8.13.1. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o
prazo de 15 (quinze) dias úteis, contado da data da intimação.
8.14. Os atos previstos como infrações administrativas na Lei nº 14.133/2021 ou em outras leis de licitações e contratos da Administração Pú
12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na
8.15. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática
confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com p
do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla
8.16. É admitida a reabilitação da CONTRATADA perante a própria autoridade que aplicou a penalidade, nos termos do art. 163 da Lei nº 14.133/2021
8.17. O CONTRATANTE deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizad
publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbi
8.18. Da aplicação das sanções de advertência, multa ou impedimento de licitar ou contratar caberá recurso no prazo de 15 (quinze) dias úteis, contad
8.18.1 O recurso deverá ser dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) d
superior, a qual deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos, conforme art. 167 da L
8.19. Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar caberá apenas pedido de reconsideração, que deverá ser ap
intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.
8.20. Fica estabelecido que as situações omissas serão resolvidas entre as partes contratantes, respeitados o objeto do contrato, a legislação e
14.133/2021, aplicando-lhe, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

9. Critérios e Práticas de Sustentabilidade Socioambiental:

9.1. Critérios e práticas de sustentabilidade exigidos na contratação e os meios e momento para comprovação:

9.1.1. A partir de consulta ao sistema "Painel Gerencial - Critérios de Sustentabilidade," selecionamos a Informação SEGESA/COGE
tratar de aquisição de licenças de software, bastante semelhante, portanto, à aquisição ora pretendida.

9.1.2. A referida informação traz a seguinte recomendação quanto aos critérios de sustentabilidade:

"10. Em suma, sugere-se a verificação sobre a incidência dos seguintes critérios de sustentabilidade:

- *A contratada não deve possuir inscrição no cadastro "lista suja" de empregadores flagrados explorando trabalhad*
- *A contratada ou seus dirigentes não devem ter sido condenados por infringir as leis de combate à discriminação de*
- *Apresentação do Programa de Controle Médico de Saúde Ocupacional (PCMSO);*
- *Atendimento à reserva de vagas para pessoas com deficiência;*
- *Priorização do uso de mídia digital.*
- *Acessibilidade para o uso de softwares e aplicativos."*

9.1.3. No entendimento desta Equipe de Planejamento da Contratação, apenas os seguintes critérios de sustentabilidade são necessário

9.1.3.1. Comprovar, como condição para participação na licitação, não possuir inscrição no cadastro de empregadores que ten
(Portaria Interministerial MTPS/MM/IRDH nº 4/2016). A comprovação desse critério será efetuada a partir da c
(https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/areas-de-atuacao/cadastro_de_empregadores.pdf
Ministério do Trabalho e Emprego.

9.1.4. Comprovar, como condição para contratação, não ter sido condenada, a adjudicatária e seus dirigentes, por infringir as leis de co
ao trabalho escravo, em afronta ao previsto nos arts. 1º e 170 da Constituição Federal de 1988; no art. 149 do Código Penal; no Decret
Convenções nºs 29 e 105 da Organização Internacional do Trabalho. Deverá ser apresentada Certidão Judicial de Distribuição ("nada c
Comum, Federal e Estadual**,** da adjudicatária e de seus dirigentes.

9.1.5. Priorização do uso de mídia digital.

9.1.6. As licenças adicionais de uso da ferramenta, a serem fornecidas em decorrência da eventual contratação, devem preferencialmer
a partir da internet.

9.2. Justificativa fundamentada para eventual afastamento de critérios ou práticas de sustentabilidade sugeridos pela Unidade de Gest

9.2.1. Os seguintes critérios foram afastados:

9.2.1.1. Apresentação do Programa de Controle Médico de Saúde Ocupacional (PCMSO) e Atendimento à reserva de vagas para pes
referente ao licenciamento do produto, e conta apenas com serviços pontuais, como a instalação das próprias licenças adqui
licenciamento atual (Tenable.sc+ e Tenable One Standard), e demandas eventuais de suporte técnico.
9.2.1.2. Acessibilidade para uso de softwares e aplicativos, uma vez que não se trata de software para utilização para o público em
que não tem necessidades de acessibilidade. Adicionalmente, trata-se de solução de mercado muito específica, que não dispõe de re

9.3. Acessibilidade:

9.3.1. Não aplicável, visto que trata-se de fornecimento de subscrição de licenciamento de software, e da eventual prestação de serviço de

10. Informações Complementares:

10.1. Restrições de caráter técnico, operacional, regulamentar, financeiro e/ou orçamentário:

10.1.1. Não há. Trata-se software já adquirido previamente e em utilização no TSE, de forma que todos os requisitos necessários já se enco

10.2. Cessão de Direitos patrimoniais do projeto:

10.2.1. Não aplicável, visto se tratar de subscrição de licenciamento de software com serviço de suporte eventual.

10.3. Classificação Contábil (contratação de softwares):

10.3.1. A classificação contábil é LOCAÇÃO DE SERVIÇOS (SUBSCRIÇÃO DE SOFTWARE) - ALUGUEL DE SOFTWARE DESPESA CORRENTE
10.3.2. Não é possível estimar com certo grau de certeza o tempo (ou prazo) de utilidade do ativo intangível a ser adquirido, sendo con subscrição de software.

10.4. Vedações de Contratação:

10.4.1 Não há.

10.5. Outras Observações:

10.5.1 Não há.

CARLOS EDUARDO MIRANDA ZOTTMANN
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **10/10/2023, às 14:04**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

REINALDO NONATO DA SILVA
TÉCNICO(A) JUDICIÁRIO(A)

Documento assinado eletronicamente em **10/10/2023, às 14:04**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

KEMEO RAMALHO DE MELO
ANALISTA JUDICIÁRIO(A)

Documento assinado eletronicamente em **10/10/2023, às 16:25**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Tribunal Superior Eleitoral

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2636688&crc=E7B7205 e o código CRC **E7B72055**.