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. Identificação e gestão das vulnerabilidades existentes ao ambiente de tecnologia da informação do TSE, de forma a contribuir ocorrência de incidentes de segurança cibernética que afetem o tribunal. Complementação das funcionalidades já existentes na soluç de forma a também viabilizar essa identificação e gestão de vulnerabilidades no ambiente de containers, implementado no tribunal e equipe de cibersegurança do TSE de funcionalidades que facilitem a tarefa de comunicar o status de riscos cibernéticos à alta gestão compreendida sob o ponto de vista negocial.

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 p Tecnologia da Informação e Comunicação - TIC como meio para atingirem seus objetivos. Dessa forma, ocorre um aumento da mundial - Internet, o que expõe ao mundo externo uma maior quantidade de vulnerabilidades existentes em seu ambiente de T crescimento dos incidentes de segurança.

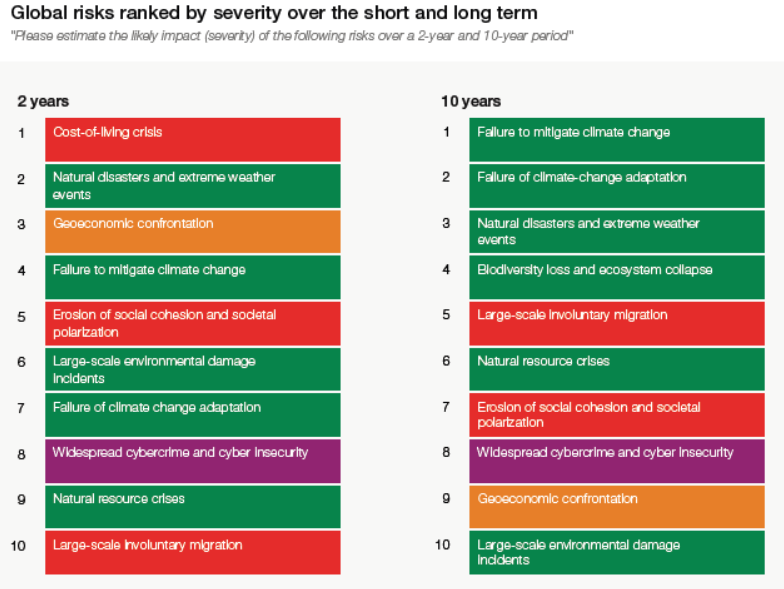
1.2.1.2. Segundo a referência do *Gartner* sobre Gerenciamento de Exposição Cibernética (*Exposure Management*), "Até 2026, as investimentos em segurança com base em um programa contínuo de gerenciamento de exposição, terão três vezes menc (*Implement a Continuous Threat Exposure Management* - CTEM - *Program, Gartner,* julho de 2022) (ht 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 (G cibernética.

1.2.1.2.2. Através do Gerenciamento de Exposição o TSE tem uma visão completa de toda a superfície de ataque (vulnera precisa de acordo com a 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 maturidade de avaliação dos riscos e do impacto positivo das correções sugeridas.

1.2.1.3. De acordo com o *Global Risks Report* de 2023, publicado pelo *World Economic Forum* [1] o risco de ciber crimes e insegu *and cyber insecurity*) figura em oitavo lugar tanto na estimativa dos riscos mais relevantes a curto prazo (2 years - 2 anos) qu conforme a figura abaixo:



1.2.1.4. O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), por sua vez, provê gráficos anu segurança. No gráfico abaixo, podemos observar que de janeiro a junho de 2023, já ocorreram 69% de incidentes em comparação con

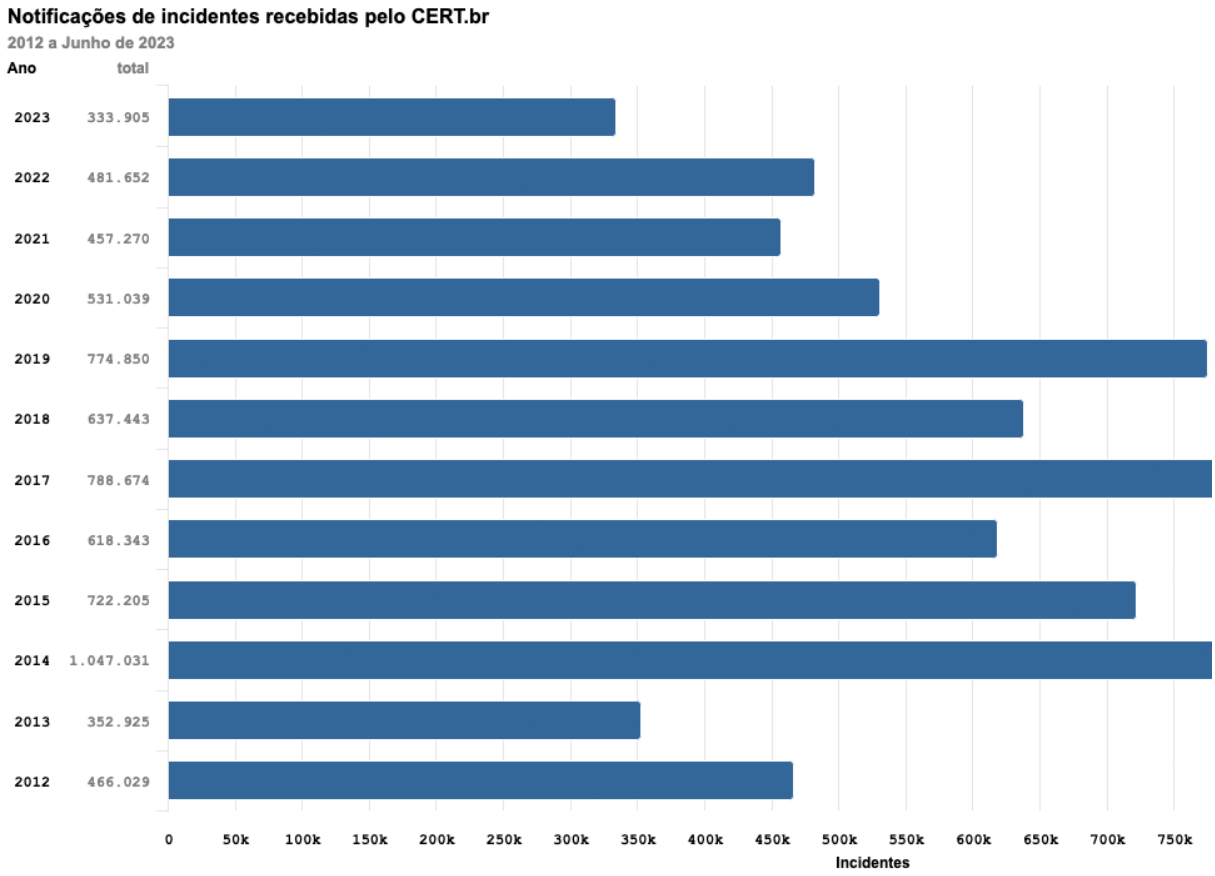


Imagem 01 - Notificações de Incidentes recebidos pelo CERT.BR (Fonte: CERT.BR disponível em https://stats.cert.br/incidentes/ acess

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

1.2.1.6. Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem re organização, os quais podem ser evitados por 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, po segurança.

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 sistem hardware com *keyloggers*;

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 d funcionamento dos sistemas, bem como eventualmente possibilita o sequestro de dados, instalação e ativação de n

1.2.1.8.5. Software: falhas na implementação dos requisitos de segurança ou na codificação dos sistemas operacion desenvolvimento de sistemas, abrindo "brechas" com potenciais pontos de exploração de vulnerabilidades no ambi

1.2.1.9. Os atacantes se utilizam, como uma das primeiras etapas do planejamento e realização de um ataque, de técnicas de varredu como alvo, com o intuito de identificar vulnerabilidades ali existentes. Esse processo da varredura é tecnicamente conhecido como CERT.BR reportados de janeiro a junho de 2023, demonstram que os incidentes por "*Scan*" correspondem a 68,67% do total de incidentes.

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Junho de 2023

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%)		Out
jan	59.030	11.827	20,04	2.843	4,82	63	0,11	41.691	70,63	605	1,02	2.00
fev	47.990	7.503	15,63	2.510	5,23	82	0,17	37.037	77,18	643	1,34	21
mar	53.792	8.258	15,35	2.987	5,55	105	0,20	40.289	74,90	1.230	2,29	92
abr	41.809	6.404	15,32	2.669	6,38	165	0,39	30.195	72,22	1.027	2,46	1.34
mai	69.974	2.369	3,39	3.631	5,19	143	0,20	44.519	63,62	363	0,52	18.94
jun	61.310	3.460	5,64	2.814	4,59	100	0,16	35.576	58,03	295	0,48	19.06
Total	333.905	39.821	11,93	17.454	5,23	658	0,20	229.307	68,67	4.163	1,25	42.50

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

1.2.1.10. Isso significa que, para a construção de um sistema de defesa cibernética eficaz, o TSE necessita conhecer as vulner esse conhecimento precisa ser complementado por informações que indiquem como tratar tais vulnerabilidades, de forma identificadas e exploradas por atacantes. Essa é a função principal 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, para auxiliar na prevenção e limita com análise contínua e adaptável de risco e confiança, a fim de manter a confidencialidade, a disponibilidade e a integrid cobertura e de suas funcionalidades, atualização de versão, suporte técnico especializado e horas de customizações e configu dos contratos TSE nº 109/2020 e TSE nº 128/2022, garantindo alcançar todos os Ativos de de TI pertinentes, propiciando as panorama completo sobre as vulnerabilidades existentes e possam direcionar esforços para mitigá-los, de forma a atingir melh relação ao ambiente de TI do Tribunal.

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 sistema possibilidade de ocorrência de 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 comprometer a s **segurança cibernética** derivados de vulnerabilidades existentes no ambiente computacional do TSE não poder conhecimento (detecção), fragilizando assim o ambiente e incrementando a probabilidade da ocorrência de incident

1.2.4.2. Dependendo do tipo de vulnerabilidade, poderá ocorrer indisponibilidade de sistemas, bloqueio e usurp Eleitoral, com o potencial de 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 d

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

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

1.2.6.1. A solução deve ser capaz de identificar, no parque de tecnologia da informação do TSE, vulnerabilidades já catalogadas vulnerabilidades de aceitação mundial, além de possuir funcionalidades que permitam a identificação de quais vulnerabilidades de TI do tribunal, e deve ser capaz de gerar visualizações e relatórios que possam suportar decisões referentes à priorização do t

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 atrav
SEI nº 2020.00.000008444-6);

2.2. Fase Interna da Licitação (Exigências e sugestões exaradas pela Assessoria Jurídica (Pareceres Asjur) e Controle Interno
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
divisão do licenciamento.

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, dili
certame anterior.

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 contra

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 pe
prestados ao longo dos contratos 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 d
Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Br
3.1.1.2. O principal objetivo do Portal é promover o desenvolvimento de uma ambiente colaborativo que não só reduz os cu
desenvolvimento de artefatos tecnológicos. O conceito de utilização livre de código fonte, é central para o Portal do Software Púb
3.1.1.3. Já são 81 softwares catalogados para compartilhamento. **Não foi encontrada solução de gestão de vulnerabilida
ETP. (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 que a STI/TSE desenvolvesse uma solução (hardware e softwar
já catalogadas em repositório internacional confiável, realizasse rotinas de varreduras (scans) de vulnerabilidades sobre o amb
diversos tipos de ativos (servidores de rede, servidores de aplicações, servidores de bancos de dados, estações de trabalho, etc
riscos e impactos dessas vulnerabilidades sobre o ambiente do TSE.
3.2.1.2. Este tipo de desenvolvimento demandaria da equipe de TI do TSE uma expertise que esta não possui, além de repres
complexa, composta por diversos 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
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 (co
solução desenvolvida.
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 mód
funções de gestão de vulnerabilidades em ambiente de conteiners, e façam a Gestão da Exposição cibernética do Tribunal, conforme r

3.3.1.1. Renovação do licenciamento do Tenable.sc (o atual licenciamento dos direitos de atualização de versões e s
30/12/2023)
3.3.1.1.1. Rastreamento automatizado de ativos, vulnerabilidades e progresso de SLA com base em uma variec
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, analise e calcule a eficácia das operações de segurança e faça uma análise compara
segmento;

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

3.3.1.4. Vantagens

3.3.1.4.1. A continuidade de utilização da ferramenta de Gestão de Vulnerabilidades já adquirida pelo TSE, apro empregado na instalação e configuração da solução, bem como o conhecimento técnico já adquirido pela equip

3.3.1.4.2. Expansão das funcionalidades disponíveis no licenciamento atual, permitindo que o tribunal efetue a componentes de seu parque atualmente não atendidos.;

3.3.1.5. Desvantagens

3.3.1.5.1. Maior dificuldade na fiscalização e gestão contratual, pois seriam adquiridos três licenciamentos disti módulos;

3.3.1.5.2. Maior dificuldade na configuração da console de gerência da solução, pois os três licenciamentos teri separadamente na console;

3.3.1.5.3. Nesse modelo, a console de gerência permaneceria sendo instalada e operada na infraestrutura do t equipe técnica seja a responsável pelas tarefas de manutenção e atualização das versões de software dessa co

3.4. - 4ª Solução:

3.4.1. Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativ o licenciamento dos módulos adicionais citados na 3ª Solução por meio de um pacote de Licenciamento integrado dispor como "*Tenable One Standard*".

3.4.1.1 Vantagens

3.4.1.1.1. Todos os módulos são licenciados sob um mesmo pacote de licenciamento, facilitando a gestão e fisc
3.4.1.1.2. As quantidades de licenças passam a poder flutuar entre os módulos licenciados. Assim, caso, em un necessárias mais licenças para o módulo *Tenable Cloud Security* e menos licenças para o Tenable.sc+, essa flu necessidade de modificação do licenciamento (i.e., sem a necessidade de modificações contratuais);
3.4.1.1.3. Disponibiliza, sob o mesmo pacote de licenciamento, as funcionalidades adicionais abaixo detalhadas licenciamento individual);
3.4.1.1.4. A console de gerenciamento passa a operar em provedor de nuvem do próprio fabricante, desoneran manutenção e atualização do software dessa console de gerenciamento.

3.4.1.2. 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 risco tratados, mais notadamente com relação à sua confidencialidade. Entretanto, esse risco é mitigado pelos contr fabricante, tais como a utilização de Duplo Fator de Autenticação (2FA) como controle de acesso à console, o is diferentes clientes, e <garantia técnica de não acesso das informações dos clientes por parte do próprio fabrica informações contidas no documento "*Your Data Security and Privacy Requirements Define How We Operate*", a número 2604878
    - Outras soluções de segurança adquiridas pelo tribunal já fazem uso do modelo de console instalada e a exemplo da solução *antimalware* (conhecida como EDR/XDR, adquirida pelo tribunal por meio do co nº 2021.00.000012017-0);
  - O licenciamento da solução de Gestão de Vulnerabilidades para o pacote "*Tenable One Standard*" representa u modelo de licença perpétua de software (atualmente contratado pelo tribunal, e que é o modelo associado à 3ª subscrição. Tal mudança não representa desvantagem para o tribunal, na medida em que esse tipo de solução perpétuo, é diretamente dependente dos direitos de atualização da solução, que englobam o fornecimento de vulnerabilidades conhecidas e suas respectivas formas de mitigação, direitos esses que não compõem as licen vigentes para que a solução seja eficaz.
    - É importante observar que as estimativas de preços solicitadas já contemplaram a conversão das lice tribunal em abatimento do valor da 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 ativ licenciamento dos módulos adicionais citados na 3ª Solução, e ainda dois módulos adicionais, responsáveis pelo Gerencia (*Attack Surface Managemnt*) e pela Identificação de Caminhos de Ataque que podem ser explorados por eventuais atacan de um pacote de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "*Tenable One Enterprise*":
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 deter necessárias mais licenças para o módulo Tenable Cloud Security e menos licenças para o Tenable.sc+, essa flutuaçã de modificação do licenciamento (i.e., sem a necessidade de modificações contratuais)
3.5.1.3. Disponibiliza, sob o mesmo pacote de licenciamento, as funcionalidades adicionais abaixo detalhadas (em c o pacote Tenable One Standard).
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 Intern conhecidos e desconhecidos.
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 ambiente na nuvem.

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

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.

3.5.1.4. Vantagens:

3.5.1.4.1. Essa opção traz o maior conjunto de funcionalidades relativas ao Gerenciamento de Exposição Ciberr

3.5.1.4.1.1. A funcionalidade de Gerenciamento da Superfície de Ataque permite conhecer, em tempo real efetivamente sob o alcance de potenciais atacantes externos;

3.5.1.4.1.2. A funcionalidade de Análise de Caminhos de Ataque permite uma melhor visibilidade sobre os auxiliando a priorizar a implantação das correções de segurança mais urgentes;

3.5.1.4.2. A utilização da console de gerenciamento hospedada na nuvem do fabricante elimina os esforços par solução, bem como para a atualização para novas versões;

3.5.1.4.3. Este modelo permite a flutuação (flexibilização/mobilidade) do licenciamento entre funcionalidades d cenários de utilização, bem como na avaliação de eventuais novas funcionalidades vem a ser disponibilizadas p licenciamento adicional (quantidade).

3.5.1.5. Desvantagens:

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

3.5.1.5.2. As funcionalidades de "*Attack Surface Management*" e "*Attack Path Analysis*" são ofertas recentes da análise mais detida sobre as informações que provêem.

- Observações:
  - A exemplo da 4ª solução, A utilização da console de gerenciamento da solução em ambiente de riscos à segurança dos dados por ela tratados, mais notadamente com relação à sua confidencia mitigado pelos controles de segurança implantados pelo fabricante, tais como a utilização de Du controle de acesso à console, o isolamento entre os ambientes de diferentes clientes, e <garant informações dos clientes por parte do próprio fabricante>, conforme comprovado por informaçõ *Security and Privacy Requirements Define How We Operate*", acostado ao presente processo sol
    - Outras soluções de segurança adquiridas pelo tribunal já fazem uso do modelo de con do fabricante, a exemplo da solução *antimalware* (conhecida como EDR/XDR, adquirid TSE nº 11/2022 - Processo SEI nº 2021.00.000012017-0);
  - O licenciamento da solução de Gestão de Vulnerabilidades para o pacote "*Tenable One Enterpris* licenciamento, do modelo de licença perpétua de software (atualmente contratado pelo tribunal Solução), para o modelo de subscrição. Tal mudança não representa desvantagem para o tribun solução, mesmo quando licenciada de modo perpétuo, é diretamente dependente dos direitos d englobam o fornecimento de atualizações das bases de dados de vulnerabilidades conhecidas e mitigação, direitos esses que não compõem as licenças perpétuas, e devem estar sempre vigen
    - É importante observar que as estimativas de preços solicitadas já contemplaram a cor adquiridas pelo tribunal em abatimento do valor da subscrição do pacote "Tenable On

3.6. Órgãos públicos e/ou entidades que adotam solução similar:

3.6.1. Os seguintes órgãos públicos adotam soluções Tenable.

3.6.1.1 Tenable sc+: TRE-PB, e todos os demais TREs que foram partícipes da respectiva Ata de Registro de preços
3.6.1.1.1 Ata de Registro de Preços nº 101/2020 TRE-PB,

3.6.1.2 Tenable One (versão Standard ou Enterprise)
3.6.2.1. Tribunal Regional do Trabalho da 8ª Região - TRT 8;
3.6.2.1.1. Pregão Eletrônico nº 004/2022 (SRP);
3.6.2.2. Procuradoria Geral do Estado da Bahia - PGE BA;
3.6.2.2.1. Pregão Eletrônico nº 007/2022;
3.6.2.3. Empresa Mato-Grossense de Tecnologia da Informação - MTI/MT;
3.6.2.3.1. Pregão Eletrônico nº 023/2022.

Quadro Resumo Comparativo

Solução	Descrição	Itens e Quantidades	Custo Estimado (R$)	
1ª	Substituição da solução de Gestão de Vulnerabilidades já adquirida por outra disponível no Portal do Software Público Brasileiro	- x -	sem custo de licenciamento	Solução cons desvantagens
2ª	Desenvolvimento de uma solução própria de Gerenciamento de Vulnerabilidades	- x -	sem custo de licenciamento	Solução cons desvantagens
3ª	Renovar o licenciamento da solução de Gestão de Vulnerabilidades atualmente utilizada pelo TSE (Tenable.sc+) e adquirir módulos da mesma solução que atendam às funções de gestão de vulnerabilidades em ambiente de containers, e façam a Gestão da Exposição cibernética do Tribunal	Tenable.sc+: 2.500 licenças Tenable Cloud Security: 300 licenças Tenable Lumin: 2.500 licenças	R$ 2.315.100,00	Esta solução necessárias ac

Solução	Descrição	Itens e Quantidades	Custo Estimado (R$)	
4ª	Renovar o licenciamento do módulo responsável pela funcionalidade de gerenciamento de vulnerabilidades de ativos de rede (Tenable.sc+) e contratar o licenciamento dos módulos adicionais citados na 3ª Solução por meio de um pacote de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "**Tenable One Standard**"	2.500 licenças	R$ 2.235.000,00	A solução co necessitadas flutuação de l Assim, será po de Cloud Secu de vulnerab necessidade d
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	A solução co opção anteric *Attack Surfac* Superfície de de Caminhos d

4. A Solução Escolhida:

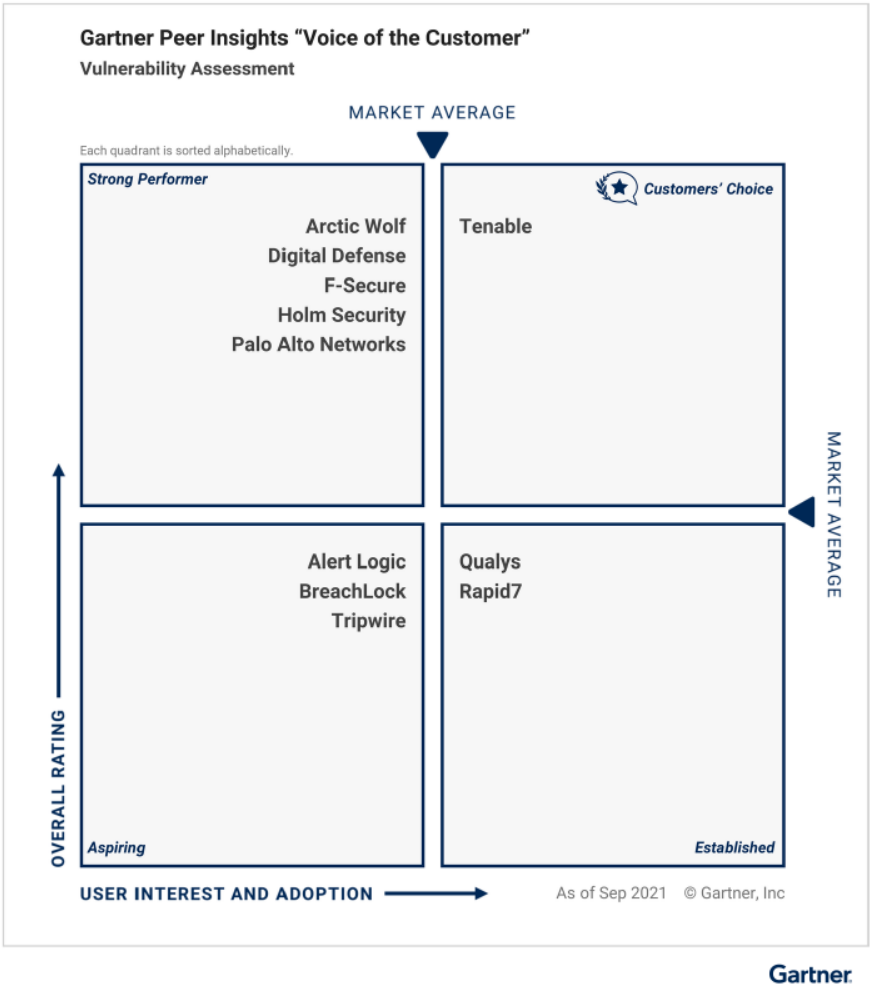
4.1. Os motivos ou as justificativas técnicas e econômicas para a escolha da solução, destacando o que a faz mais identificadas:

4.1.1. A solução entendida como mais adequada para o TSE é a 4ª Solução - "Renovar o licenciamento do módulo responsável p vulnerabilidades de ativos de rede (*Tenable.sc+*), contratar o licenciamento dos módulos adicionais citados na 3ª Solução, e ainda m de Licenciamento integrado disponibilizado pelo fabricante, conhecido como "*Tenable One Standard*".

4.1.2. A escolha se justifica pelo fato de a solução contemplar as funcionalidades mínimas necessitadas pelo tribunal, relacionad vantagens sobre a mesma, notadamente as funcionalidades adicionais fornecidas em função deste modelo de licenciamento, e a desc tarefas de manutenção e atualização de versões da console de gerenciamento, que, por ser instalada em ambiente de nuver responsabilidade deste.

4.1.3. A título de informação, destacamos ainda que a solução Tenable continua posicionada como líder do mercado de soluções comprovado pelo documento 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 produto (Eixo Y - *Overall Rating*) quanto na quantidade de adoções pelos diversos clientes do mercado de cibersegurança (Eixo X



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

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 investiga e priorizar de forma célere os ativos e as vulnerabilidades mai cruciais.
Nessus	• Avaliação de vulnerabilidades; • Implantação em diversas plataformas. • Mais de 50 modelos pré-configurados que ajudam a entender rapidamente onde há vulnerabilidades.
Tenable Lumin	• Visualização dos riscos cibernéticos. • Apoio à decisão, analise e cálculo da eficácia das operações d segurança, e realização de uma análise comparativa com empresas do mesmo segmento. • 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 c ajustes mínimos. • Visibilidade de componentes vulneráveis de aplicações WEB e de vulnerabilidades de código personalizado.

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

b.1) Atualmente o TSE possui o licenciamento do software de gestão de vulnerabilidades com cobertura de 2.500 ativos, cobrind de ativos de rede (*switches*, roteadores, *storages*, etc.). Porém não está coberto ainda o ambiente de "containers" (ambiente aplicações, adotado pelo tribunal no passado relativamente recente). Assim, as vulnerabilidades existentes no ambiente de gerenciadas, e, caso sejam identificadas por atacantes, podem vir a representar incidentes cibernéticos sobre o ambiente de TI c

b.2) A expansão do licenciamento previa uma expansão da quantidade de servidores virtuais para atender às demandas do velocidade esperada. Atualmente, a quantidade de ativos de rede, englobando servidores de rede físicos e virtuais, *switches*, 2009 ativos, conforme detalhamento 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.

b.3) Conforme citado anteriormente, o tribunal implementou o ambiente de *containers*. Hoje temos cerca de 1200 serviços im significa que temos 1200 imagens de conteiners.

b.4) Atualmente, portanto, temos 3209 ativos que necessitam ser gerenciados quanto a vulnerabilidades.

b.5) Segundo informações prestadas pela SESOP, a estimativa é de que a quantidade de servidores virtuais seja triplicada. teríamos 5100 servidores virtuais.

b.6) A proposta que trazemos neste ETP é de formalização de uma Ata de Registro de Preços (ARP) que contemple parte do cre demanda inicial sobre essa eventual ARP em quantidade idêntica à atual.

b.6.1) Assim, a proposta é de formalização de um Registro de Preços para **3.500 licenças**, porém com adesão inicial de 2 atenderiam a eventual crescimento dos ambientes de servidores e de *containers* durante o período de 12 meses de sua vig

c) Garantia Técnica/Assistência Técnica/ Suporte Técnico:

c.1) A contratação deverá prever o suporte por parte do fabricante da solução, pelo período de 36 (trinta e seis) meses, p licitações, atualizações de versões e aplicações de parches, durante o mesmo período, e consultoria para fins de customiza práticas definidos pelo fabricante e configuração avançada da solução.

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 Se ENSEC-PJ.
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 pr exemplo do CIS *Controls* (utilizado pelo CNJ como base para a Estratégia Nacional de Segurança Cibernética do Poder Judiciário auditorias sobre segurança cibernética, e pela própria Estratégia Nacional de Segurança da Justiça Eleitoral), bem como da ISO 2
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 licitação.
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 de serviços associados às 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.s funcionalidades adicionais a este 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 12 meses, prorrogáveis

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 necessár

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
c.1.1.1.1) A fiscalização deverá emitir o Termo de Recebimento Definitivo 01 - TRD01, após confirmação de que especificado no Termo de 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 atu 20 (vinte) dias úteis após a 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 previstos no subitem acima;
c.1.4) Após a validação dos serviços previstos no subitem "c.1.2)", a fiscalização deverá emitir o Termo de Recebimento I útil;
c.1.4.1) No caso de os fiscais entenderem que a instalação do item "c.1.2)" não esteja em conformidade com o Te realizar a correção dos serviços 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 à 40h (quarenta horas), a fiscais de contrato e a contratada.
c.1.5.1) Os fiscais de contrato deverão emitir o TRD03 em até 05 (cinco) dias úteis, após o término das 40h (quare equipe técnica do TSE.
c.1.6) O serviço de suporte e horas de customizações deverão ser executados sob demanda, dentro da vigência do contra Referência.

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 para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida na legislação de licitações e c
c.2.2. O atesto de cada item contratado, licenciamento, instalação/configuração/customização, repasse de conhecimento sob demanda será pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica nº 14/2017 - TSE. O fiscal administrativo terá o prazo de 5 (cinco) dias úteis para emitir a NTA e remeter o processo à Co Financeira - CEOFI, contados do recebimento do documento fiscal, do Termo de Recebimento Definitivo - TRD e dos dema pagamento da despesa.
c.2.3. A contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento após o re
c.2.4. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta de Fornecedores - SICAF, ou nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratação perante Fundo de Garantia por Tempo de serviço e a Justiça Trabalhista.

d) Indicadores de Desempenho e Remuneração Variável:

d.1. Não aplicável.

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 funcion ativadas sobre a solução já existente, não gerando qualquer impacto ambiental.

f) Elementos da Matriz de Alocação de Riscos:

f.1. Tendo em vista que a matriz de alocação de riscos irá descrever as ameaças que possam vir a comprometer o sucesso e o c de que formas devem ser tratadas, ela permeará todo processo de contratação:

01 - RISCOS DO PROCESSO DE CONTRATAÇÃO	
Risco 01:	Não aprovação do Termo de Referência
Probabilidade:	Baixa

Dano	
Impossibilidade da contratação	Paralisação do Softwa Vulnerabilidades
Ação Preventiva	**Re**
Revisar criteriosamente todos os documentos da elaboração do TR	Equipe de Planejamen
Ação de Contingência	**R**
Manutenção do modelo atualmente praticado	Equipe de Planejamen

Risco 02:	Morosidade na conclusão do procedimento licitatório
Probabilidade:	Baixa

Dano	**Im**
Atraso na contratação	Aumento no prazo estima serviços e possibilidade d Gestão de Vulnerabilidad
Ação Preventiva	**Resp**
Acompanhamento minucioso do processo de contratação	Equipe de Planejamento
Ação de Contingência	**Resp**
Sensibilizar a alta gestão para a importância da contratação	Equipe de Planejamento

Risco 03:	Atraso no trâmite dos documentos
Probabilidade:	Baixa

Dano	
Atraso na conclusão do processo licitatório	Aumento no praz serviços
Ação Preventiva	
Agenda de reunião com os dirigentes das Unidades responsáveis	Equipe de Planej
Ação de Contingência	
Monitorar a tramitação dos documentos, buscando sensibilizar as Unidades correspondentes da importância na agilidade da tramitação	Equipe de Planej

Risco 04:	Baixa qualidade dos documentos
Probabilidade:	Baixa

Dano	
Atraso na conclusão do processo licitatório	Aumento no praz serviços
Ação Preventiva	
Revisão dos artefatos por toda a equipe de planejamento da contratação	Equipe de Planej
Buscar o envolvimento dos diversos atores envolvidos no processo para que os documentos alcancem o grau de maturidade necessário para a aprovação nas diversas fases	Equipe de Planej
Ação de Contingência	
Elaboração de novos documentos, com vistas à melhoria na qualidade	Equipe de Planej

Risco 05:	Não conclusão do processo licitatório e/ou assinatura do contrato
Probabilidade:	Baixa

Dano	
Impossibilidade de detecção de novas vulnerabilidades em ativos e aplicativos do TSE	Impossibilidade
Ação Preventiva	
Monitorar criteriosamente a tramitação do processo, inclusive na fase externa	Equipe de Planej
Ação de Contingência	
Sensibilizar a alta gestão do TSE sobre a importância e necessidade dos serviços dispostos na contratação	Equipe de Planej

Risco 06:	Impugnação do processo licitatório
Probabilidade:	Baixa

Dano	
Atraso na contratação	Possibilidade de Vulnerabilidades

Ação Preventiva	
Monitorar criteriosamente a tramitação do processo, inclusive na fase externa	Equipe de Planej
Ação de Contingência	
Ajustar documentação do processo	Equipe de Planej

02 - RISCOS DO PROCESSO DE GESTÃO CONTRATUAL	
Risco 01:	Descumprimento de cláusulas contratuais pela contratada
Probabilidade:	Baixa

Dano	
Indisponibilidade do serviço	Dificuldade na ge
Atraso na entrega do serviço	Impossibilidade d
Ação Preventiva	
Acompanhar a execução do contrato e cobrar da contratada o cumprimento das cláusulas	Equipe de fiscaliz
Ação de Contingência	
Cobrar a contratada quanto à importância do cumprimento das obrigações assumidas	Equipe de fiscaliz
Aplicação de sanções administrativas	Equipe de fiscaliz

Risco 02:	Suspensão dos serviços e/ou revogação do contrato
Probabilidade:	Baixa

Dano	**Impacto**
Indisponibilidade da solução	Impossibilidade de efetuar pagamer
Ação Preventiva	**Responsável**
Gestão eficiente e efetiva do contrato	Equipe de fiscalização do contrato
Ação de Contingência	**Responsável**
Elaborar novo processo de contratação	Equipe de fiscalização do contrato e planejamento contratação

Risco 03:	Contratada se tornar inidônea durante a execução do contrato
Probabilidade:	Baixa

Dano	
Impedimento de continuidade dos serviços	Impossibilidade d
Ação Preventiva	
Acompanhar a execução do contrato e, antes de efetuar pagamentos, verificar a documentação comprobatória	Equipe de fiscaliz
Ação de Contingência	
Suspender a liquidação da fatura	Equipe de fiscaliz

03 - RISCOS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO	
Risco 01:	Falha na entrega dos serviços contratados
Probabilidade:	Baixa

Dano	
Indisponibilidade do serviço	Ocorrência de in
Ação Preventiva	
Acompanhar a execução dos serviços	Equipe de fiscaliz
Ação de Contingência	
Exigir da contratada o restabelecimento urgente do funcionamento da solução assim como da prestação de serviços	Equipe de fiscaliz
Aplicação de sanções administrativas	Equipe de fiscaliz

Risco 02:	Morosidade na disponibilização dos produtos após a contratação
Probabilidade:	Baixa

Dano	
Atraso na implementação e entrega dos serviços	Ocorrência de in
Ação Preventiva	

Acompanhar a execução dos serviços e cobrar da contratada a execução dos serviços	Equipe de fiscaliz
Ação de Contingência	
Exigir da contratada a devida prestação. dos serviços conforme contratado	Equipe de fiscaliz
Aplicação de sanções	Equipe de fiscaliz

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 licenças adquiridas por meio do contrato TSE 128/2022;
4.4.2. O quantitativo adicional previsto neste ETP é devido à expansão do escopo da solução, para que seja capaz de efetuar o gerenc os objetos do tipo "*container*".

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

Não aplicável.

5.1. Os valores para a contratação foram estimados a partir de propostas comerciais recebidas de fornecedores dos produtos do fa
2605096 (Servix) e 2605101 (Global Sec). Foram adotados como base os valores informados no primeiro documento (Servix), por sere
propostas.

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
produto Tenable.sc+ (2.500). O mesmo quantitativo foi considerado para a funcionalidade *Lumin*, pois as regras de licenciam
funcionalidade deve ser licenciada para o total de ativos gerenciados. A quantidade de licenças para a gerência de vuln
inicialmente em 300, embora a quantidade já existente de imagens de *containers* seja de 1200. Tal decisão deveu-se ao fato de
em containers é uma disciplina que será iniciada a partir desse novo licenciamento, e sua utilização pode evidenciar boas
necessário o gerenciamento de um sub-conjunto dos containers existentes (por hipótese, podemos chegar à conclusão de que
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 apar
apresentadas no item 3 deste ETP), e a segunda tabela traz os valores referentes ao licenciamento na modalidade *Tenable One*
as apresentadas no item 4 deste ETP - solução efetivamente escolhida).

5.1.1.3. Esclarecemos que, na modalidade de licenciamento *Tenable One Standard*, a quantidade de licenças pode flutuar entr
produto. Assim, considerando-se que o crescimento previsto desde a última contratação ainda não se materializou, parte das
serão utilizadas para o início do trabalho de gerenciamento de vulnerabilidades de conteiners. Em função disso, as 300 li
disponibilizadas no cenário de licenciamento baseado no *Tenable One.*

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	Diferenc aquisiçã
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 func
adicionais. A segunda tabela também evidencia que a modalidade escolhida, de upgrade do licenciamento atual para o lice
inferior ao custo de uma eventual aquisição inicial do mesmo produto, comprovando que as licenças atualmente detidas pel
abatimento no custo de licenciamento.

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,**
de 36 meses.

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 d
Standard, de forma a acomodar o crescimento do parque de TI do TSE, tanto em termos da quantidade de ativos de rede, quanto da q

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	Diferen aquisiç
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 (lic
solução escolhida, representa 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 não é divisível, visto que trata-se de software de gestão de vulnerabilidades integrado, composto por módulos específico
gerenciamento.

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

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) Não aplicável.

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 ser parceiro do fabricante do software e os serviços deverão ser prestados por colaborado vulnerabilidades.

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 ec

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 deverá ser certificada pelo fabricante do software.

c) Formação de Consórcio:

c.1) Não aplicável. Trata-se de software com console única para gestão de vulnerabilidades.

d) Participação de Cooperativas:

d.1) Não aplicável. A participação de cooperativas no certame não ampliará a competitividade e não proporcionará a ob inviabilidade técnica para o fornecimento do objeto de modo fracionado.

e) Participação de Empresas Estrangeiras:

e.1) Não aplicável, uma vez que, o fabricante do software possui vários representantes (revendas) em todo território nacional.

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 suport

7.3. Particularidades da Contratação:

a) Índice de reajuste:

a.1) O índice de reajuste que deverá ser necessário, em caso de prorrogação de contrato, é o IPCA, conforme o Novo Regime Fi nº 95/2016.

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:

b) Preços diferentes para o mesmo item:

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

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

8.1. Prazo de execução e/ou vigência contratual:

8.1.1. Caso a contratada descumpra total ou parcialmente o objeto contratado, garantida a prévia defesa e o contraditório, ficará sujei
- 8.1.1.1. Advertência;
- 8.1.1.2. Multa;
- 8.1.1.3. Impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 05 (cinco) anos;
  - 8.1.1.3.1. Será aplicada a penalidade descrita no subitem "c)", a contratada que:
    - 8.1.1.3.1.1. ensejar o retardamento da execução do objeto contratado;
    - 8.1.1.3.1.2. falhar ou fraudar na execução do contrato;
      - 8.1.1.3.1.2.1. para efeito de aplicação do disposto no subitem 8.1.1.3.1.2., será considerada falha na execução e nos de inexecução parcial que resultem na rescisão contratual.
- 8.1.1.4. Comportar-se de modo inidôneo;
- 8.1.1.5. Fizer declaração falsa; ou
- 8.1.1.6. cometer fraude fiscal.

8.2. As sanções previstas nos subitens 8.1.1.1. e 8.1.1.3, poderão ser aplicadas à contratada, justamente com as multas convencionais e de dos pagamentos a serem efetuados, após o encerramento do procedimento de penalidade, e quando cabível, sem prejuízo do ressarcimer das demais cominações legais.

8.2.1. 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	1% sobre o valor total contratado
3	1,5 % sobre o valor total da licença não entregue
4	1,5% sobre o valor referente ao serviço de suporte e garantia
5	3% inexecução parcial
6	5% inexecução total

Item	**Descrição**	**Incidência**	**Limite máximo de aplicação**	**Grau**
1	Deixar de cumprir quaisquer das obrigações previstas no Edital e não prevista neste tabela de multas	Por ocorrência	1 (uma) ocorrência	1
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) ocorrências	2
3	Deixar de cumprir o prazo para entrega do objeto.	Por dia	10 (dez) dias corridos	3
4	Deixar de cumprir os prazos previstos, no Termo de Referência, para os tempos de atendimento às solicitações de suporte e atualizações da solução.	Por hora	72 (setenta e duas horas) úteis	4
5	Inexecução parcial	Única		5
6	Inexecução total	Única		6

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 SEGE referência (doc. 1672942), por se tratar de aquisição de licenças de software, bastante semelhante, portanto, à aquisiçã

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 tr às de escravo;*
- *A contratada ou seus dirigentes não devem ter sido condenados por infringir as leis de combate à discrimi trabalho infantil e ao trabalho escravo;*
- *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

9.1.3.1. A contratada não deve possuir inscrição no cadastro "lista suja" de empregadores flagrados explorando trab de escravo;

9.1.4. A comprovação deverá ser efetuada a partir da consulta a lista de empregadores flagrados explorando trabalhado escravo emitida pelo a Secretaria de Trabalho do Ministério do Trabalho e Previdência, no sítio eletrônico (https://www.g br/composicao/orgaos-especificos/secretaria-de-trabalho/inspecao/areas-de-atuacao/cadastro_de_empregadores.pdf).

9.1.5. A contratada ou seus dirigentes não devem ter sido condenados por infringir as leis de combate à discriminação de infantil e ao trabalho escravo;

9.1.6. A comprovação deverá ser efetuada a partir da apresentação de Certidão Judicial de Distribuição ("nada consta" ou **Federal e da justiça comum** para a contratada e seus dirigentes.

9.1.7. Priorização do uso de mídia digital.

9.1.8. As licenças adicionais de uso da ferramenta, a serem fornecidas em decorrência da eventual contratação, devem p meio de arquivo digital que possa ser obtido a partir da internet.

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

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 contratação é primordialmente referente ao licenciamento do produto, e conta apenas com serviços pontuais, como a instalação de conhecimento a respeito das diferenças entre o licenciamento atual (Tenable.sc+ e Tenable One Standard), e demandas ever
9.2.1.2. Acessibilidade para uso de softwares e aplicativos, uma vez que não se trata de software para utilização para o públic de cibersegurança do tribunal, que não tem necessidades de acessibilidade. Adicionalmente, trata-se de solução de mercado mu de acessibilidade, assim como seus competidores.

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 serviç

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

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 CORRENT
10.3.2. Não é possível estimar com certo grau de certeza o tempo (ou prazo) de utilidade do ativo intangível a ser adquirido, COMPL/SAD nº 3/2021 (1764143), 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 **14/09/2023, às 19:17**, 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 **14/09/2023, às 19:18**, 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 **14/09/2023, às 19:19**, 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=2605122&crc=170B1BD3, informando, caso não preenchido, o código verificador **2605122** e o código CRC **170B1BD3**.