TRIBUNAL SUPERIOR ELEITORAL

ESTUDO TÉCNICO PRELIMINAR

CAPÍTULO 1. NECESSIDADE/DEMANDA A SER ATENDIDA

1.1 Indicação da necessidade

Assegurar o funcionamento de equipamentos denominados Firewall, essenciais para a rede de comunicação de dados do TSE.

1.2 Descrição da necessidade

a) Detalhamento da necessidade

a.1) Situações/problemas/dificuldades enfrentadas

A Secretaria de Tecnologia da Informação (STI) do Tribunal Superior Eleitoral (TSE) é responsável por garantir o pleno funcionamento dos sistemas informatizados e assegurar a segurança cibernética da instituição. No contexto atual, essa segurança é diretamente impactada pela infraestrutura de firewall, que desempenha papel fundamental na proteção da rede do TSE contra ameaças cibernéticas, acessos não autorizados e interrupções indesejadas.

Fim de garantia

Atualmente, o TSE possui quatro equipamentos firewall da marca Checkpoint, modelo 23500, adquiridos por meio do **Contrato TSE 83/2019**, vinculado ao processo administrativo nº 2019.00.000002707-2. A garantia desses equipamentos, que incluía atualizações de software e suporte técnico, expirou em 16/12/2024, cinco anos após a emissão do Termo de Recebimento Definitivo (SEI 1220151). Com isso, os equipamentos não contam mais com atualizações de segurança, correções de vulnerabilidades e suporte técnico especializado.

A ausência de atualizações e suporte técnico acarreta riscos operacionais significativos, uma vez que qualquer falha de software ou hardware pode comprometer a segurança da rede do TSE, expondo seus sistemas a possíveis ataques cibernéticos e interrupções. Além disso, sem suporte, a solução de problemas críticos torna-se mais complexa, podendo resultar em períodos de inoperância que impactam diretamente os serviços prestados pelo Tribunal.

Diante desse cenário, a STI precisa garantir a continuidade da proteção cibernética do TSE, minimizando riscos de indisponibilidade e vulnerabilidades na rede. A contratação em questão busca solucionar essa lacuna, assegurando que os mecanismos de segurança permaneçam eficazes e alinhados às melhores práticas de proteção da informação.

Capacidade de processamento

Há de se observar ainda que a capacidade dos firewall do TSE manteve-se a mesma de 2019, haja visto não ter sido realizado nenhum "upgrade" em tais equipamentos, ao passo em que o volume de tráfego na rede de comunicação de dados tem aumentado de forma contínua devido à publicação de novos serviços informatizados a cada ano.

A título de exemplo, no ano de 2019 o alistamento eleitoral e transferência de domicílio eleitoral seriam operações realizadas apenas nos Cartórios Eleitorais. Atualmente tais operações podem ser realizadas diretamente no site de internet do TSE.

Outro grande exemplo diz respeito à implantação, após o ano de 2019, no datacenter do TSE, dos sistemas PJE de 1º e 2º Graus de todos os TRE.

Por fim, citamos a implantação da tecnologia 5G no Brasil em julho de 2022, fazendo com que houvesse maior demanda por tráfego de rede de comunicação de dados.

A medição de tráfego realizada no mês de março de 2025 pela equipe técnica identificou pico de 17,1 Gigabits por segundo (Gbps) de tráfego. No entanto, a capacidade dos Firewall Checkpoint 23500 alcança apenas 11 Gbps quanto habilitadas as funcionalidades de Threat Prevention e Sandblast (vide performance highlights, página 1 do datasheet do equipamento). Para que os firewall continuem funcionando, por vezes torna-se necessário desativar as funções mais avançadas de proteção para que seja dada vazão ao tráfego que flui pelo equipamento.

Para dimensionamento adequado da necessidade, esta equipe de planejamento entende que deverá ser considerada velocidade de 34,2 Gbps como capacidade dos futuros equipamentos, de modo a suportar o aumento de tráfego de dados quando do perído eleitoral.

Registra-se que operar um firewall com até 50% de sua capacidade de processamento é uma prática fundamental para garantir a resiliência e a eficiência da infraestrutura de rede. Manter essa margem de segurança permite que o equipamento absorva picos de tráfego, como os gerados por atividades sazonais ou eventos inesperados, sem comprometer o desempenho ou a estabilidade. Além disso, em cenários de ataques cibernéticos, como DDoS ou tentativas de intrusão, essa capacidade extra é crucial para que o firewall continue processando e filtrando o tráfego de forma eficaz, bloqueando ameaças sem sobrecarga. Por outro lado, operar continuamente próximo à capacidade máxima é um cenário indesejado e pode levar à degradação do serviço, aumento da latência e, em casos extremos, falhas no processamento de regras de segurança, expondo a rede a riscos desnecessários. Portanto, dimensionar firewalls para operar abaixo de sua capacidade total não apenas assegura

maior robustez operacional, mas também fortalece a postura de segurança da organização, alinhando-se a boas práticas de governança e mitigação de riscos.

a.2) Contexto externo

Evolução tecnológica

Mesmo com a evolução de tecnologias de segurança cibernética, os equipamentos firewall permanecem necessários a todas as organizações que possuem uma rede de comunicação de dados.

A evolução tecnológica, no entanto, exige que os firewall possuam cada vez mais capacidade de processamento. A exemplo de outros equipamentos de informática, há lançamentos de novos modelos ao passo em que ocorre a obsolescência de outros.

No caso dos equipamentos utilizados pelo TSE, identificou-se que o fabricante já publicou a data de obsolescência para eles, qual seja: 31 de dezembro de 2025 (vide link). Por outro lado, os fabricantes de firewall já lançaram novas gerações de produtos com capacidades que atendem às novas demandas de tráfego de rede do TSE.

A geração de equipamentos que sucedeu os equipamentos modelo **23500** foi a geração **16200**, conforme é possível observar no site do fabricante (https://www.checkpoint.com/support-services/support-life-cycle-policy/).

Em sequência, a geração **16200** foi substituída pelos equipamentos modelo **19200**.

As imagens abaixo, retiradas do site do fabricante Checkpoint, demonstram essa evolução de gerações:

Legislação

O Acórdão 2387/2024 do Plenário do Tribunal de Contas da União (TCU) refere-se a uma auditoria operacional realizada para avaliar os controles de cibersegurança e de segurança da informação implementados pelas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp). Este acórdão destaca a necessidade de melhorias significativas na gestão de riscos de segurança da informação dentro da administração pública federal.

De acordo com o TCU, as organizações públicas de tecnologia da informação não estão adequadamente protegidas contra ataques cibernéticos, indicando deficiências nos controles de segurança e cibersegurança. Foram utilizados critérioso guia **Controles CIS versão 8** e o **Framework do PPSI.**

O acórdão sugere que essas organizações devem adotar medidas mais eficazes para proteger seus sistemas e dados contra ameaças cibernéticas, alinhando-se com as melhores práticas internacionais de segurança da informação.

Um dos pontos que o TCU pontua diz respeito à implementação e gerenciamento de firewall para proteção dos equipamentos servidores e rede de comunicação de dados dos órgãos da administração pública federal (vide Tabela 1 - Percentual de organizações que implementam as Medidas de Segurança IG1 do citado Acórdão).

Considerando-se a relevância da proteção cibernética necessária aos processos informatizados do TSE, há de ser objeto de atenção a proteção da rede de comunicação de dados por meio da utilização de firewalls eficazes e com manutenção e gestão adequadas.

a.3) Processos anteriores no TSE para atendimento da necessidade

A contratação anterior fora conduzida no TSE por meio do processo 2019.00.000002707-2.

O Estudo Técnico Preliminar então elaborado encontra-se no documento SEI 1105978.

O Edital de Pregão Eletrônico 62/2019 encontra-se no documento SEI 1173551.

O Anexo I - Termo de Referência encontra-se no documento SEI 1173563.

O Contrato 83/2019 está no SEI 1215061.

Consistiu da aquisição de 4 equipamentos firewall Marca Checkpoint, modelo 23500 Security Gateway, a um valor total de **R$ 7.748.000,00**.

Atualizando-se o valor acima pelo IPCA desde a data de assinatura do Contrato TSE 62/2019 (12/12/2019) até 28/02/2025, temos um valor atualizado de **R$ 10.613.482,09** (dez milhões, seiscentos e treze mil quatrocentos e oitenta e dois reais e nove centavos).

A atualização dos valores pelo IPCA foi realizada por meio do site calculoexato.com.br, obtendo-se uma variação do IPCA de 36,9835% entre 12/12/2019 e 19/03/2025.

b) Público alvo a ser atendido

O público-alvo primário desta contratação são os servidores, colaboradores e autoridades do Tribunal Superior Eleitoral (TSE), que dependem de um ambiente de rede seguro e estável para desempenhar suas atividades institucionais. A proteção da infraestrutura de TI é essencial para garantir a integridade, a confidencialidade e a disponibilidade dos sistemas informatizados do Tribunal, permitindo o funcionamento ininterrupto dos serviços prestados.

Indiretamente, eleitores, advogados, partidos políticos e a sociedade em geral também são beneficiados, uma vez que a infraestrutura protegida pelos firewalls viabiliza o correto funcionamento de sistemas críticos, como os de gestão eleitoral, o Processo Judicial Eletrônico (PJe) e demais plataformas institucionais do TSE. O não aten pode comprometer a segurança desses sistemas, aumentando a exposição a vulnerabilidades e colocando em risco a continuidade dos serviços essenciais à democracia e à Justiça Eleitoral.

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

A não mitigação dos riscos relacionados à desatualização de falta de manutenção ou garantia dos firewalls de rede pode resultar em:

- Indisponibilidade de sistemas essenciais (ex.: sistemas eleitorais e administrativos);
- Maior tempo de resposta para resolução de falhas críticas;
- Exposição a ataques cibernéticos, comprometendo dados sensíveis;
- Desgaste na imagem institucional do TSE devido a potenciais interrupções em períodos sensíveis, como eleições.

d) Objetivo(s) estratégico(s) do TSE com os quais necessidade está alinhada, assim como, caso convier, demonstrar a aderência com o Plano Diretor de Informática

A necessidade analisada no presente Estudo Técnico Preliminar está alinhada com o seguinte Objetivo Estratégico:

OE4 – Aperfeiçoar a segurança da informação
Justificativa: A substituição dos switches obsoletos e a contratação de serviços de manutenção estão diretamente relacionadas ao aumento da segurança da informação, pois mitigam vulnerabilidades técnicas que poderiam ser exploradas por invasores. O investimento em infraestrutura atualizada e confiável fortalece as defesas cibernéticas e garante a continuidade das operações em conformidade com boas práticas de governança.

e) Critérios de sustentabilidade para avaliação da necessidade

O presente estudo considera a continuidade de utilização de bens já adquiridos quando isso for possível (quando houver peças de reposição, mesmo que recondicionadas).

Não há regramento específico de sustentabilidade para os equipamentos que são objeto do presente estudo. Os regramentos a serem considerados são genéricos, envolvendo equipamentos de tecnologia da informação.

CAPÍTULO 2. DIFERENTES SOLUÇÕES DE MERCADO QUE POSSAM ATENDER À NECESSIDADE

Para alcance dos objetivos pretendidos neste Estudo Técnico Preliminar, foram analisadas as seguintes soluções:

a) 1ª Solução: Contratação de serviços de expansão de garantia dos equipamentos atuais;

b) 2ª Solução: Substituição dos equipamentos atuais pela geração mais atual; e

c) 3ª Solução: Substituição dos equipamentos atuais por equipamentos de quaisquer fabricantes.

2.1 1ª Solução: Contratação de serviços de expansão de garantia dos equipamentos atuais

a) Descrição sucinta da solução:

Esta solução consiste na avaliação de viabilidade de contratação de suporte técnico e atualizações para os quatro equipamentos firewall Check Point modelo 23500 já instalados no TSE. A medida visa prolongar a vida útil dos dispositivos existentes, garantindo correções de vulnerabilidades e assistência técnica especializada até o fim do período contratado.

Observação:

Esclarecemos que a Solução 1 não se mostra viável, haja vista que o mercado comercializa extensão de garantia de firewalls por anualidade, não sendo firmada por fração inferior a um ano.

Considerando-se que resta menos de um ano até que os Firewall CheckPoint 23500 cheguem ao fim de vida decretado pelo fabricante, não é possível levar a efeito a contratação por 12 meses.

No entanto, esta equipe de planejamento entendeu por relevante ofertar ao adminitrador a visão do custo anual da extensão de garantia.

Tais valores permitem balizamento para que se dimensione se é mais caro ou mais barato adquirir novos equipamentos, em comparação com o custo de extensão de garantia de equipamentos de mesma natureza.

b) Indicação resumida dos serviços e materiais que compõem a solução com as respectivas quantidades

Item	Quantidade	Justificativa da quantidade
Contratação de garantia estendida, com suporte 24x7 e com direito de atualização corretiva e evolutiva dos softwares de Firewall Check Point, modelo 23500.	4	Consiste da quantidade atualmente necessária e suficiente para que o TSE gerencie a segmentação de sua rede local e rede WAN.

c) Potenciais fornecedores e/ou fabricantes

Dentre os principais fornecedores, aqueles mais atuantes em licitações são:

- AX4B SISTEMAS DE INFORMATICA LTDA
- CG ONE (COMPUGRAF SEGURANÇA DIGITAL)
- CINCO TI
- CONTACTA SEGURANCA EM CONECTIVIDADE LTDA
- CONVERSYS IT SOLUTIONS COMERCIO
- GLOBAL IP TECNOLOGIA DA INFORMACAO LDTA
- ISH TECNOLOGIA S.A.
- L8 GROUP S.A.
- MULTIDATA LTDA
- NETSCIENCE TECNOLOGIA INDUSTRIA DE EQUIPAMENTOS DE COMUNICAÇAO LTDA
- NTSEC SOLUCOES EM TELEINFORMATICA LTDA
- ORBITEL TELECOMUNICACOES E INFORMÁTICA LTDA
- RL2 INFORMATICA LTDA
- SCANSEC TECNOLOGIA LTDA
- SECURITY4IT
- SOLO NETWORK BRASIL S.A.
- TELEFONICA BRASIL S.A.

d) Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos

d.1) **TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO - SANTA CATARINA**

Pregão 9665/2023 - UASG 80013

Ata de Registro de Preços nº 01/2023 - https://pncp.gov.br/app/atas/00509968000148/2023/1136/1

Estudo Técnico Preliminar (link)

A contratação realizada pelo TRT12 consistiu da extensão da garantia de firewalls já implantados nos Tribunais que participaram da formação da ARP TRT12 nº 01/2023.

O pregão fora adjudicado à empresa NTSEC SOLUCOES EM TELEINFORMATICA LTDA.

Particularmente, o item 1 da ARP consiste da extensão da garantia, por 24 meses, para o equipamento Firewall de mesma marca e modelo que o TSE possui (Check Point 23500).

A extensão de garantia por 24 meses custou à época (a sessão pública do Pregão 9665/2023 ocorreu em 17 de agosto de 2023), o valor de R$ 720.000,00.

Atualizando-se esse valor pelo IPCA entre 17/08/2023 e 19/03/2025 or meio do portal Cálculo Exato, temos um valor atualizado de **R$ 777.993,84** para uma extensão de garantia por 24 meses.

Depreende-se das informações acima que a extensão de garantia custou ao TRT12 o valor de **R$ 388.996,92** por equipamento-ano, correspondendo a um valor de **R$ 1.555.987,68 para quatro firewalls a cada ano.**

d.2) **TRIBUNAL REGIONAL ELEITORAL DO PARÁ**

Pregão Eletrônico N° 90045/2024 - UASG 70004

https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-1?compra=07000405900452024

A contratação realizada pelo TRE-PA consistiu da extensão de garantia para dois firewalls do fabricante Palo Alto Networks, modelo PA-3260.

O valor obtido pelo TRE-PA para a contratação da extensão de garantia por 36 meses para os dois equipamentos foi de R$ 2.466.000,00.

A proposta vencedora foi apresentada ao TRE-PA pela empresa Approach Tecnologia, em 20/08/2024. Realizando-se a atualização de preços pelo IPCA, temos o valor de R$ 2.549.926,95, aplicando-se uma variação do IPCA no percentual de 3,4034% entre 20/08/2024 e 19/03/2025.

Depreende-se das informações acima que a extensão de garantia custou ao TRE-PA o valor de **R$ 424.987,82** por equipamento-ano, correspondendo a um valor de **R$ 1.699.951,28 para quatro firewalls a cada ano.**

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

Não se aplica.

f) Requisitos de tecnologia da informação presentes na solução

Considerando-se que a solução ora pretendida consiste de uma solução de tecnologia da informação, passaremos a analisar seu contexto em relação a Políticas, Modelos ou Padrões de Governo a serem observados.

A análise da aderência da Solução 1 aos padrões e políticas de governo envolve verificar sua conformidade com as normativas aplicáveis, boas práticas de tecnologia da informação e segurança cibernética, além das diretrizes específicas do Tribunal Superior Eleitoral (TSE). A seguir, são destacados os principais aspectos:

1. Conformidade com Normativas de Segurança da Informação

Política de Segurança da Informação (PGSI):

O TSE deve seguir uma Política Geral de Segurança da Informação que estabelece requisitos mínimos para proteção dos ativos de TI. A manutenção de equipamentos sem suporte técnico adequado pode violar esses requisitos, especialmente no que se refere à atualização de patches de segurança e mitigação de vulnerabilidades.

Análise: A contratação de serviços de expansão de garantia garante ao menos temporariamente o cumprimento dessas exigências, pois possibilita a correção de vulnerabilidades conhecidas e o suporte técnico necessário.

Normas ABNT NBR ISO/IEC 27001 e 27002:

Essas normas internacionais estabelecem um framework para gestão da segurança da informação, recomendando a adoção de controles técnicos atualizados e monitoramento constante.
Análise: Embora a solução preserve o funcionamento dos equipamentos existentes, ela não resolve o problema estrutural relacionado ao fim de vida dos dispositivos, o que pode comprometer a conformidade com essas normas em médio prazo.

2. Diretrizes de Governança de TI

Instrução Normativa SLTI nº 4/2020 – Guia de Boas Práticas de Governança de TI:

Esta instrução recomenda que órgãos públicos priorizem soluções que minimizem riscos operacionais e financeiros, considerando a relação custo-benefício.

Análise: A expansão de garantia apresenta menor custo inicial, mas não elimina os riscos associados ao fim de vida dos equipamentos. Assim, a solução pode ser vista como insuficiente para garantir governança de longo prazo.

3. Aspectos Relacionados à Segurança Cibernética

Estratégia Nacional de Segurança Cibernética (E-Ciber):

A E-Ciber recomenda a adoção de tecnologias atualizadas e resilientes para proteger infraestruturas críticas contra ameaças cibernéticas.

Análise: A manutenção de equipamentos próximos ao fim de vida, mesmo com suporte temporário, representa um risco significativo para a segurança cibernética do TSE, especialmente considerando a evolução das ameaças digitais.

Política de Gestão de Riscos:

O TSE deve implementar medidas para identificar, avaliar e mitigar riscos relacionados à segurança da informação.

Análise: Embora a expansão de garantia reduza alguns riscos imediatos, ela não elimina os riscos associados à obsolescência tecnológica e ao fim de vida dos equipamentos, o que pode comprometer a eficácia da gestão de riscos cibernéticos.

4. Padrões de Sustentabilidade e Eficiência

Agenda de Desenvolvimento Sustentável (ODS):

O Governo Federal orienta os órgãos públicos a adotarem práticas sustentáveis, incluindo o uso eficiente de recursos tecnológicos.

Análise: A Solução 1, ao prolongar o uso de equipamentos existentes, pode ser vista como uma prática de economia de recursos. No entanto, ela não contribui totalmente para a eficiência tecnológica a longo prazo, uma vez que os equipamentos continuarão a ser obsoletos, sobretudo com a previsão de fim de vida prevista pelo fabricante para 31 de dezembro de 2025.

Conclusão: Adesão aos Padrões e Políticas

A Solução 1 apresenta aderência parcial aos padrões e políticas de governo. Ela atende a requisitos de curto prazo, como segurança jurídica, economicidade e mitigação de riscos imediatos. No entanto, falha em alinhar-se às diretrizes de modernização tecnológica, sustentabilidade e segurança cibernética de longo prazo. Portanto, embora seja viável como medida temporária, esta solução não deve ser considerada definitiva, devendo ser acompanhada por um plano estratégico para substituição dos equipamentos antes do fim de vida anunciado pelo fabricante.

g) Custos estimados

Considerando-se as contratações efetivadas pelo TRT12 e pelo TRE-PA, temos o seguinte valor médio estimado para a extensão de garantia de um firewall:

Órgão	Descrição	Valor unitário
TRT12	d.1) Extensão da garantia de firewalls já implantados (por firewall)	R$ 388.996,92
TRE-PA	d.2) Extensão da garantia de firewalls já implantados (por firewall)	R$ 424.987,82
	Valor médio:	R$ 406.992,37

Multiplicando-se pelo quantitativo de firewalls a serem manutenidos, temos o seguinte valor total estimado para solução 1:

Item	Descrição	Quantidade	Valor unitário	Valor Total anual	Valor total 60 meses
1	Contratação de garantia estendida, com suporte 24x7 e com direito de atualização corretiva e evolutiva dos softwares de Firewall Check Point, modelo 23500, por 60 meses**(*)**.	4	R$ 406.992,37	R$ 1.627.969,48	R$ 8.139.847,40

(*) em que pese não ser viável a contratação da solução 1 haja vista o intercurso inferior a um ano até que o equipamento entre em fim de vida, a equipe de planejamento optou por manter a estimativa de custo de eventual extensão de garantia por 60 meses a fim de prover ao administrador uma visão comparativa de custos entre esta solução e as demais.

h) Vantagens e desvantagens

Solução 1: Contratação de serviços de expansão de garantia dos equipamentos atuais

Vantagens:

- **Continuidade operacional imediata**: A solução mantém os equipamentos já instalados e em funcionamento, sem necessidade de interrupções para substituição.
- **Custo inicial reduzido**: A expansão de garantia geralmente apresenta um custo inicial inferior à aquisição de novos equipamentos, permitindo uma gestão orçamentária mais equilibrada no curto prazo.
- **Familiaridade técnica**: A equipe técnica do TSE já está familiarizada com a operação e manutenção dos equipamentos Check Point modelo 23500, reduzindo o tempo de adaptação e treinamento.
- **Suporte técnico especializado**: A contratação de suporte e atualizações garante que as vulnerabilidades sejam corrigidas e que problemas técnicos sejam resolvidos por profissionais qualificados.

Desvantagens:

- **Inviabilidade técnica de implementação**: a contratação de garantia de um firewall, é prática de mercado a comercialização desta por um mínimo de 12 meses, não sendo praticada a venda por oito meses, como seria o caso concreto da presente contratação.
- **Fim de vida próximo**: O fabricante anunciou que o modelo 23500 terá fim de vida em 31/12/2025, o que significa que, mesmo com a expansão de garantia, a solução é temporária e não resolve o problema estrutural.
- **Obsolescência tecnológica**: Equipamentos próximos ao fim de vida podem não acompanhar as demandas crescentes de segurança cibernética, tornando-os menos eficazes contra ameaças modernas.
- **Risco de descontinuidade**: Após o fim de vida, o fabricante pode cessar completamente o suporte técnico e as atualizações, expondo o TSE a riscos ainda maiores no médio prazo.

2.2 2ª Solução

a) Descrição sucinta da solução

Propõe-se a substituição dos firewalls modelo 23500 por equipamentos mais modernos do mesmo fabricante, aproveitando a compatibilidade com a infraestrutura existente e assegurando tecnologia atualizada, desempenho superior e suporte técnico de longo prazo. Assim, esta solução se caracteriza

como sendo Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.

b) Indicação resumida dos serviços e materiais que compõem a solução com as respectivas quantidades

Item	Quantidade	Justificativa da quantidade
Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	4	Consiste da quantidade atualmente necessária e suficiente para que o TSE gerencie a segmentação de sua rede local e rede WAN. A definição do modelo 19200 ou superior dá-se pelo fato de ser esta a geração mais atual dos equipamentos 23500, conforme demonstrado no item 1.2.a.2 deste ETP.

c) Potenciais fornecedores e/ou fabricantes

Dentre os principais fornecedores, aqueles mais atuantes em licitações são:

- AX4B SISTEMAS DE INFORMATICA LTDA
- CG ONE (COMPUGRAF SEGURANÇA DIGITAL)
- CINCO TI
- CONTACTA SEGURANCA EM CONECTIVIDADE LTDA
- CONVERSYS IT SOLUTIONS COMERCIO
- GLOBAL IP TECNOLOGIA DA INFORMACAO LDTA
- ISH TECNOLOGIA S.A.
- L8 GROUP S.A.
- MULTIDATA LTDA
- NETSCIENCE TECNOLOGIA INDUSTRIA DE EQUIPAMENTOS DE COMUNICAÇAO LTDA
- NTSEC SOLUCOES EM TELEINFORMATICA LTDA
- ORBITEL TELECOMUNICACOES E INFORMÁTICA LTDA
- RL2 INFORMATICA LTDA
- SCANSEC TECNOLOGIA LTDA
- SECURITY4IT
- SOLO NETWORK BRASIL S.A.
- TELEFONICA BRASIL S.A.

d) Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos

d.1) **TRIBUNAL SUPERIOR ELEITORAL**

Contrato TSE 83/2019 - SEI 1211870

Por meio do Contrato TSE 83/2019 foram adquiridos quatro firewalls Check Point Modelo 23500, a um custo unitário de R$ 1.937.000,00 (o valor total do contrato foi de R$ 7.748.000,00).

Atualizando-se o valor acima pelo IPCA desde a data de assinatura do Contrato TSE 62/2019 (12/12/2019) até 28/02/2025, temos um valor atualizado de **R$ 10.613.482,09** (dez milhões, seiscentos e treze mil quatrocentos e oitenta e dois reais e nove centavos), correspondendo a um valor unitário ATUALIZADO, por firewall Check Point Modelo 23500, de **R$ 2.653.370,52, com garantia de 60 meses**.

A atualização dos valores pelo IPCA foi realizada por meio do site calculoexato.com.br, obtendo-se uma variação do IPCA de 36,9835% entre 12/12/2019 e 19/03/2025.

d.2) **TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO**

Edital nº 90070/2024 - UASG 070017

Contrato 115/2024 - CONTACTA SEGURANÇA EM CONECTIVIDADE LTDA

https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-1?compra=07001705900702024

Por meio do Pregão 90070/2024 o TRE-RJ licitou 10 Firewalls Check Point Modelo 1535 e 2 Firewalls modelo 9800. Destinam-se a substituir modelos de Firewall que estão em processo de Fim de vida, os modelos 1430 e 15600, respectivamente.

Apesar de consistirem de modelos inferiores aos do TSE, a contratação em questão presta-se a ilustrar que a opção de contratação com indicação de marca é praticada por órgãos de renome.

d.3) **SUPERIOR TRIBUNAL DE JUSTIÇA**

Edital nº 00120/2023 - UASG 050001

https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/landing?destino=acompanhamento-compra&compra=05000105001202023

Consistiu de pregão onde o STJ indicou que os equipamentos existentes deveriam ser substituídos por equipamentos do **mesmo fabricante.**

No Edital de Licitação, o STJ fez constar as justificativas para indicação de marca. Vejamos:

> 4.10.0 STJ dispõe atualmente de equipamentos da fabricante Foftinet, e a equipe de planejamento desta contratação considera que se deve manter tal fabricante para o melhor benefício de todos os usuários dos serviços do Tribunal, considerando alguns aspectos negativos e desafios para uma organização, citados abaixo, em caso de substituição:
>
> a. Curva de aprendizado: Cada fabricante de firewall possui sua própria interface de gerenciamento, terminologia, configurações e recursos específicos. Ao trocar de fabricante, a equipe de TI e segurança precisará se adaptar a uma nova plataforma e aprender a trabalhar com ela. Isso pode exigir treinamento adicional e tempo para se familiarizar com a nova
> solução. Cabe ressaltar que na recente contratação de um serviço de SOC por esta Corte, por meio do Processo STJ n. 022086/2022, há a exigência de profissional especialista com
> certificados específicos nas soluções do fabricante Fortinet. A troca do fabricante da solução implicaria na troca dos profissionais alocados ou treinamento destes com a necessidade de obtenção de novas certificações para atender as obrigações contratuais, bem como alterações no referido contrato.
>
> b. Integração com o ambiente existente: A migração para uma nova solução de firewall é complexa especialmente em organizações que já possuem uma infraestrutura implantada e vários sistemas interligados. A integração da nova solução com o ambiente existente pode requerer esforço significativo e cuidadosa coordenação para garantir que todos os serviços e aplicativos continuem funcionando sem problemas.
>
> c. Perda de configurações personalizadas: As configurações e regras personalizadas feitas na solução anterior podem não ser diretamente transferíveis para a nova plataforma, como
> configurações de SD-WAN, Internet Database Services, inspeção de tráfego de dados em profundidade (deep inspection). Isso significa que a equipe de segurança precisará recriar
> todas as configurações personalizadas na nova solução, o que pode ser um processo demorado e propenso a erros, e exigir complementações com outras soluções para que seja possível obter o mesmo resultado.
>
> d. Possíveis interru2ções de serviço: Durante o processo de migração, pode haver interrupções temporárias nos serviços de rede e comunicação. Se a transição não for bem planejada e executada, isso pode levar a períodos de tempo de inatividade não planejados, o que pode afetar negativamente as operações da organização.
> e. Risco de inconsistências de segurança: Mudar para uma nova solução de firewall pode criar brechas de segurança temporárias e até definitivas se as regras e configurações não forem adequadamente replicadas na nova plataforma ou pela inexistência de recursos na nova solução. Isso pode deixar a rede vulnerável a ataques ou ameaças durante o período de transição.

O modelo ofertado pela empresa NCT INFORMATICA LTDA, foi o FortiGate-2600F. Consiste de modelo inferior ao utilizado pelo TSE. Apesar de consistirem de modelos inferiores aos do TSE, a contratação em questão presta-se a ilustrar que a opção de contratação com indicação de marca é praticada por órgãos de renome.

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

Não se aplica.

f) Requisitos de tecnologia da informação presentes na solução

Considerando-se que a solução ora pretendida consiste de uma solução de tecnologia da informação, passaremos a analisar seu contexto em relação a Políticas, Modelos ou Padrões de Governo a serem observados.

A análise da aderência da Solução 2 aos padrões e políticas de governo envolve verificar sua conformidade com normativas aplicáveis, boas práticas de segurança cibernética, diretrizes de governança de TI e requisitos técnicos específicos. A seguir, são destacados os principais aspectos:

1. Conformidade com Normativas de Segurança da Informação

Política de Segurança da Informação (PGSI):

O TSE deve seguir uma Política Geral de Segurança da Informação que estabelece requisitos mínimos para proteção dos ativos de TI, incluindo a adoção de tecnologias avançadas de prevenção contra ameaças.

Análise: A substituição por equipamentos mais modernos da mesma marca garante funcionalidades avançadas de threat prevention , como Application Control , IPS , URL Filtering , Anti-Bot , Anti-Virus , Anti-Spam , e DNS Security , atendem plenamente às exigências de segurança da informação.

Normas ABNT NBR ISO/IEC 27001 e 27002:

Essas normas internacionais recomendam controles técnicos atualizados, monitoramento constante e capacidade de resposta a incidentes.

Análise: A nova geração de firewalls Check Point oferece suporte às melhores práticas de gestão de riscos e controles de segurança, alinhando-se diretamente às normas ISO/IEC 27001 e 27002.

2. Diretrizes de Governança de TI

Estratégia de Modernização Tecnológica do Governo Federal:

O Governo Federal incentiva a modernização tecnológica para garantir eficiência, segurança e sustentabilidade dos sistemas públicos.

Análise: A Solução 2 está totalmente alinhada à estratégia de modernização tecnológica, pois

substitui equipamentos obsoletos por dispositivos mais avançados, garantindo desempenho superior e maior resiliência.

Instrução Normativa SLTI nº 4/2020 – Guia de Boas Práticas de Governança de TI:

Esta instrução recomenda que órgãos públicos priorizem soluções que minimizem riscos operacionais e financeiros, considerando a relação custo-benefício.

Análise: Embora o custo inicial seja elevado, a solução reduz significativamente os riscos operacionais e financeiros a longo prazo, alinhando-se às boas práticas de governança, sobretudo ao consideramos que os equipamentos são fornecidos com garantia de cinco anos

3. Políticas de Compras Públicas

Lei nº 14.133/2021 (Nova Lei de Licitações):

A nova legislação enfatiza a necessidade de planejamento estratégico nas contratações públicas, considerando critérios como economicidade, sustentabilidade e segurança jurídica.

Análise: A substituição dos equipamentos atuais por modelos mais modernos é uma solução estratégica que atende aos princípios de economicidade (redução de riscos futuros) e sustentabilidade (uso eficiente de recursos tecnológicos).

Gestão de Ativos de TI - Portaria 477/2022:

A Portaria 477/2022 prevê a substituição gradual de equipamentos obsoletos, alinhando-se às necessidades institucionais e às melhores práticas de mercado.

Análise: A Solução 2 está plenamente alinhada, pois promove a renovação tecnológica necessária para garantir a continuidade e eficácia dos serviços prestados pelo Tribunal.

4. Aspectos Relacionados à Segurança Cibernética

Estratégia Nacional de Segurança Cibernética (E-Ciber):

A E-Ciber recomenda a adoção de tecnologias atualizadas e resilientes para proteger infraestruturas críticas contra ameaças cibernéticas.

Análise: A nova geração de firewalls Check Point oferece funcionalidades avançadas de prevenção contra ameaças e capacidade de inspeção de 34Gbps com as funções de threat prevention ativadas, atendendo plenamente às exigências da E-Ciber.

Gestão de Riscos :

O TSE deve implementar medidas para identificar, avaliar e mitigar riscos relacionados à segurança da informação.

Análise: A substituição dos equipamentos elimina os riscos associados à obsolescência tecnológica e ao fim de vida dos dispositivos, mitigando riscos.

5. Requisitos Técnicos Específicos

Funcionalidades de Threat Prevention

Os requisitos técnicos especificados incluem:

- Application Control.
- IPS (Intrusion Prevention System)
- URL Filtering
- Anti-Bot
- Anti-Virus
- Anti-Spam
- DNS Security

Capacidade de Inspeção de 34Gbps com funções de Threat Prevention ativadas : Os novos modelos Check Point atendem a este requisito, garantindo alto desempenho mesmo com todas as funcionalidades habilitadas.

Certificações Ambientais e de Segurança

- Certificações de segurança : CB IEC 62368-1 e UL62368-1
- Certificações de emissões : CE e FCC
- Certificações ambientais : ROHS e ISO 14001

Capacidade de Gestão de Conexões de

- Pelo menos 20 milhões de conexões simultâneas;
- Recepçao de até 1 milhão de novas conexões por segundo.

6. Padrões de Sustentabilidade e Eficiência

Agenda de Desenvolvimento Sustentável (ODS):

O Governo Federal orienta os órgãos públicos a adotarem práticas sustentáveis, incluindo o uso eficiente de recursos tecnológicos.

Análise: A Solução 2 contribui para a eficiência tecnológica, pois substitui equipamentos obsoletos por dispositivos modernos e certificados ambientalmente, alinhando-se à Agenda de Sustentabilidade.

7. Conclusão: Adesão aos Padrões e Políticas

A Solução 2 apresenta alta aderência aos padrões e políticas de governo. Ela atende plenamente aos requisitos técnicos especificados, incluindo funcionalidades avançadas de threat prevention , capacidade de inspeção e gestão de conexões, além de certificações ambientais e de segurança. Além disso, está alinhada às diretrizes de modernização tecnológica, governança de TI e segurança cibernética, representando uma solução estratégica e sustentável para garantir a continuidade da segurança da rede do TSE.

Portanto, esta solução é altamente recomendada para atender às necessidades institucionais, mitigar riscos e assegurar conformidade com os padrões já adotados.

g) Custos estimados para fins de análise comparativa

Considerando-se o Pregão Eletrônico 90906/2024, realizado pelo SERPRO (UASG 803080), é possível obter-se o preço dos firewalls Checkpoint 19200. A documentação desse pregão está disponível em https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-2?compra=80308005909062024

Os Firewall Check Point 19200 foram ofertados pela empresa NTSec, a qual sagrou-se vencedora do Pregão SERPRO 90906/2024. adjucatária dos itens desse pregão.

O item 1 do Pregão do SERPRO consistiu de oito pares (clusters) de Firewalls CheckPoint 19200, com garantia de 60 meses.

Cada par de Firewall Check Point custou R$ 3.173.837,00. Assim, cada Firewall Check Point 19200, com garantia de 60 meses, custou R$ 1.586.918,50.

Depreende-se das informações acima que o custo estimado para a Solução 2 seria de R$ 6.347.674,00.

Item	Descrição	Quantidade	Valor unitário	Valor Total
1	Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	4	R$ 1.586.918,50	R$ 6.347.674,00

h) Vantagens e desvantagens

Solução 2: Substituição dos equipamentos atuais pela geração mais atual (manter o mesmo fabricante: Check Point)

Vantagens:

- **Compatibilidade e integração**: Os novos equipamentos da mesma marca garantem maior compatibilidade com a infraestrutura existente, facilitando a migração e minimizando impactos operacionais.
- **Tecnologia atualizada**: A adoção de equipamentos da geração mais recente proporciona maior eficiência, desempenho e capacidade de resposta às ameaças cibernéticas emergentes.
- **Suporte técnico prolongado**: Novos equipamentos virão com garantia e suporte técnico estendidos, assegurando proteção contínua por um período mais longo.
- **Facilidade de transiçã**o: A equipe técnica já possui experiência com soluções Check Point, reduzindo o tempo necessário para adaptação e treinamento.

Desvantagens:

- **Alto custo inicial**: A aquisição de novos equipamentos pode representar um investimento inicial significativo quando comparado ao custo da contratação de garantia.
- **Tempo de implementação**: A substituição dos equipamentos exigirá planejamento detalhado e possíveis interrupções temporárias durante a instalação e configuração.

2.3 3ª Solução: Substituição dos equipamentos atuais por equipamentos de quaisquer fabricantes.

a) Descrição sucinta da solução

Propõe-se a substituição dos firewalls modelo 23500 por equipamentos de qualquer fabricante. Assim, esta solução se caracteriza como sendo Aquisição de Appliance de firewall NGFW com Threat Prevention, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (NGFW e threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.

b) Indicação resumida dos serviços e materiais que compõem a solução com as respectivas quantidades

Item	Descrição	Quantidade	Justificativa da quantidade

Item	Descrição	Quantidade	Justificativa da quantidade
1	Appliance de firewall NGFW com Threat Prevention, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (NGFW e threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	4	Consiste da quantidade atualmente necessária e suficiente para que o TSE gerencie a segmentação de sua rede local e rede WAN.
2	Migração das configurações dos firewalls atuais para os novos equipamentos	4	As configurações de cada um dos quatro firewalls existentes no TSE terão que ser migradas para os firewall do novo fabricante.
3	Serviço gerenciado mensal	18 meses	Com a adoção de uma tecnologia desconhecida pelas equipes do TSE, haverá necessidade de que sejam contratados serviços de gerenciamento dos equipamentos, para que realizem operação assistida, e resposta a incidentes de segurança envolvendo os equipamentos, durante um período que ultrapasse o final das eleições gerais de 2026.
4	Treinamento na nova tecnologia	1	Considera-se, para esse quantitativo a necessidade de realização de uma turma de treinamento para as equipes da COINF que realizam gestão do Firewall (SESOP e SDCiber)

c) Potenciais fornecedores e/ou fabricantes

- 2R DATATEL TELEINFORMATICA LTDA
- ADD VALUE PARTICIPACOES, COMERCIO E SERVIÇOS DE INFORMÁTICA LTDA
- APPROACH TECNOLOGIA LTDA
- BLUE EYE SOLUCOES EM TECNOLOGIA LTDA
- CG ONE (COMPUGRAF SEGURANÇA DIGITAL
- CINCO TI
- CLARO S.A.
- CONTACTA SEGURANCA EM CONECTIVIDADE LTDA
- CONTACTA
- CONVERSYS IT SOLUTIONS COMERCIO
- FAST HELP INFORMATICA LTDA
- FIRE ANT TECNOLOGIA DE REDE DE COMPUTADORES LTDA
- GHF TECNOLOGIA E COMUNICACAO LTDA
- GLOBAL IP TECNOLOGIA DA INFORMACAO LDTA
- ISH TECNOLOGIA S.A.
- L8 GROUP S.A.
- MGAX4B INOVACOES EM TECNOLOGIA LTDA
- MULTIDATA LTDA
- NETSCIENCE TECNOLOGIA INDUSTRIA DE EQUIPAMENTOS DE COMUNICAÇAO LTDA
- NIVA TECNOLOGIA DA INFORMACAO LTDA
- NORDEN TECNOLOGIA LTDA
- NTSEC SOLUCOES EM TELEINFORMATICA LTDA
- ORBITEL TELECOMUNICACOES E INFORMÁTICA LTDA
- RL2 INFORMATICA LTDA
- SERVIX INFORMATICA LTDA

- SOLO NETWORK BRASIL S.A.
- TELEFONICA BRASIL S.A.
- TELTEC SOLUTIONS LTDA

d) Órgãos públicos e/ou entidades que tenham adotado solução similar e análise dos respectivos contratos

d.1) **TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO**

Pregão Eletrônico N° 90014/2024 - UASG 90029

https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-1?compra=09002905900142024

O Pregão Eletrônico consistiu da aquisição de firewalls para atender a necessidades do TRF3 e de outros Tribunais partícipes a exemplo do TRF1, TRF2 e TRF4.

Teve valor final homologado em R$ 33.155.693,83.

A empresa adjudicada foi a NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA, a qual ofertou firewalls **Check Point modelo 19100**.

Apesar de consistirem de modelos inferiores aos do TSE, a contratação em questão presta-se a ilustrar que a opção de contratação com indicação de marca é praticada por órgãos de renome.

d.2) **SERPRO - REGIONAL SÃO PAULO**

Pregão Eletrônico 90906/2024 - UASG 803080

https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-2?compra=80308005909062024

O pregão eletrônico consistiu de contratação de soluções de proteção de redes para os Clientes e Data Centers do Serpro e para Segmentação de suas Redes Locais internas, com garantia técnica, compostas por clusters de firewalls NGFW (Next-Generation Firewall, ou Firewall de Próxima Geração).
A competição estabelecida pelo SERPRO foi aberta, com participação, pelo menos, dos fabricantes Fortinet e CheckPoint.
Assevera-se a restrição "pelo menos" no parágrafo acima, pelo fato de que, dentre as sete licitantes, apenas duas indicaram marca e modelo dos equipamentos ofertados. São elas: NCT Informática (ofertou equipamento Fortinet) e NTSec Soluções (Ofertou Check Point, sagrando-se vencedora).

O item 1 do Pregão do SERPRO consistiu de oito pares (clusters) de Firewalls CheckPoint 19200, com garantia de 60 meses.
Cada par de Firewall Check Point custou R$ 3.173.837,00.

Depreende-se das informações acima cada Firewall Check Point 19200 com garantia de 60 meses custou R$ 1.586.918,50

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

Não se aplica.

f) Requisitos de tecnologia da informação presentes na solução

Considerando-se que a solução ora pretendida consiste de uma solução de tecnologia da informação, passaremos a analisar seu contexto em relação a Políticas, Modelos ou Padrões de Governo a serem observados.

A análise da aderência da Solução 3 aos padrões e políticas de governo envolve verificar sua conformidade com normativas aplicáveis, boas práticas de segurança cibernética, diretrizes de governança de TI e requisitos técnicos específicos. A seguir, são destacados os principais aspectos:

1. Conformidade com Normativas de Segurança da Informação

Política de Segurança da Informação (PGSI):

O TSE deve seguir uma Política Geral de Segurança da Informação que estabelece requisitos mínimos para proteção dos ativos de TI, incluindo a adoção de tecnologias avançadas de prevenção contra ameaças.

Análise: A substituição por equipamentos de diferentes fabricantes pode atender às exigências de segurança da informação, desde que os novos dispositivos ofereçam funcionalidades avançadas de threat prevention , como Application Control , IPS , URL Filtering , Anti-Bot , Anti-Virus , Anti-Spam , e DNS Security . Entretanto, a diversificação de fornecedores pode introduzir inconsistências na gestão de segurança.

Normas ABNT NBR ISO/IEC 27001 e 27002:

Essas normas internacionais recomendam controles técnicos atualizados, monitoramento constante e capacidade de resposta a incidentes.

Análise: A solução é viável se os fabricantes selecionados oferecerem produtos certificados e compatíveis com as melhores práticas de gestão de riscos e controles de segurança. No entanto, a integração de diferentes tecnologias pode demandar maior esforço para garantir conformidade.

2. Diretrizes de Governança de TI

Estratégia de Modernização Tecnológica do Governo Federal:

O Governo Federal incentiva a modernização tecnológica para garantir eficiência, segurança e sustentabilidade dos sistemas públicos.

Análise: A Solução 3 está alinhada à estratégia de modernização tecnológica, pois substitui equipamentos obsoletos por dispositivos mais avançados. A diversificação de fornecedores também promove flexibilidade e inovação.

Instrução Normativa SLTI nº 4/2020 – Guia de Boas Práticas de Governança de TI:

Esta instrução recomenda que órgãos públicos priorizem soluções que minimizem riscos operacionais e financeiros, considerando a relação custo-benefício.

Análise: A diversificação de fornecedores pode reduzir a dependência de um único fabricante, mitigando riscos financeiros e comerciais. No entanto, a complexidade de integração e adaptação pode aumentar os custos iniciais.

3. Políticas de Compras Públicas

Lei nº 14.133/2021 (Nova Lei de Licitações):

A nova legislação enfatiza a necessidade de planejamento estratégico nas contratações públicas, considerando critérios como economicidade, sustentabilidade e segurança jurídica.

Análise: A abertura para diferentes fabricantes permite maior competitividade e melhores condições contratuais, alinhando-se ao princípio de economicidade. No entanto, a diversificação exige planejamento detalhado para evitar inconsistências e garantir segurança jurídica.

Gestão de Ativos de TI - Portaria 477/2022:

A Portaria 477/2022 prevê a substituição gradual de equipamentos obsoletos, alinhando-se às necessidades institucionais e às melhores práticas de mercado.

Análise: A Solução 3 está plenamente alinhada, pois promove a renovação tecnológica necessária para garantir a continuidade e eficácia dos serviços prestados pelo Tribunal.

4. Aspectos Relacionados à Segurança Cibernética

Estratégia Nacional de Segurança Cibernética (E-Ciber):

A E-Ciber recomenda a adoção de tecnologias atualizadas e resilientes para proteger infraestruturas críticas contra ameaças cibernéticas.

Análise: A solução atende à E-Ciber se os novos equipamentos forem certificados e incorporarem funcionalidades avançadas de threat prevention . A diversificação de fornecedores pode, no entanto, introduzir desafios na padronização de políticas de segurança.

Política de Gestão de Riscos (PGRC):

O TSE deve implementar medidas para identificar, avaliar e mitigar riscos relacionados à segurança da informação.

Análise: A substituição dos equipamentos elimina os riscos associados à obsolescência tecnológica. No entanto, a diversificação de fornecedores pode aumentar a complexidade na gestão de riscos, especialmente em termos de integração e monitoramento.

5. Requisitos Técnicos Específicos

Funcionalidades de Threat Prevention

Os requisitos técnicos especificados incluem:

- Application Control.
- IPS (Intrusion Prevention System)
- URL Filtering
- Anti-Bot
- Anti-Virus
- Anti-Spam
- DNS Security

Capacidade de Inspeção de 34Gbps com funções de Threat Prevention ativadas : Os novos modelos Check Point atendem a este requisito, garantindo alto desempenho mesmo com todas as funcionalidades habilitadas.

Certificações Ambientais e de Segurança

- Certificações de segurança : CB IEC 62368-1 e UL62368-1
- Certificações de emissões : CE e FCC
- Certificações ambientais : ROHS e ISO 14001

Capacidade de Gestão de Conexões de

- Pelo menos 20 milhões de conexões simultâneas;
- Recepçao de até 1 milhão de novas conexões por segundo.

6. Padrões de Sustentabilidade e Eficiência

Agenda de Desenvolvimento Sustentável (ODS):

O Governo Federal orienta os órgãos públicos a adotarem práticas sustentáveis, incluindo o uso eficiente de recursos tecnológicos.

Análise: A Solução 3 contribui para a eficiência tecnológica, pois substitui equipamentos obsoletos por dispositivos modernos e certificados ambientalmente, alinhando-se à Agenda de Sustentabilidade. A diversificação de fornecedores também promove inovação e competição.

Conclusão: Adesão aos Padrões e Políticas

A Solução 3 apresenta alta aderência aos padrões e políticas de governo, desde que os equipamentos selecionados atendam aos requisitos técnicos especificados. Ela atende plenamente às funcionalidades avançadas de threat prevention , capacidade de inspeção e gestão de conexões, além de certificações ambientais e de segurança. No entanto, a diversificação de fornecedores introduz desafios adicionais,

como maior complexidade de integração, curva de aprendizado para a equipe técnica e potencial inconsistência na gestão de segurança.

Portanto, esta solução é recomendada apenas se houver um planejamento detalhado para mitigar os riscos associados à diversificação de fornecedores e garantir a padronização e interoperabilidade dos novos equipamentos.

g) Custos estimados para fins de análise comparativa

g.1) Item 1: Appliance de firewall NGFW com Threat Prevention, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (NGFW e threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.

Inicialmente cumpre informar que os equipamentos necessários ao TSE possuem capacidade de processamento superior à média utilizada pelo mercado. Devido à realização de Eleições, o tráfego de rede que passa pelos equipamentos exige que os Firewalls a serem adquiridos pelo TSE sejam de alta capacidade.

Pesquisando-se o Portal Nacional de Compras Públicas, somente o Edital 90906/2024 publicado pelo SERPRO (UASG 803080) possui características compatíveis com a necessidade do TSE.

Adicionalmente, registramos que não é efetiva a comparação utilizando equipamentos de menor capacidade que as necessárias ao TSE.

Para fins de análise comparativa, foi realizada comparação de preços utilizando-se os produtos abaixo, ofertados por licitantes para o pregão realizado pelo SERPRO. Vide documentação do pregão no link https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-2?compra=80308005909062024.

A empresa NCT ofertou, para o Item 1, o par (cluster) de Firewall Fortinet FG-3000F a um preço unitário de R$ 2.487.209,00, correspondendo a um valor unitário de R$ 1.243.604,50, por firewall.

A empresa NTSec ofertou, para o item 1, o par (cluster) de Firewall Check Point 19200 a um preço unitário de R$ 3.173.837,00, correspondendo a um valor unitário de R$ 1.586.918,50, por firewall.

Licitante	Fabricante	Modelo	Capacidade de Threat Prevention	Preço unitário por firewall
NTSec	Check Point	19200	36,9 Gbps	R$ 1.243.604,50
NCT	Fortinet	FG-3000F	33 Gbps	R$1.586.918,50
			Valor médio	R$ 1.415.261,50

g.2) Item 2: Migração das configurações dos firewalls atuais para os novos equipamentos

Para referência de preços para os serviços em questão, consignou-se por referência os serviços exigidos pelo SERPRO Edital 90906/2024 - UASG 803080. Considerando-se que as dimensões dos Firewalls necessários ao SERPRO equivalem ao do TSE, é razoavel entender que o esforço de migração, por firewall, é equivalente.

Para a realização desse serviço a empresa NTC ofertou valor de R$ R$ 18.586,77 por firewall, enquanto a empresa NTSec ofertou valor de R$ 16.500,00 por firewall.

Licitante	Fabricante	Modelo	Serviço de migração	Valor unitário por migração
NTSec	Check Point	19200	1	R$ 18.586,77
NCT	Fortinet	FG-3000F	1	R$ 16.500,00
			Valor médio	R$ 17.543,38

g.3) Item 3: Serviço gerenciado mensal

Para referência de preço dos serviços de gerenciamento necessários a apoiar as equipes técnicas do TSE em uma nova tecnologia, Identificamos os serviços do item 7 do Grupo 2 do Pregão 9665/2023 do Tribunal Regional do Trabalho da 12ª Região - Santa Catarina (TRT12). Vide documentação em https://pncp.gov.br/app/atas/00509968000148/2023/1136/1.

O item em questão inclui o serviço gerenciado durante 24 meses para um cluster (um par) de Firewall 23500, de mesmo porte do equipamento do TSE, a um valor de R$ 309.500,00.
Considerando-se a proporcionalidade de 18 meses e que o preço ofertado cobre um par de firewalls, temos que o custo de serviços gerenciados para um firewall durante 18 meses é de R$ 116.062,50. Considerando-se que A Ata de Registro de Preços oriunda desse pregão fora publicada em 14 de setembro de 2023, atualizamos o IPCA entre 14/09/2023 a 24/03/2025 por um fator de 7,8067% (mediante consulta ao site calculo exato). O valor resultante foi de R$ 125.123,20

Licitante	Fabricante	Modelo	Serviço gerenciado por firewall	Valor unitário do serviço de 18 meses (por firewall)

Licitante	Fabricante	Modelo	Serviço gerenciado por firewall	Valor unitário do serviço de 18 meses (por firewall)
NTSec	Check Point	23500	4	R$ 125.123,20

g.4) Item 4: Treinamento na nova tecnologia

Para referência de preços de treinamento das equipes da COINF, identificamos o item 6 do PRegão Eletrônico 65/2023 do STF (UASG 40001).

A documentação do referido pregão pode ser obtida em http://comprasnet.gov.br/livre/pregao/ata2.asp?co_no_uasg=40001&numprp=000652023&codigoModalidade=5

A proposta emitida pela empresa NCT para o STF possui data de 10/10/2023. O valor ofertado para o treinamento foi de R$ 60.000,00. Atualizando-se o valor por meio do site calculo exato, temos que o IPCA acumulado entre 10/10/2023 e 24/03/2025 foi de 7,5272%

Licitante	Fabricante	Modelo	Treinamento	Valor unitário
NCT	Fortinet	FG-3000F	1	R$ 64.516,30

g.5) Consolidando-se os valores analisados acima, temos o seguinte quadro estimativo de custos para a solução 3:

Item	Descrição	Quantidade	Valor unitário	Valor Total
1	Appliance de firewall NGFW com Threat Prevention, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (NGFW e threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	4	R$ 1.415.261,50	R$ 5.661.046,00
2	Migração das configurações dos firewalls atuais para os novos equipamentos	4	R$ 17.543,38	R$ 70.173,52
3	18 meses de serviços gerenciados (por firewall)	4	R$ 125.123,20	R$ 500.492,80
4	Treinamento na nova tecnologia	1	R$ 64.516,30	R$ 64.516,30
			TOTAL	**R$ 6.296.228,62**

h) Vantagens e desvantagens

Solução 3: Substituição dos equipamentos atuais por equipamentos de quaisquer fabricantes

Vantagens:

- **Ganho em concorrência:** A licitação aberta a diversos fabricantes pode levar a uma competição maior, reduzindo custos e ampliando as opções.
- **Possibilidade de melhor custo-benefício**: O interesse de fabricantes em ter o TSE em sua lista de clientes pode ensejar a apresentação de preços mais vantajosos.

Desvantagens:

- **Complexidade de integração:** Equipamentos de diferentes fabricantes podem apresentar desafios de compatibilidade com a infraestrutura existente, exigindo ajustes técnicos e maior esforço de implementação.
- **Curva de aprendizado:** A equipe técnica precisará ser treinada para operar e manter os novos equipamentos, o que pode demandar tempo e recursos adicionais.
- **Risco de inconsistências:** A diversificação de fornecedores pode introduzir inconsistências na gestão da segurança da rede, dificultando a padronização e o monitoramento.
- **Custo inicial elevado:** Assim como na Solução 2, a substituição completa dos equipamentos implica um investimento significativo, além de custos associados à migração e treinamento.

2.4 Resumo comparativo das soluções

Quadro Resumo Comparativo das Soluções

Solução	Descrição	Unidade de medida	Quantidades	Custo estimado	Comentários

Solução	Descrição	Unidade de medida	Quantidades	Custo estimado	Comentários
1ª	Contratação de garantia estendida, com suporte 24x7 e com direito de atualização corretiva e evolutiva dos softwares de Firewall Check Point, modelo 23500, por 60 meses.	Por firewall instalado no TSE	4	R$ 8.139.847,40	Em que pese não ser viável a contratação da solução 1 haja vista o intercurso inferior a um ano até que o equipamento entre em fim de vida, a equipe de planejamento optou por manter a estimativa de custo de eventual extensão de garantia por 60 meses a fim de prover ao administrador uma visão comparativa de custos entre esta solução e as demais.
2ª	Substituição dos firewalls modelo 23500 por equipamentos mais modernos **do mesmo fabricante**, aproveitando a compatibilidade com a infraestrutura existente e assegurando tecnologia atualizada, desempenho superior e suporte técnico de longo prazo. Assim, esta solução se caracteriza como sendo Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	Por firewall instalado no TSE	4	R$ 6.347.674,00	
3ª	Substituição dos firewalls modelo 23500 por equipamentos de **qualquer fabricante**. Assim, esta solução se caracteriza como sendo Aquisição de Appliance de firewall NGFW com Threat Prevention, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (NGFW e threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses.	Vide tabela no item 2.3.g.5	Vide tabela no item 2.3.g.5	R$ 6.296.228,62	

CAPÍTULO 3. A SOLUÇÃO ESCOLHIDA

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

A escolha da Solução 2 – "*Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses*", apresenta diversas vantagens estratégicas, técnicas e operacionais em comparação com as demais soluções. A seguir, destacam-se os principais benefícios, com ênfase na preservação do conhecimento técnico da equipe atual:

3.1.1. Preservação do Conhecimento Técnico Especializado

Experiência Consolidada:

A equipe técnica do TSE possui mais de 12 anos de experiência na administração de firewalls Check Point, tornando-se altamente especializada nessa tecnologia. A troca para um fabricante diferente exigiria que esses profissionais aprendessem uma nova plataforma, comprometendo a eficiência operacional e

aumentando o tempo de adaptação.

Vantagem sobre a Solução 3: Ao manter o mesmo fabricante, a equipe técnica pode aplicar seu conhecimento profundo imediatamente, sem interrupções ou perda de produtividade. Tal benefício consiste de elemento fundamental em um cenário de frequentes tentativas de ataques cibernéticos à Justiça Eleitoral e necessidade de proteção dos sistemas informatizados e à imagem do TSE.

Redução da Curva de Aprendizado:

A migração para equipamentos da mesma marca minimiza a necessidade de treinamento extensivo, reduzindo custos e esforços associados à capacitação técnica.

Vantagem sobre a Solução 3: Em contraste, a adoção de firewalls de outro fabricante transformaria a equipe técnica em "iniciantes", aumentando a probabilidade de erros operacionais durante o período de transição.

3.1.2. Compatibilidade e Continuidade Tecnológica

Integração Simplificada:

Os novos equipamentos Check Point são totalmente compatíveis com a infraestrutura existente, facilitando a migração e minimizando impactos operacionais.

Vantagem sobre a Solução 3: A substituição por firewalls de outros fabricantes pode introduzir desafios de integração, como incompatibilidade de protocolos, APIs ou sistemas de gerenciamento centralizados, possibilitando inconsistências na rede e instabilidades durante longos períodos.

Padronização de Segurança:

Manter a mesma plataforma permite a continuidade das políticas de segurança já implementadas, garantindo consistência na gestão de riscos.

Vantagem sobre a Solução 3: A diversificação de fornecedores pode fragmentar as práticas de segurança, dificultando a padronização e aumentando a complexidade operacional.

3.1.3. Redução de Riscos Operacionais

Suporte Técnico Familiar:

A equipe técnica já está acostumada com os processos de suporte técnico da Check Point, o que facilita a resolução de problemas críticos e a implementação de atualizações.

Vantagem sobre a Solução 1: Diferentemente da expansão de garantia, que é uma solução temporária, a substituição por equipamentos novos garante suporte técnico prolongado, eliminando riscos associados ao fim de vida dos dispositivos atuais.

Minimização de Interrupções:

A migração para equipamentos da mesma marca reduz significativamente o risco de interrupções durante a implementação, pois os processos e ferramentas já são conhecidos pela equipe.

Vantagem sobre a Solução 3: A adoção de uma nova tecnologia pode introduzir falhas ou inconsistências durante a transição, impactando diretamente os serviços prestados pelo TSE.

3.1.4. Modernização Tecnológica e Sustentabilidade

Tecnologia Atualizada:

A substituição dos equipamentos antigos por modelos mais modernos da Check Point garante acesso a funcionalidades avançadas de threat prevention, maior capacidade de inspeção e escalabilidade, alinhando-se às melhores práticas de segurança cibernética.

Vantagem sobre a Solução 1: A expansão de garantia mantém equipamentos obsoletos, enquanto a Solução 2 promove a modernização tecnológica necessária para proteger a infraestrutura crítica do TSE.

Eficiência Energética e Certificações Ambientais:

Os novos equipamentos Check Point atendem a certificações ambientais como ROHS, WEEE e ISO 14001, contribuindo para a sustentabilidade e eficiência energética.

Vantagem sobre a Solução 3: Embora outros fabricantes também ofereçam certificações ambientais, a escolha da Check Point garante a continuidade dessas práticas dentro de uma plataforma já consolidada.

3.1.5. Economicidade e Planejamento Estratégico

Custo-Benefício a Longo Prazo:

Embora a Solução 2 tenha um custo inicial elevado se comparado à Solução 1, ela elimina os riscos associados à obsolescência tecnológica e ao fim de vida dos equipamentos, garantindo um retorno sobre o investimento a longo prazo.

Vantagem sobre a Solução 1: A expansão de garantia é uma solução paliativa que não resolve o problema estrutural, enquanto a Solução 2 oferece uma solução definitiva.

Planejamento Alinhado ao PDTI:

A substituição dos equipamentos atuais por modelos mais modernos está plenamente alinhada ao Plano Diretor de Tecnologia da Informação (PDTI) do TSE, que prevê a renovação gradual da infraestrutura tecnológica.

Vantagem sobre a Solução 3: A diversificação de fornecedores pode introduzir incertezas no

planejamento estratégico, enquanto a escolha da Check Point mantém a previsibilidade e controle sobre os investimentos.

3.1.6. Segurança Cibernética Fortalecida

Funcionalidades Avançadas de Threat Prevention:

Os novos firewalls Check Point oferecem todas as funcionalidades de threat prevention exigidas, como Application Control , IPS , URL Filtering , Anti-Bot , Anti-Virus , Anti-Spam e DNS Security , além de capacidade de inspeção dsuperior a 34Gbps com as funções ativadas.

Vantagem sobre a Solução 3: Embora outros fabricantes também possam oferecer essas funcionalidades, a expertise da equipe técnica em Check Point garante uma implementação mais rápida e eficiente.

Capacidade de Gestão de Conexões:

Os novos equipamentos atendem aos requisitos de gestão de 20 milhões de conexões simultâneas e crescimento de até 1 milhão de novas conexões por segundo, garantindo escalabilidade e desempenho.

Vantagem sobre a Solução 1: A expansão de garantia mantém equipamentos com capacidade limitada, enquanto a Solução 2 oferece recursos adequados às demandas crescentes do TSE.

3.1.7. Maturidade na gestão de vulneravibilidades

Um levantamento de todas as vulnerabilidades conhecidas e relacionadas a quatro grandes fabricantes de firewall (vide Planilha de Análise de fabricantes - falhas e tempo de correção - SEI3189441) demonstrou que os produtos do fabricante da solução escolhida pelo TSE apresentaram, ao longo dos últimos cinco anos, um volume muito inferior de vulnerabilidades. Tal fato evidencia zelo com a segurança cibernética e maturidade em seu processo de ciclo de vida do produto (testes, controles, validações).

Tal característica consiste de elemento extremamente relevante para a condução de eleições, haja vista que a segurança cibernética ser essencial para um processo intimamente ligado com a soberania nacional e a segurança nacional.

Total de vulnerabilidades por ano					
Fornecedor	**2024**	**2023**	**2022**	**2021**	**2020**
Check Point	2	3	6	4	7
Palo Alto	56	22	21	34	70
Fortinet	84	88	86	98	60
Cisco	6	40	136	64	105

De forma complementar, ao observarmos o tempo (em dias) que os fabricantes levaram para lançar uma correção de vulnerabilidades altas e críticas, vemos que há novamente uma vantagem considerável para o fabricante da solução escolhida por esta equipe técnica.

Registre-se que uma vulnerabilidade alta ou uma vulnerabilidade crítica representa uma situação onde o produto ofertado perdeu sua eficiência. Consiste de situação em que o produto permite a invasão da rede de comunicação de dados. Assim, há extrema relevância que as eventuais e indesejadas vulnerabilidades altas e críticas sejam corrigidas no menor intervalo possível.

Tempo para corrigir apenas vulnerabilidades críticas + altas (dias)					
Fornecedor	**2024**	**2023**	**2022**	**2021**	**2020**
Check Point	1	2	1	0	2
PAN	17	2	6	18	46
Fortinet	28	34	29	30	5
Cisco	19	15	43	24	50

Os dados apresentados evidenciam a superioridade da solução escolhida por esta equipe técnica na gestão de vulnerabilidades cibernéticas. Com apenas 5 vulnerabilidades identificadas desde 2023, o fabricante se destaca por sua robustez tecnológica, enquanto outros concorrentes como Palo Alto (78 vulnerabilidades), Fortinet (172 vulnerabilidades) e Cisco (46 vulnerabilidades) apresentaram números significativamente maiores.

Além disso, o fabricante Check Point demonstrou uma resposta rápida e eficaz, corrigindo as vulnerabilidades em média em 6 dias e as classificadas como "High/Critical" em apenas 1 dia , muito abaixo das médias de seus

concorrentes (por exemplo, Palo Alto demorou 111 dias para corrigir vulnerabilidades críticas).

Conclusão

A escolha do fabricante Check Point para a solução de firewalls do TSE é uma decisão técnica reforçada por dois pilares relevantes: a preservação do conhecimento técnico da equipe especializada e a maturidade demonstrada pelo fabricante na gestão de vulnerabilidades.

Primeiramente, a equipe técnica do TSE possui mais de 12 anos de experiência com soluções Check Point, o que garante um alto nível de expertise e eficiência operacional. Ao manter a mesma tecnologia, evita-se a perda de conhecimento impossível de recuperar rapidamente apenas com treinamentos. Seriam necessários anos de experiência até que a recuperar a plena proficiência da equipe técnica do TSE adaptada à nova tecnologia. Minimiza-se, assim, riscos de interrupções e garante-se a continuidade dos serviços essenciais.

Adicionalmente, a capacidade do fabricante da solução escolhida em mitigar rapidamente ameaças cibernéticas reforça a segurança cibernética, alinhando-se perfeitamente aos requisitos estratégicos da Justiça Eleitoral.

3.2 Detalhamento da solução

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

A solução que se deseja contratar consiste de"*Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses*".

b) Quantidades e as respectivas unidades de medida/fornecimento, com as devidas justificativas, acompanhadas das memórias de cálculo e dos documentos que lhe dão suporte

Item	Descrição	Unidade	Quantidade	Valor unitário	Valor Total
1	Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses. Account ID do TSE: 0008229609	unidade	4	R$ 1.586.918,50	R$ 6.347.674,00

O TSE possui atualmente 4 equipamentos firewall do fabricante Check Point, modelo 23500. E deseja atualizá-los para a geração mais recente: Check Point modelo 19200, conforme apresentado no item 1.2.a.2 deste Estudo Técnico Preliminar.

A aquisição de firewalls para o Tribunal Superior Eleitoral (TSE) mediante indicação de marca e modelo está fundamentada no Art. 41 da Lei nº 14.133/2021 , que permite tal medida em situações excepcionais, desde que formalmente justificada. No presente caso, a escolha do fabricante Check Point e de seus modelos mais recentes é necessária e justificável pelas seguintes razões:

3.2.b.1) Padronização do Objeto

O TSE já utiliza equipamentos firewall da marca Check Point há mais de uma década, o que resultou na padronização de suas plataformas de segurança cibernética. A substituição dos equipamentos atuais por modelos mais modernos da mesma marca garante a continuidade dessa padronização, evitando inconsistências operacionais e reduzindo os riscos associados à adoção de tecnologias incompatíveis. A manutenção da mesma plataforma tecnológica também facilita a integração com sistemas existentes, garantindo eficiência e desempenho.

3.2.b.2) Compatibilidade com Plataformas e Padrões Já Adotados (Inciso I, Alínea "b"):

A infraestrutura de segurança do TSE foi desenvolvida e otimizada ao longo dos anos para operar com soluções Check Point. A troca para um fabricante diferente poderia comprometer a compatibilidade com as políticas de segurança, protocolos e ferramentas de gerenciamento já implementadas, introduzindo complexidade técnica desnecessária. Além disso, a equipe técnica do TSE possui expertise consolidada na administração de firewalls Check Point, o que minimiza a curva de aprendizado e maximiza a eficiência operacional durante a transição para os novos equipamentos.

3.2.b.3) Atendimento às Necessidades Específicas do TSE (Inciso I, Alínea "c"):

A Justiça Eleitoral demanda um nível elevado de segurança cibernética para proteger sua infraestrutura crítica contra ameaças avançadas. Dados recentes demonstram que o fabricante Check Point apresenta o menor número de vulnerabilidades entre os principais fornecedores de firewall, além de ser o mais ágil na correção dessas vulnerabilidades, com tempos médios de resolução. Essa maturidade na gestão de vulnerabilidades torna o Check Point a única solução capaz de atender plenamente às necessidades de

segurança do TSE, especialmente considerando a criticidade dos serviços prestados pelo Tribunal.

3.2.b.4) Preservação do Conhecimento Técnico Especializado:

A equipe técnica do TSE possui mais de 12 anos de experiência na administração de soluções Check Point, sendo altamente especializada nessa tecnologia. A adoção de um novo fabricante exigiria treinamento extensivo, aumentando custos e introduzindo riscos operacionais durante o período de adaptação. Manter o mesmo fabricante preserva o conhecimento técnico acumulado, garantindo maior agilidade na implementação e suporte contínuo.

3.2.b.5) Segurança Cibernética e Continuidade Operacional:

A segurança cibernética é um pilar fundamental para a Justiça Eleitoral, dada a sensibilidade das informações e processos sob sua responsabilidade. A escolha do Check Point, comprovadamente superior em termos de robustez tecnológica e resposta rápida a vulnerabilidades, reforça o compromisso do TSE com a proteção de sua infraestrutura crítica. A substituição dos equipamentos atuais por modelos mais modernos da mesma marca assegura a continuidade operacional, eliminando os riscos associados ao fim de vida dos dispositivos existentes.

A indicação de marca e modelo em uma contratação pública, embora justificada com base no Art. 41 da Lei nº 14.133/2021, exige medidas robustas para mitigar o risco de sobrepreço por parte do fabricante ou seus representantes. A equipe técnica de planejamento do Tribunal Superior Eleitoral (TSE) adotará as seguintes estratégias para garantir a economicidade e transparência do processo:

a) Utilização de Preços de Referência Baseados em Licitações Competitivas

A equipe técnica utilizará preços de referência obtidos de licitações anteriores em que todos os fornecedores participaram, mas nas quais a Check Point foi declarada vencedora. Essa abordagem garante que os valores considerados como base já foram submetidos à concorrência e validados pelo mercado. Ao adotar esse critério, o TSE assegura que os preços praticados estejam alinhados ao valor de mercado e refletem condições competitivas, reduzindo significativamente o risco de sobrepreço.

b) Identificação e Comparação de "Part Numbers" com Preços Praticados pelo Fabricante

A equipe técnica identificará todos os "part numbers" necessários para a implementação da solução, incluindo equipamentos, licenças de software, serviços de suporte e acessórios. Esses itens serão comparados com os preços efetivamente praticados pelo fabricante em outros contratos públicos e privados. Essa análise detalhada permitirá verificar se os valores propostos estão dentro da média de mercado e evitará discrepâncias significativas entre os preços ofertados e os valores reais praticados pelo fabricante.

c) Análise Crítica de Preços com Base em "Price Lists" Internacionais

Conforme recomendação do Acórdão TCU 1432/2024 - PLENÁRIO, a equipe técnica realizará uma análise crítica dos preços por meio da comparação com "price lists" publicados no exterior pelo fabricante Check Point. Essa prática permite verificar se os valores cobrados no Brasil estão alinhados aos preços internacionais, considerando ajustes de câmbio, impostos e eventuais custos logísticos. A utilização de listas de preços internacionais é um mecanismo eficaz para identificar possíveis distorções e garantir que os preços contratados estejam em conformidade com padrões globais.

c) Garantia Técnica/Assistência Técnica/ Suporte Técnico

A solução a ser contratada deverá contemplar a garantia técnica do fabricante, durante um período de 60 meses.

Devido à relevância dos equipamentos para o funcionamento da rede de comunicação de dados do TSE e dos sistemas informatizados, o atendimento em garantia deverá ser prestado em formato "24x7".

d) Normas Legais exclusivas

- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

e) Normas Técnicas aplicáveis

No escopo da solução a ser contratada são aplicáveis as seguintes normas técnicas:

1. ABNT NBR ISO/IEC 27032

A norma ABNT NBR ISO/IEC 27032 estabelece diretrizes para a gestão da segurança cibernética, abordando aspectos relacionados à proteção de infraestruturas críticas contra ameaças digitais. Ela enfatiza a importância de soluções tecnológicas robustas, como firewalls, para mitigar riscos cibernéticos e garantir a continuidade dos serviços.

Aplicação na Compra:

Os novos firewalls Check Point devem ser avaliados quanto à sua capacidade de implementar funcionalidades avançadas de threat prevention , como IPS , URL Filtering , Anti-Bot , Anti-Virus , DNS Security , entre outras, conforme recomendado pela norma. Além disso, os equipamentos devem ser

capazes de inspecionar tráfego em alta velocidade (34Gbps) com todas as funções ativadas, garantindo desempenho sem comprometer a segurança.

2. ABNT NBR ISO/IEC 15408 (Common Criteria)

A norma ABNT NBR ISO/IEC 15408 , conhecida como Common Criteria , define um framework para avaliar a segurança de produtos de Tecnologia da Informação (TI). Ela certifica que os equipamentos atendem a requisitos rigorosos de segurança funcional e garantia, com base em perfis de proteção reconhecidos internacionalmente.

Aplicação na Compra:

Os firewalls Check Point devem possuir certificação Common Criteria ou equivalente, comprovando sua conformidade com padrões globais de segurança. Essa certificação garante que os equipamentos foram submetidos a avaliações rigorosas por laboratórios credenciados, validando sua eficácia contra vulnerabilidades e ataques cibernéticos.

3. ABNT NBR ISO/IEC 27001 e 27002:

Essas normas estabelecem requisitos para sistemas de gestão da segurança da informação (SGSI) e boas práticas para controles de segurança. Os firewalls devem suportar políticas de segurança alinhadas a essas normas, facilitando a integração com o SGSI do TSE.

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

Não se aplica. Não há alocação de equipe técnica.

g) Transição contratual

Não há necessidade.

h) Transferência de conhecimento

Considerando-se que a solução escolhida refere-se à manutenção da mesma tecnologia já em uso no TSE há mais de 12 anos e a proficiência da equipe técnica do TSE na solução escolhida, não há necessidade de transferência de conhecimento.

i) Treinamento

Considerando-se que a solução escolhida refere-se à manutenção da mesma tecnologia já em uso no TSE há mais de 12 anos e a proficiência da equipe técnica do TSE na solução escolhida, não há necessidade de treinamento.

j) Deslocamentos e Reembolso de Diárias e Passagens

Não se aplica.

3.3. Outros aspectos relacionados à execução contratual

a) vigência da ata de registro de preços, vigência contratual e prazo de execução

a.1) vigência da ata de registro de preços (ARP), se for o caso.

Não se aplica, haja vista que a contratação ora pretendida não exigirá publicação de ata de registro de preços.

a.2) vigência contratual

Esta equipe de planejamento prevê a vigência de 63 meses para o contrato, assim detalhada:

- 3 meses para entrega dos equipamentos no TSE.
- 60 meses de garantia dos equipamentos. Durante o período de garantia, a empresa contratada deverá responsabilizar-se pelo efetivo atendimento para suporte aos equipamentos, devendo apresentar garantia contratual válida até o final do contrato.

a.3) se aplicável, também deve ser informado o prazo de execução do serviço.

Os equipamentos devem ser fornecidos ao TSE e instalados no prazo de até 90 dias contados da publicação do Contrato no PNCP.

b) Ordem de Serviço Inicial

Não há necessidade. O fornecimento e respectiva instalação dos equipamentos terá seu prazo de início contabilizado a partir da publicação do contrato no PNCP.

c) Impactos ambientais

A aquisição de novos firewalls Check Point pelo Tribunal Superior Eleitoral (TSE) incorpora medidas robustas para mitigar impactos ambientais, alinhando-se às melhores práticas de sustentabilidade e conformidade com normas internacionais. Para garantir que os equipamentos adquiridos sejam ambientalmente responsáveis, foram estabelecidos critérios rigorosos baseados em normas técnicas reconhecidas e práticas sustentáveis.

1. Conformidade com Normas de Segurança, Emissões e Sustentabilidade

Os novos firewalls devem atender a um conjunto abrangente de normas que garantem segurança operacional, controle de emissões e sustentabilidade ambiental:

Normas de Segurança:

Os equipamentos devem estar em conformidade com as normas **CB IEC 62368-1 , CE LVD EN62368-1 , UL62368-1 e ASNZS 62368.1** , que regulamentam a segurança elétrica e mecânica dos dispositivos. Essas certificações asseguram que os produtos não representam riscos ao meio ambiente ou à saúde humana durante sua operação.

Normas de Emissões:

A mitigação de interferências eletromagnéticas é garantida pela conformidade com as normas **CE , FCC IC , VCCI e ASNZS ACMA**. Essas certificações garantem que os equipamentos operam dentro dos limites aceitáveis de emissões, minimizando impactos no ambiente eletromagnético.

Normas Ambientais:

Os firewalls devem atender às normas **ROHS** (Restrição de Substâncias Perigosas), **REACH** (Registro, Avaliação, Autorização e Restrição de Substâncias Químicas), **WEEE** (Resíduos de Equipamentos Elétricos e Eletrônicos) e **ISO 14001** (Sistema de Gestão Ambiental). Essas normas asseguram que os equipamentos são fabricados sem o uso de materiais nocivos ao meio ambiente, promovem a reciclagem adequada e estão inseridos em processos de gestão ambiental certificados.

2. Logística Reversa de Peças Substituídas

Como parte das medidas de mitigação de impactos ambientais, a contratada será obrigada a assumir a responsabilidade pela logística reversa de peças eventualmente substituídas durante a implementação ou manutenção dos equipamentos. Isso inclui a coleta, transporte e destinação adequada de componentes obsoletos ou danificados, garantindo que esses materiais sejam reciclados ou descartados de forma ambientalmente correta, conforme as normas **WEEE** e **ISO 14001** .

3. Documentação em Meio Eletrônico

Para reduzir o consumo de papel e promover práticas sustentáveis, toda a documentação técnica relacionada aos equipamentos, incluindo manuais de operação, guias de instalação e certificações, deverá ser fornecida exclusivamente em meio eletrônico . Essa exigência não apenas contribui para a preservação dos recursos naturais, mas também facilita o acesso e armazenamento seguro das informações por parte da equipe técnica do TSE.

3.4 Serviços e/ou materias complementares não contemplados na solução escolhida

a) Contratação adicional

Não se aplica.

b) Ajustes em outras contratações existentes

Não se aplica.

c) Requisitos de TI

Não se aplica.

d) Adequação das Instalações e Infraestrutura do TSE

A instalação dos novos firewall deverá ocorrer de forma a não interromper o funcionamento dos atuais firewalls.

Devido a isso, é necessário que a equipe de rede do TSE reserve espaço no datacenter, em região próxima aos atuais firewall, para que os novos sejam instalados.

Após a instalação dos novos firewalls, haverá a comutação da rede para estes equipamentos e, assim, os antigos poderão ser desativados.

CAPÍTULO 4. ANÁLISE DO PROCESSO DE CONTRATAÇÃO ANTERIOR

4.1 Procedimento SEI, Contrato ou Nota de Empenho

A contratação anterior fora conduzida no TSE por meio do processo 2019.00.000002707-2.

O Estudo Técnico Preliminar então elaborado encontra-se no documento SEI 1105978.

O Edital de Pregão Eletrônico 62/2019 encontra-se no documento SEI 1173551.

O Anexo I - Termo de Referência encontra-se no documento SEI 1173563.

Consistiu da aquisição de 4 equipamentos firewall Marca Checkpoint, modelo 23500 Security Gateway, a um valor total de **R$** 7.927.000,00 (sete milhões novecentos e vinte e sete mil reais).

Atualizando-se o valor acima pelo IPCA desde a data de assinatura do Contrato TSE 62/2019 (12/12/2019) até 28/02/2025, temos um valor atualizado de **R $ 10.718.273,19 (dez milhões, setecentos e dezoito mil duzentos e setenta e três reais e dezenove centavos).**

A atualização dos valores pelo PICA foi realizada por meio do site calculoexato.com.br, obtendo-se uma variação do IPCA de 35,2122% entre 12/12/2019 e 28/02/2025.

4.2 Fase Interna da Licitação (exigências e sugestões exaradas pelas unidades técnicas da SAD e Assessoria Jurídica)

Quanto ao Despacho SEARE 1006471

A equipe de planejamento apresentara apenas uma solução nos Estudos Preliminares então realizados. Desta feita, a equipe de planejamento pesquisou outras possiveis soluções, com respectivo detalhamento.

Houve dúvidas sobre exigência de manter-se o mesmo fabricante dos equipamentos anteriores visando compatibilidade. O atual ETP dedicou uma seção à analisar os benefícios relacionados a tal questão.

A SEARE questionou se a contratação ds firewalls poderia ser realizada de forma conjugada com a contratação de serviços do Backbone da Justiça Eleitoral (enlaces de comunicação de dados entre o TSE e os TRE), o presente ETP detalha a vantajosidade de que os dois projetos sejam realizados de forma apartada.

Por fim, a SEARE recomendou que fossem juntados aos autos os documentos que demonstravam vantajosa a implementação de VPN entre o TSE e os TRE, em detrimento da atualização dos firewalls dos TRE. Ressaltamos que não é objeto do presente ETP os firewalls dos TRE, deixando de fazer sentido tal consideração da SEARE. Registre-se, no entanto, que todo o levantamento de estimativa de preços das soluções ora aventadas, estão detalhadas neste documento.

Quanto à Informação AGES 96 (1135445)

Consistiu de análise de critérios socioambientais constantes do projeto de atualização dos equipamentos.

Os critérios sugeridos foram:

1. Apresentação do Certificado de Registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais (CTF/APP) para atendimento ao art. 17 da Lei nº 6.938/81 - Política Nacional do Meio Ambiente.
2. Os equipamentos eletrônicos não devem conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS.
3. Utilização de embalagens fabricadas com materiais que propiciem a reutilização ou a reciclagem, art. 32 da Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos.
4. Logística reversa com destinação ambientalmente adequada dos resíduos, art. 33 da Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos.
5. Fornecimento aos empregados dos equipamentos de segurança que se fizerem necessários para a execução de serviços, art. 6º da IN MPOG nº 01/2010.
6. Realização de programa interno de treinamento de seus empregados para a redução de consumo de energia elétrica, consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais, art. 6º da IN MPOG nº 01/2010.
7. A contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo;
8. A contratada, ou seus dirigentes, não deve ter sido condenada por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo.
9. Elaboração e implementação do Programa de Controle Médico de Saúde Ocupacional (PCMSO) e do Programa de Prevenção de Riscos Ambientais (PPRA).
10. Atendimento ao art. 93 da Lei nº 8.213/91.

Dentre os critérios acima, não possuem coerência com o objeto da presente contratação os de número 5, 6 e 9, haja vista que não há, na contratação pretendida, o fornecimento de mão de obra.

Quanto ao Parecer ASJUR 550 (1151455)

O Parecer Jurídico destaca a necessidade de ajustes técnicos, legais e formais na minuta de edital e seus anexos. As principais providências incluem: correção de inconsistências textuais, inclusão de cláusulas específicas sobre garantia e suporte, uniformização de prazos e códigos orçamentários, e observância das normas de sustentabilidade e critérios de participação de ME/EPP. Vejamos:

1. Aspectos Legais e Regulatórios

Regime de Execução do Contrato :

O regime de execução do contrato deve ser claramente definido como "empreitada por preço global" , conforme o art. 6º, VIII, “a” da Lei nº 8.666/93.

Manifestação desta equipe de planejamento: Na elaboração do termo de referência, em consonacia com o objeto contratado, deverá ser registrado claramente o regime de execução observando-se o que prevê a Lei 14.133/2021.

Aplicação do Decreto nº 8.538/2015 (ME/EPP) :

Não é possível aplicar a reserva de 25% do quantitativo para microempresas (ME) e empresas de pequeno porte (EPP) devido à ausência de equipamentos nacionais com características técnicas adequadas.

Manifestação desta equipe de planejamento: Manter a justificativa no Termo de Referência (TR) sobre a impossibilidade de aplicação da cota reservada.

Critérios de Sustentabilidade :

A inclusão de critérios de sustentabilidade é obrigatória, conforme legislação vigente (ex.: Constituição Federal, Lei nº 12.305/2010, Diretiva RoHS).

Manifestação desta equipe de planejamento: Assegurar que os critérios de sustentabilidade estejam claramente definidos no Termo de Referência e Edital.

2. Ajustes na Minuta de Edital e Anexos

Erros de Digitação e Padronização :

Corrigir erros ortográficos e inconsistências (ex.: "Checkpoint" para "Check Point", "Contrato 88/2018" para "Contrato 88/2015").

Manifestação desta equipe de planejamento: Realizar revisão textual e padronização terminológica.

Garantia Técnica e Suporte :

Incluir subitens no item 4.6 para detalhar obrigações de suporte técnico, como:

Disponibilização de sistema de abertura de chamados com acompanhamento online.

Responsabilidade total da contratada pelas despesas geradas pelo suporte técnico.

Capacitação e certificação dos técnicos de suporte pela fabricante.

Manifestação desta equipe de planejamento: Assegurar que as obrigações atinentes ao suporte técnico estejam ricamente detalhadas no Termo de Referência e que a Minuta de Contrato faça remissão a tais obrigações.

Atualizações de Software :

Garantir que a contratada disponibilize atualizações de software e firmware sem custos adicionais durante o período de garantia.

Manifestação desta equipe de planejamento: Assegurar que as obrigações atinentes às atualizações de software e de firmware estejam ricamente detalhadas no Termo de Referência e que a Minuta de Contrato faça remissão a tais obrigações.

Níveis de Severidade :

Questionar a área técnica sobre a necessidade de detalhar melhor os níveis de severidade (ex.: indisponibilidade total ou parcial dos produtos).

Manifestação desta equipe de planejamento: Assegurar que os níveris de severidade de incidentes e respectivos prazos de atendimento esteam ricamente detalhados no Termo de Referência e que a Minuta de Contrato faça remissão a tais obrigações.

Padronização de Prazos :

Uniformizar os prazos mencionados no edital e anexos (ex.: "contados da data de abertura do Pregão").

Manifestação desta equipe de planejamento: Revisar e alinhar os prazos nos documentos.

3. Outras Providências

Estimativa de Preços :

Garantir que a estimativa de preços seja baseada em múltiplas fontes de pesquisa de mercado, conforme jurisprudência do TCU.

Manifestação desta equipe de planejamento: Confirmar a adequação da metodologia utilizada, sob a luz das exigências da Lei 14.133/2021

Subcontratação :

Manter a vedação à subcontratação integral ou parcial do objeto, conforme item 13 do TR.

Manifestação desta equipe de planejamento: Assegurar que as limitações de subcontratação estejam claramente registrada no ETP, TR e Edital.

Revogação de Processos Anteriores :

Cancelar processos anteriores (SEI 2017.00.000008300-1 e SEI 2017.00.000008899-2) que foram substituídos ou tornados prejudicados.

Manifestação desta equipe de planejamento: Realizar pesquisa sobre outros eventuais processos que tratem do mesmo objeto e formizar seu cancelamento, caso existam.

Decretos Revogados :

Observar que o Decreto nº 10.024/2019 revogou os Decretos nº 5.450/2005 e nº 5.504/2005, sendo necessário ajustar o edital aos novos termos.

Manifestação desta equipe de planejamento: Realizar revisão da legislação e normas eventualmente citadas no ETP e TR, a fim de não relacionar aqueles que já tiverem sido

revogados e citar versões atualizadas destas.

Quanto ao Parecer ASJUR 588 (1167810)

Este Parecer Jurídico complementar destaca a necessidade de ajustes adicionais na minuta de edital e seus anexos, com foco em justificativas para garantias técnicas, padronização textual, inclusão de cláusulas específicas e alinhamento às normas vigentes. Vejamos:

1. Aspectos Legais e Regulatórios

Justificativa para Garantia Técnica de 60 Meses :

O Termo de Referência inicialmente previa garantia técnica de 48 meses, mas foi alterado para 60 meses, alinhando-se às cotações de preços e ao estudo preliminar.

Contudo, há necessidade de justificar a exigência de garantia de 60 meses com base no mercado, pois essa decisão pode onerar a contratação.

Providência: A área demandante deve apresentar justificativa detalhada sobre a viabilidade e competitividade do período de garantia no mercado.

Assinaturas no Termo de Referência :

A Instrução Normativa nº 1/2019 exige que o TR seja assinado pela Equipe de Planejamento da Contratação, pela autoridade máxima da Área de TIC e aprovado pela autoridade competente (Diretor-Geral).

Embora a aprovação pelo Diretor-Geral ainda não seja obrigatória no âmbito do Tribunal Superior Eleitoral (TSE), é recomendável como boa prática.

Providência: Garantir que o TR atenda aos requisitos formais de assinatura e aprovação.

Revogação de Decretos Anteriores :

O Decreto nº 10.024/2019 revogou os Decretos nº 5.450/2005 e nº 5.504/2005, sendo necessário ajustar o edital aos novos termos.

Providência: Alinhar o edital às disposições do Decreto nº 10.024/2019.

2. Ajustes na Minuta de Edital e Anexos

A) Minuta do Termo de Referência (TR)

Correções Textuais e Padronização :

Foram corrigidos diversos erros de digitação e inconsistências textuais apontados no Parecer anterior (ex.: "Contrato 88/2018" para "Contrato 88/2015", "Checkpoint" para "Check Point").

Providência: Confirmar que todas as correções foram implementadas.

Garantia Técnica e Suporte :

O período de garantia técnica foi ajustado para 60 meses, conforme as cotações de preços.

Foi incluída cláusula para responsabilizar a contratada por todas as despesas geradas pelo suporte técnico durante o período de garantia.

Providência: Revisar se a redação final atende às necessidades técnicas e legais.

Atualizações de Software :

A área técnica entendeu que não é necessário disponibilizar atualizações de software tão logo ocorram seus lançamentos, pois isso pode exigir planejamento prévio.

Providência: Assegurar que as necessidades de atualização de software (a exemplo de prazos) estejam claramente definidas no Termo de Referência.

Tabela de Infrações :

Foi incluído um novo item na tabela de infrações: “Deixar de cumprir determinação formal ou instrução dos fiscais ou Comissão de Recebimento, limitado a 5 ocorrências”.

Providência: Assegurar que as alterações eventualmente realizadas em ETP e/ou TR sejam harmonizadas com o Edital.

B) Minuta do Contrato

Garantia Técnica de 60 Meses :

Assim como no TR, a minuta de contrato também prevê garantia técnica mínima de 60 meses.

Providência: Justificar a exigência com base no mercado e verificar a viabilidade financeira.

Cláusulas de Atualização e Suporte :

As cláusulas relativas a atualizações de software e firmware foram mantidas sem alterações, com base na justificativa da área técnica.

Providência: Confirmar que a redação atende às necessidades do TSE.

3. Outras Providências

Discrepâncias Detectadas :

Foi identificada discrepância entre o TR, o estudo preliminar e as cotações de preços quanto ao período de garantia técnica.

Providência: Harmonizar os documentos para evitar inconsistências.

Definições Claras :

A área técnica substituiu expressões subjetivas (ex.: "satisfatória") por definições mais objetivas nos itens do TR.

Providência: Revisar os ajustes para garantir clareza e objetividade.

Padronização de Prazos :

Os prazos mencionados no edital foram uniformizados, eliminando divergências entre dias úteis e feriados.

Providência: Confirmar que todos os prazos estão consistentes.

Parecer ASJUR 643 (1186322)

O Parecer Jurídico em questão trata da análise de uma minuta de edital para aquisição de uma Solução de Segurança (firewall em cluster de alta disponibilidade) destinada à atualização tecnológica do parque de segurança da Justiça Eleitoral. Este parecer complementa análises anteriores, abordando ajustes realizados no Termo de Referência (TR), na minuta de edital e no contrato, com foco na aplicação da disciplina prevista no § 4º do art. 21 da Lei nº 8.666/1993.

Este Parecer Jurídico destaca a obrigatoriedade de republicação do edital e reabertura do prazo inicial, independentemente da natureza das alterações realizadas. As principais providências incluem: exclusão de exigências documentais, adequação ao Decreto nº 10.024/2019 e observância das normas sobre alterações no instrumento convocatório.

Abaixo estão elencadas as principais recomendações e providências exigidas no Parecer.

1. Aspectos Legais e Regulatórios

Alterações no Edital e Reabertura de Prazo :

Conforme o § 4º do art. 21 da Lei nº 8.666/1993, qualquer modificação no edital exige divulgação pela mesma forma que o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando a alteração não afetar a formulação das propostas.

Providência: Caso haja necessidade de republicação, há de ser respeitado prazo estabelecido na Lei 14.133/2021.

Revogação de Decretos Anteriores :

O Decreto nº 10.024/2019 revogou os Decretos nº 5.450/2005 e nº 5.504/2005, sendo necessário ajustar o edital aos novos termos.

Providência: Assegurar que o Edital esteja alinhado às disposições do Decreto nº 10.024/2019.

2. Ajustes na Minuta de Edital e Anexos

A) Termo de Referência (TR)

Exclusão de Exigências Documentais :

A COINF excluiu a exigência constante do subitem 5.1.4 do Capítulo 5 do TR, atendendo a solicitação da empresa Pisontec Comércio e Serviços em Tecnologia da Informação EIRELI.

Providência: Assegurar que haja harmonizção entre ETP, TR, Edital e Minuta de Contrato.

Alterações em Conformidade com o Decreto nº 10.024/2019 :

Foram efetuadas alterações na minuta de edital para adequação ao novo decreto, já analisadas nos Pareceres nº 618/2019 e nº 613/2019.

Providência: Assegurar que haja harmonizção entre ETP, TR, Edital e Minuta de Contrato.

B) Minuta de Edital

Suspensão da Licitação :

A licitação fora suspensa conforme aviso de suspensão (SEI 1186196).

Providência: Aguardar a republicação do edital após as modificações necessárias.

Republicação e Reabertura de Prazo :

Mesmo que as alterações reduzam exigências ou ampliem o universo de competidores, é obrigatória a republicação do edital e a reabertura do prazo inicial, conforme entendimento do TCU (Acórdão nº 1197/2010).

Providência: Caso haja necessidade de republicação, há de ser respeitado prazo estabelecido na Lei 14.133/2021.

4.3 Fase Externa da Licitação (questionamentos, pedidos de impugnação, diligências, inabilitações, recursos etc)

Questionamentos formulados pela empresa NEC (SEI 1175931):

1. Conforme edital, página 25, item “3.5.6. Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS e TLS”, entendemos que não é requerido a função de AntiSpam para o equipamentos de Firewall, então o protocolo SMTP pode ser desconsiderado deste item. O nosso entendimento está correto?

Não. O entendimento não está correto.

É necessário suporte ao protocolo SMTP de modo que a solução de firewall possa encaminhar arquivos recebidos por correio eletrônico para análise pela solução Checkpoint Sandblast de propriedade do TSE, conforme item 3.5.4. "os appliances de firewall deverão ser capazes e estar licenciados para enviar, de forma automática, arquivos trafegados para análise na solução Check Point Sandblast em uso atualmente no Tribunal Superior Eleitoral".

No entanto, o Edital não exige a funcionalidade de antispam para os equipamentos de firewall.

2. Conforme edital, página 26, item “3.5.10. Implementar e identificar existência de malware em anexos de email e URL ´s conhecidas ”, entendemos que não é requerido a função de AntiSpam para o equipamentos de Firewall, então o texto “anexos de e-mail” pode ser desconsiderado deste item. O nosso entendimento está correto?

Não. O entendimento não está correto.

A identificação de malwares existentes em anexos de e-mail ocorrerá por meio do encaminhamento do arquivo para a solução Checkpoint Sandblast de propriedade do TSE, conforme item 3.5.4. "os appliances de firewall deverão ser capazes e estar licenciados para enviar, de forma automática, arquivos trafegados para análise na solução Check Point Sandblast em uso atualmente no Tribunal Superior Eleitoral".

Conforme já dito anteriormente, o Edital não exige a funcionalidade de antispam para os equipamentos de firewall.

3. Conforme edital, página 26, item “3.5.17. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP”, entendemos que não é requerido a função de AntiSpam para o equipamentos de Firewall, então o texto “Message Transfer Agent (MTA)” pode ser desconsiderado deste item. O nosso entendimento está correto?

Não. O entendimento não está correto.

A solução de firewall deverá atuar tanto de forma Inline, quanto como Message Transfer Agent (MTA) e suportar Mirror/TAP, de modo a permitir o encaminhamento de arquivos para a solução Checkpoint Sandblast de propriedade do TSE, conforme item 3.5.4. "os appliances de firewall deverão ser capazes e estar licenciados para enviar, de forma automática, arquivos trafegados para análise na solução Check Point Sandblast em uso atualmente no Tribunal Superior Eleitoral".

4. Conforme edital, página 26, item “3.5.26. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, HTTPS, SMTP)”, entendemos que não é requerido a função de AntiSpam para o equipamentos de Firewall, então o protocolo “SMTP” pode ser desconsiderado deste item. O nosso entendimento está correto?

Não. O entendimento não está correto.

É necessário suporte ao protocolo SMTP de modo que a solução de firewall possa encaminhar arquivos recebidos por correio eletrônico para análise pela solução Checkpoint Sandblast de propriedade do TSE, conforme item 3.5.4. "os appliances de firewall deverão ser capazes e estar licenciados para enviar, de forma automática, arquivos trafegados para análise na solução Check Point Sandblast em uso atualmente no Tribunal Superior Eleitoral".

Conforme já dito anteriormente, o Edital não exige a funcionalidade de antispam para os equipamentos de firewall.

5. Conforme edital, página 28, item “3.6.42. Deverá possibilitar a criação ou migração de assinaturas customizadas no formato SNORT e/ou Suricata”, entendemos que solução ofertada deve permitir a criação e/ou customização de assinaturas de IPS, opcionalmente podendo importar assinaturas de padrão SNORT e/ou Suricata O nosso entendimento está correto?

Não. O entendimento não está correto.

Conforme o item questionado, é necessário que a solução suporte assinaturas no formato SNORT ou Suricata ou ambos os formatos.

6. Conforme edital, página 28, item “3.6.43. Suportar o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, SMB/CIFS e SMTP”, entendemos que não é requerido a função de AntiSpam para o equipamentos de Firewall, então o protocolo “SMTP” pode ser desconsiderado deste item. O nosso entendimento está correto?

Não. O entendimento não está correto.

A solução deve ser capaz de bloquear arquivos contaminados por vírus e spywares recebidos por e-mail, utilizando o protocolo SMTP.

Considerações da equipe de planejamento:

Pelo que se observa dos aspectos técnicos dos questionamentos, estes não consistiram de duvidas ou mal entendimento das exigências editalícias, mas sim de uma tentativa de que fossem desconsideradas exigências de compatibilidade com outras soluções existentes no TSE.

Questionamentos formulados pela empresa Exceed Partners (SEI 1178388 e 1179215):

1. Conforme item “3.5.4. Os appliances de firewall deverão ser capazes e estar licenciados para enviar, de forma automática, arquivos trafegados para análise na solução Check Point Sandblast em uso atualmente no Tribunal Superior Eleitoral. O ambiente do TSE possui instalado 5 (cinco) equipamentos Check Point Sandblast;”. Entendemos que somente o fabricante Check Point atende o requisito, por isso solicitamos a retirada do item do edital. Nosso entendimento está correto?

Não, o entendimento não está correto.

O item em questão, assim como diversas outras exigências do Termo de Referência, destina-se a assegurar a integração dos equipamentos ao ambiente de datacenter do TSE.

Seria inadequado para o TSE ter que adaptar o ambiente de datacenter ao produto a ser fornecido pelos licitantes. O correto é que a solução fornecida seja integrada ao ambiente.

Outrossim, a solução Check Point Sandblast suporta implantação com gateways Check Point de forma nativa, mas também suporta o uso do protocolo ICAP, conforme manual (https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm topic .= documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/190309), garantindo assim a integração com produtos de terceiros. Caso a implantação seja realizada através do protocolo ICAP, deverão ser fornecidos todos produtos e licenças necessários para o funcionamento em conjunto com a solução Check Point SandBlast.

2. Conforme item “3.5.5. A solução deve ser capaz de bloquear uma conexão até que a classificação da mesma seja completada;”. Entendemos que somente o fabricante Check Point atende o requisito, por isso solicitamos a retirada do item do edital. Nosso entendimento está correto?

Não, o entendimento não está correto.

O item em questão, assim como diversas outras exigências do Termo de Referência, destina-se a assegurar a integração dos equipamentos ao ambiente de datacenter do TSE.

Seria inadequado para o TSE ter que adaptar o ambiente de datacenter ao produto a ser fornecido pelos licitantes. O correto é que a solução fornecida seja integrada ao ambiente.

Outros fabricantes também possuem mecanismos para bloqueio de conexões durante o processo de classificação de forma nativa ou através de conjunto de produtos, a exemplo dos fabricantes a seguir:

Fortinet: https://help.fortinet.com/fsandbox/cli-olh/2-5-0/index.htm - fortimail-expired: Enable/Disable expired timeout option for FortiMail files. By default, FortiMail will hold a mail for set period to wait for the verdict from FortiSandbox. When FSA scans an attachment or URL from FortiMail, it will check if the verdict is still needed as FortiMail might already have already released the email. If not, the scan will have an Unknown rating and skipped the status. Users

can run this command to enable or disable this expiration check.

Fabricante Forcepoint: https://www.websense.com/content/support/library/email/hosted/admin_guide/email_threat_analysis . as.px - Select the analysis mode you wish to use:Enforce holds any messages with attachments sent for analysis, and then quarantines those messages found to contain malicious attachments.

3. Conforme item “3.5.17. A solução deve suportar as seguintes topologias de implantação: Inline, Message Transfer Agent (MTA) e Mirror/TAP;”. Entendemos que somente o fabricante Check Point atende o requisito, por isso solicitamos a retirada do item do edital. Nosso entendimento está correto?

Não, o entendimento não está correto.

O item em questão, assim como diversas outras exigências do Termo de Referência, destina-se a assegurar a integração dos equipamentos ao ambiente de datacenter do TSE.

Seria inadequado para o TSE ter que adaptar o ambiente de datacenter ao produto a ser fornecido pelos licitantes. O correto é que a solução fornecida seja integrada ao ambiente.

Outros fabricantes também suportam tais topologias de implantação nativamente ou através de conjunto de produtos.

Fabricante Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf - Página 4: Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions - Integrated mode with FortiMail: SMTP, POP3, IMAP - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB.

Fabricante Cisco: https://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html - Cisco AMP for Networks builds on the Cisco Firepower Next-Generation Intrusion Prevention System NGIPS. When the system is deployed in line, it detects and blocks client-side exploit attempts that can lead to malicious file downloads, commonly referred to as drive-by attacks. https://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/data-sheet-c78-729751.html - Cisco Email Security Appliance now includes Cisco Advanced Malware Protection. It offers file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the email gateway. Users can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly. Advanced Malware Protection is available to all Email Security Appliance customers as an additionally licensed feature. https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01011010.html - Passive Interfaces on the Firepower System: You can configure one or more physical ports on a managed device as passive interfaces.

4. Conforme item “3.6.42. Deverá possibilitar a criação ou migração de assinaturas customizadas no formato SNORT e/ou Suricata;”. Entendemos que somente o fabricante Check Point atende o requisito, por isso solicitamos a retirada do item do edital. Nosso entendimento está correto?

Não, o entendimento não está correto.

O item em questão, assim como diversas outras exigências do Termo de Referência, destina-se a assegurar a integração dos equipamentos ao ambiente de datacenter do TSE.

Seria inadequado para o TSE ter que adaptar o ambiente de datacenter ao produto a ser fornecido pelos licitantes. O correto é que a solução fornecida seja integrada ao ambiente.

Outros fabricantes também suportam assinaturas criadas no padrão SNORT ou SURICATA, conforme demonstrado a seguir.

Fabricante Cisco: https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/117924-technote-firesight-00.html.

Fabricante Forcepoint: https://support.forcepoint.com/KBArticle?id=How-to-use-Firewall-Enterprise-user-defined-IPS-signatures.

5. Entendemos que presente licitação tem por objeto a aquisição de Solução de Segurança para atualização do parque de segurança da Justiça Eleitoral, contemplando o fornecimento de Firewall em um cluster de alta disponibilidade, pelo prazo de 12 (doze) meses, contemplando neste período a garantia e suporte técnico, está correto nosso entendimento?

Não, o entendimento não está correto.

O prazo de 12 (doze) meses indicado no Objeto do Edital diz respeito à vigência do contrato. O prazo de garantia e suporte técnico deverá ser de, no mínimo, 60 (sessenta) meses, conforme especificado no item 4.3: "O período de Garantia Técnica deverá ser de, no mínimo, 60 (sessenta) meses, e será contado a partir da data de recebimento definitivo do(s) equipamento(s) e/ou software(s)." Durante o período de 60 meses da garantia deverão ser prestados todos os serviços indicados na Seção 4 do Termo de Referência - Anexo I do Edital.

Considerações da equipe de planejamento:

Pelo que se observa dos aspectos técnicos dos questionamentos, estes não consistiram de duvidas ou mal entendimento das exigências editalícias, mas sim de uma tentativa de que fossem desconsideradas exigências de compatibilidade com outras soluções existentes no TSE.

Questionamento formulado pela empresa Pisontec (SEI 1182576):

1. Diante de todo o exposto, em respeito aos princípios da Legalidade, da Ampla Concorrência e da Isonomia, entendemos que, tendo em vista a afronta à legislação vigente, bem como ao entendimento do TCU e da SEFTI, não se aplica o subitem 2.4.1 transcrito acima, no sentido de exigir documentação específica de comprovação. Está correto o nosso entendimento?

Sim. O entendimento está correto. O subitem 2.4.1. do Capítulo VIII do Edital não deverá ser aplicado à contratação em questão.

Considerações da equipe de planejamento:

O item 2.4.1 do Capítulo VIII do Edital dizia respeito a apresentação, dentre os documentos da proposta da licitante, de declaração de comprovação de parceria com o fabricante, através de declaração emitida pelo fabricante, ou documento impresso pelo site do fabricante ou Contrato de Distribuição.

Por se tratar de documentação não prevista na lei 14.133/2021, não poderá ser exigida dentre os documentos a serem apresentados no pregão. A interrupção do pregão e ajuste do Edital foi acertada à época.

A equipe de planejamento deverá se atentar para que nenhum documento não previsto em lei seja exigido na presente contratação.

4.4 Execução Contratual (dificuldades e problemas identificados)

Não foram identificadas ressalvas ou dificuldades.

4.5 Diferenças em relação à última contratação (especificação e quantidades)

Não há diferenças em relação à última contratação. Vejamos:

Conforme é possível observar no site do fabricante (https://www.checkpoint.com/support-services/support-life-cycle-policy/), os equipamentos 16200 sucederam a série 23500. E, por dua vez, a geração 19200 sucedeu a série 16200.

Assim, a atualização tecnológica pretendida consiste da substituição dos 4 equipamentos 23500 por outros 4 equipamentos equivalentes, de geração atual, qual seja: o modelo 19200.

Appliance Product/Model	Status	General Availability	End of Sale	Successor Model	Successor Product Availability	End of Engineering Support	End of Support	Supported Software Versions
21400 Appliance	Active	Aug-2011	Jun-2017	15600	Jan-2016	Jun-2020	Jun-2022	R80.40, R80.30, R80.20, R80.10, R77, R76, R75
21600 Appliance	Active	Oct-2012	31-Oct-2014	21700	Feb-2013	31-Oct-2017	31-Oct-2019	R80.30, R80.20, R80.10, R77, R76, R75
21700 Appliance	Active	Feb-2013	Jun-2017	23500	Jan-2016	Jun-2020	Jun-2022	R80.40, R80.30, R80.20, R80.10, R77, R76, R75
21800 Appliance	Active	Jul-2014	Jun-2017	23800	Jan-2016	Jun-2020	Jun-2022	R80.40, R80.30, R80.20, R80.10, R77.30, R77.20*, R75.47*
23500 Appliance	Active	Jan-2016	Dec-2020	16200	Apr-2020	June-2024	Dec-2025	R82, R81.20, R81.10, R81, R80.40, R80.30, R80.20, R80.10, R77.30*
16000 Appliance	Active	Jun-2019	Mar-2022	16200	May-2020	Mar-2025	Mar-2027	R80.30, R80.40, R81, R81.10, R81.20, R82
16200 Appliance	Active	May-2020	N/A	19200	Jan-2024			R80.30*, R80.40*, R81, R81.10, R81.20, R82
16600 HS	Active	April-2020	N/A	19200	Jan-2024			R80.30*, R80.40*, R81, R81.10, R81.20, R82

4.6 Necessidade de transição contratual

Não há necessidade de realização de transição contratual, considerando-se a expertise da equipe técnica do TSE na tecnologia pretendida.

CAPÍTULO 5. VALOR ESTIMADO DA CONTRATAÇÃO

Item	Descrição	Unidade	Quantidade	Valor unitário	Valor Total
1	Aquisição de Appliance de firewall Check Point modelo 19200 ou superior, com licenciamento de softwares para habilitação de todas as funcionalidades de prevenção de ameaças (threat prevention), respectivos acessórios para instalação e conexão dos equipamentos à rede do TSE e garantia de 60 meses. Account ID do TSE: 0008229609	unidade	4	R$ 1.586.918,50	R$ 6.347.674,00

A estimativa de preços acima foi realizada com base no Pregão 90906/2024 SERPRO (UASG: 803080), cuja documentação desse pregão está disponível em https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/-2?compra=80308005909062024

O item 1 desse Pregão foi vencido pela empresa NTSec, a qual ofertou oito pares (clusters) de

Firewall Check Point modelo 19200 com garantia de 60 meses.

Cada par de Firewall Check Point foi ofertado pela NTSec a um valor de R$ 3.173.837,00. Assim, cada Firewall Check Point 19200, com garantia de 60 meses, custou R$ 1.586.918,50.

Observação: Devido à grande capacidade de processamento necessária para o atendimento ao TSE, não é comum encontrar contratações que se utilizem de equipamentos de dimensões/capacidades similares à necessária ao TSE.

Até a data de conclusão deste estudo técnico preliminar, dentre os Pregões realizados nos últimos 12 meses, apenas o citado acima teve por objeto um equipamento equivalente ao pretendido pelo TSE.

CAPÍTULO 6. DIVISIBILIDADE DA SOLUÇÃO

A contratação ora pretendida consiste do fornecimento de quatro unidades do mesmo equipamento idênticos.

A solução proposta para a aquisição dos firewalls não é passível de divisibilidade, uma vez que a contratação consiste no fornecimento de quatro unidades idênticas do mesmo equipamento. A padronização dos dispositivos é essencial para garantir compatibilidade, interoperabilidade e facilitar a gestão técnica da infraestrutura de segurança do Tribunal Superior Eleitoral (TSE). Fracionar o fornecimento desses equipamentos, dividindo a responsabilidade entre empresas distintas, ensejaria um aumento desnecessário de riscos operacionais e complexidade na integração, além de potencializar inconsistências no suporte técnico e na aplicação de atualizações.

Portanto, a contratação centralizada de todos os equipamentos com um único fornecedor é a abordagem mais eficiente e segura para atender às necessidades do TSE, alinhando-se aos princípios de economicidade, segurança jurídica e eficiência previstos na Lei nº 14.133/2021.

CAPÍTULO 7. ASPECTOS ADMINISTRATIVOS RELACIONADOS

7.1 Exigências para seleção do fornecedor

a) Justificativas para inexigibilidade ou dispensa, se for o caso

Não se aplica.

b) Procedimentos auxiliares

Não se aplica.

c) Critério de julgamento das propostas

O julgamento das propostas deverá ocorrer mediante apresentação de menor preço.

d) Exigências de qualificação técnica profissional

Não se aplica.

e) Apresentação de amostras na fase de licitação e/ou prova de conceito

Não se aplica.

f) Vistoria prévia no local de execução dos serviços

A realização de vistoria técnica no local de execução dos serviços é recomendada, pois permite que a licitante tenha uma visão real do local de instalação dos firewall, garantindo que a empresa tenha ciência dos ambientes físicos e das condições operacionais que poderão influenciar o fornecimento.

A vistoria, contudo, não é obrigatória, cabendo à licitante avaliar a necessidade de sua realização. Caso opte por não realizá-la, a licitante assume integralmente os riscos decorrentes do desconhecimento das condições reais dos equipamentos e dos ambientes de instalação, não podendo alegar, posteriormente, desconhecimento de aspectos técnicos ou dificuldades não previstas para a adequada execução do contrato.

7.2 Regras de participação no procedimento de contratação

a) Subcontratação

	SIM
X	**NÃO**

b) Formação de Consórcio

X **SIM**
NÃO

Não há limite para o número de empresas consorciadas.

c) Participação de cooperativas

X **SIM**
NÃO

d) Participação de empresas estrangeiras

X **SIM**
NÃO

Justificativa caso a resposta seja "não":

e) Participação de pessoa física

SIM
X **NÃO**

Justificativa caso a resposta seja "não":
Por se tratar de contratação com valor estimado superior a R$250.000,00.

7.3 Particularidades da contratação

a) Necessidade de assinatura de termos de ciência e confidencialidade

Durante a execução do contrato, a empresas contratada terá acesso a informações sensíveis da infraestrutura de tecnologia do Tribunal Superior Eleitoral (TSE), incluindo a arquitetura da rede de comunicação de dados, endereçamento IP, segmentação de rede e demais aspectos estratégicos relacionados à segurança da informação. Em razão da criticidade desses dados, será exigida a assinatura de um Termo de Sigilo e Confidencialidade por parte da contratada, comprometendo-se a adotar todas as medidas necessárias para a proteção das informações acessadas.

A empresa contratada não poderá divulgar, reproduzir, compartilhar ou utilizar, para qualquer finalidade alheia à execução do contrato, as informações obtidas durante a prestação dos serviços, sob pena de aplicação das sanções previstas no contrato e na legislação vigente. Além disso, deverá garantir que seus empregados, prepostos e eventuais subcontratados tenham ciência dessa obrigação, adotando práticas adequadas de controle e proteção dos dados sensíveis da Administração.

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

Não é aplicável o Sistema de Registro de Preços.

b) Preços diferentes para o mesmo item

Não é aplicável o Sistema de Registro de Preços.

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

Não é aplicável o Sistema de Registro de Preços.

d) Possibilidade de adesão futura

Não é aplicável o Sistema de Registro de Preços.

CAPÍTULO 8. INFORMAÇÕES COMPLEMENTARES

8.1 Previsão no Plano de Contratações Anual (PCA)

A presente contratação está prevista no Plano de Contratações Anual 2025 sob código **STI_16**.

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

Não foram identificadas restrições.

8.3 Acessibilidade

A contratação dos novos firewalls não envolve, diretamente, o atendimento ao público ou a necessidade de adaptação de infraestrutura física para acessibilidade. No entanto, a Administração assegurará que eventuais interações presenciais da equipe contratada com os setores internos do Tribunal Superior Eleitoral (TSE) ocorram em ambientes acessíveis, garantindo que profissionais com deficiência ou mobilidade reduzida possam exercer suas atividades sem restrições.

Caso haja necessidade de deslocamento da equipe da contratada para a execução dos serviços em locais físicos do TSE, será exigido que a empresa adote medidas que garantam a acessibilidade de seus profissionais, conforme previsto na legislação vigente. Além disso, qualquer sistema, documentação ou relatório produzido no âmbito da contratação deverá ser disponibilizado em formato acessível, quando aplicável, garantindo a plena inclusão de servidores e colaboradores com deficiência que necessitem dessas informações.

8.4 Classificação Contábil (contratação de softwares)

Não se aplica.

8.5 Outras observações

Não se aplica.

CRISTIANO MOREIRA ANDRADE
COORDENADOR(A) DE INFRAESTRUTURA

Documento assinado eletronicamente em **25/04/2025, às 14:35**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

MAURO SANS JUNIOR
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **25/04/2025, às 16:07**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

ALEXANDRE DE JESUS PASCHOAL
TÉCNICO(A) JUDICIÁRIO(A)

Documento assinado eletronicamente em **28/04/2025, às 19:00**, 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=3211788&crc=51FD0766, informando, caso não preenchido, o código verificador **3211788** e o código CRC **51FD0766**.
