TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
COORDENADORIA DE INFRAESTRUTURA
SEÇÃO DE SUPORTE ÀS REDES LOCAIS

ESTUDO TÉCNICO PRELIMINAR

I – IDENTIFICAÇÃO DA DEMANDA - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO [Lei 14.133/21 - Art. 18, § 1º, inciso I]

Como forma de contextualização, é importante reforçar algumas nomenclaturas e conceitos que serão abordados no decorrer deste Estudo Preliminar:

1. Appliance: Palavra da língua inglesa, utilizada neste conceito para referenciar equipamentos (hardware) que desempenham determinada função;

2. Firewalls: É um equipamento que controla e avalia todo o tráfego que entra e sai da organização para o ambiente externo.

3. Cluster de Firewall: Dois equipamentos firewall trabalhando em conjunto oferecendo redundância e alta disponibilidade.

4. HA – HIGHT AVAILABILITY: Permitir que o acesso à base de dados do TRE-RJ, aos dispositivos ou às entidades autorizadas estejam sempre disponíveis e, conseqüentemente, não haja prejuízo à execução das atividades de servidores e de usuários em geral.

5. Next Generation Firewall: Um firewall de próxima geração (NGFW) aumenta a tecnologia de firewall tradicional com outras funções de filtragem de dispositivos de rede, como controle de aplicativos em linha, um sistema integrado de prevenção de invasões (IPS), recursos de prevenção de ameaças e proteção avançada contra malware, para melhorar a segurança da rede corporativa.

I.1 Diante do avanço constante da tecnologia cibernética, os hackers vêm desenvolvendo continuamente novas técnicas de ataques maliciosos, visando redes corporativas de instituições públicas e privadas. O objetivo desses ataques é sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e essenciais. Os criminosos virtuais, com objetivos obscuros, chegam a manter informações criptografadas como reféns, exigindo resgates em cripto moeda ou utilizando indevidamente tais informações para vantagens próprias.

I.2 Juridicamente, o Judiciário brasileiro, como um todo, vem elaborando normas governamentais, no âmbito da segurança da informação, como a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), e a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Estas normas, dentre outras, vêm impulsionando investimentos em recursos tecnológicos para garantir a proteção dos dados e das informações do Judiciário contra acessos não autorizados, garantindo a confidencialidade, integridade e disponibilidade das informações.

I.3 Consciente deste problema de segurança da informação, a Justiça Eleitoral vem promovendo constantes modernizações e ampliações dos recursos de Tecnologia da Informação, aumentando a proteção da rede, dos dados trafegados e da privacidade dos colaboradores.

I.4 O firewall é uma das ferramentas tecnológicas mais importantes para a segurança da informação de qualquer ambiente computacional em rede interligado à Internet. Trata-se de um elemento de controle e policiamento de tráfego de dados que permite o bloqueio de conexões indesejadas em uma rede de computadores. Com base em políticas definidas, o firewall garante que somente as conexões permitidas sejam estabelecidas. Por este motivo, é um elemento

caracterizado como crítico para o negócio e sua ausência ou funcionamento inadequado enseja em altíssimo risco para a segurança da informação.

I.5 O TRE-RJ começou a utilizar uma solução de Next Generation Firewall que combina hardware e software, do fabricante Check Point há mais de 12 anos, quando o TSE disponibilizou na ocasião Firewalls aos regionais deste fabricante.

I.6 Especificamente no TRE-RJ, há mais de 10 anos, a proteção de perímetro da infraestrutura de TI da Justiça Eleitoral fluminense, dos dados e das informações, bem como o controle do acesso à Internet, têm sido realizados pelo Fabricante Check Point Software Technologies Ltd. Esta solução de segurança da informação é constituída por hardware e software (Firewalls), e tem como objetivo a proteção da rede de computadores do Tribunal, funcionando como um filtro de segurança que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção configurados.

I.7 Essa solução também possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), entre outros, garantindo a checagem do conteúdo acessado na Internet pelos usuários, contribuindo com a proteção dos componentes envolvidos contra ameaças que podem interromper o funcionamento dos computadores da rede local e causar a indisponibilidade de atividades precípuas e acessos aos dados e sistemas do Tribunal.

I.8 Durante este 10 anos de utilização da solução da Checkpoint na Justiça eleitoral fluminense, o TRE-RJ sempre contou com o suporte técnico qualificado do Fabricante e Revenda que vêm garantindo que a infraestrutura de segurança permaneça com o seu funcionamento adequado de acordo com as melhores práticas, e impedindo que tentativas de ataques cibernéticos ao TRE-RJ venham prosperar.

I.9 Como já informado, o Fabricante Check Point anunciou que os equipamentos utilizados atualmente no TRE-RJ estão fora de venda, ou seja, não há mais suporte para a arquitetura aos Firewall 15.600 e 1430, e justamente por isto, devido à significativa importância do objeto, há necessidade de uma nova aquisição.

I.2 Demandas:

I.2.1 Substituição dos equipamentos Firewalls na sede da Av. Presidente Wilson judiciárias e aquisição de 10 (dez) Firewalls para Justiça Itinerante.

I.2.2 Trata-se de estudos relativos à necessidade do TRE-RJ na substituição dos Firewalls 15.600 da Checkpoint na sede da Av. Presidente Wilson e dos Firewalls 1430 da Checkpoint utilizados para Justiça Itinerante.

I.2.3 Atualmente o TRE-RJ possui o Contrato 031/2022 com a Empresa Contacta Segurança em Conectividade LTDA que realiza a prestação de serviço de renovação da garantia e licenciamento da solução em Cluster de Firewall, modelo 15.600, que possui importância estratégica ao TRE-RJ, com vigência de 60 meses, sendo que as licenças de segurança dos atuais firewalls precisam ser renovadas por mais 30 meses a partir de 12/11/2024.

I.2.4 Os atuais equipamentos Firewalls instalados na sede não são mais comercializados pelo fabricante Checkpoint e não há mais suporte para este modelo (End of Support).

I.2.5 Dentro do item de segurança da informação que envolve a Comunicação de Dados adotada pela Justiça Eleitoral, é relevante frisar que com a aquisição destes equipamentos, será possível implementar, de forma segura, os mecanismos de acesso realizados pelos servidores que utilizam o Trabalho Remoto, Teletrabalho e Justiça Itinerante à base de dados do TRE-RJ.

I.2.6 Devido a importância que estes equipamentos possuem para a segurança da informação, será necessário a aquisição de 2 (dois) firewalls que ficarão operando como Cluster, oferecendo com isto a redundância operacional necessária para a infraestrutura de rede e comunicação de dados.

I.2.7 A Aquisição de 10 firewall para serem utilizados na Justiça Itinerante, para Ação Global, com modem 3G&4G

II – DATA PARA O ATENDIMENTO DA DEMANDA

01 de novembro de 2024.

III - CONEXÃO COM O PLANEJAMENTO EXISTENTE [Art. 18, § 1º, inciso II]

III.1 A aquisição está alinhada com o seguinte objetivo Estratégico do TRE-RJ 2021-2026: Promover a transformação digital (OE nº 12).

III.2 A aquisição também está alinhada com os macros desafios da Estratégia Nacional do Poder Judiciário para o período 2021- 2026, elaborado do CNJ (Conselho Nacional de Justiça), através da Resolução nº 211 de 20.10.2020 (Objetivo Estratégicos nº 4:Promover Serviços de Infraestrutura e Soluções Corporativas).

III.3 A contratação está prevista nos itens nº 12 do Plano Anual de Contratações, do ano de 2024.

IV - ESTIMATIVA DE QUANTIDADES E MEMÓRIA DE CÁLCULO, COM JUSTIFICATIVAS QUE AS RELACIONE À DEMANDA [Art. 18, § 1º, inciso IV]

Atualmente, na sede do TRE-RJ possui 2 equipamentos Firewalls modelo 15.600 do fabricante Checkpoint e Firewalls modelo 1430 a proposta é substitui-los pelos motivos a apresentados no subitem I.1 Demandas.

ITEM	UNIDADE	QUANTIDADE	ESPECIFICAÇÃO
1	Unidade	2	Equipamento Firewall do tipo Applaince que será especificado no Termo de Referencia para atender a Sede da Av. Presidente Wilson.
2	Unidade	2	Licenças FIREWALL, IPSEC VPN, IPS, Application Control, URL Filtering, Content Awareness, Anti-Virus, Anti-Bot, Anti-Spam & Email Security pelo prazo de 30 (trinta) meses, para os Firewalls da Sede da Av. Presidente Wilson.
3	Unidade	10	Equipamento Firewall do tipo Applaince que será especificado no Termo de Referência para atender a JUSTIÇA ITINERANTE.
4	Unidade	10	Licenças FIREWALL, IPSEC VPN, IPS, Application Control, URL Filtering, Content Awareness, Anti-Virus, Anti-Bot e Anti-Spam & Email Security, pelo prazo de 30 (trinta) meses, para atender aos Firewalls da JUSTIÇA ITINERANTE.
5	Unidade	1	Suporte técnico com instalação e configuração e treinamento
6	Unidade	1	Treinamento
7	Unidade	8	Transceivers 1000BASE-T RJ45

V - LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR [Art. 18, § 1º, inciso V]

V.1 Foram identificadas quatro alternativas para atender a demanda:

Solução 01 — Renovação do contrato dos serviços de licenças dos atuais Firewalls 15.600 e 1430 do fabricante Check Point instalados na sede do TRE.

a) Vantagens:

1) Somente seria necessário realizar despesas com a renovação das licenças, o que torna o investimento financeiro menor.

b) Desvantagens:

1) Todos os atuais equipamentos Firewalls estão defasados tecnologicamente e já não são mais comercializados.

2) Devido a término de suporte (End of Support) dos firewalls, a empresa Checkpoint não fornece mais suporte, comprometendo a velocidade nas soluções dos problemas para estes equipamentos exigem e a eficácia e eficiência do trabalho da justiça eleitoral.

Solução 02 -Aquisição de nova infraestrutura composta de 02 (dois) equipamentos appliances operando em cluster e 10 (dez) equipamentos appliances, com todos os hardwares, softwares e serviços de gerência integrados, baseado em tecnologia mais atualizada do fabricante **Check Point .**

a) Vantagens:

1) Equipamentos mais modernos com padrões de segurança maior do que os atuais Firewalls em operação.

2) A nova infraestrutura de Firewalls que operará em Cluster, estará ajustada a nova realidade relativa ao incremento de carga, devido aos aumentos de velocidades que estes equipamentos suportarão, conforme descrito abaixo:

a) A mudança das velocidades dos 2 (dois) acessos à internet de 500 Mbps para 1 Gb para cada, até o final do ano (SEI: 2024.0.000002086-2)

b) 1 (um) acesso Lan-to-Lan de 1Gb interligando as sedes da Av. Presidente Wilson e Rua da Alfândega;

c) Aumento da velocidade da infraestrutura de ligação com o TSE de 60 Mbps para 150 Mbps;

d) A interligação da concentradora SD-WAN do novo Backbone das unidades judiciárias (SEI 2023.0.000033549-2) através de pelo menos 2 (duas) conexões através da rede local com velocidade de 10 Gb, podendo haver aumento destas conexões de 10 Gb,

3) Ampliar o número de portas de fibra-ótica, eliminando com isto as restrições de ampliações de novas infraestruturas.

4) Esta aquisição garantirá o devido suporte técnico seja local ou remoto com operação assistida e resposta a incidentes de segurança.

5) Manter o mesmo fabricante permitirá aproveitar os investimentos realizados nos treinamentos básicos e avançados e na experiência técnica adquirida em práticas há mais de 10 anos seja em atendimento técnico a usuários bem como nos suportes assistidos pela empresa.

5.1) Com a continuidade do uso e a manutenção da mesma solução, a equipe de TI do TRE-RJ, já familiarizada com o sistema atual, não precisaria passar por treinamentos extensivos em uma nova solução, que inevitavelmente resultaria na perda de uma eficiência operacional já adquirida, e pela criticidade dos equipamentos de segurança da informação envolvidos.

b) Desvantagens:

1) Necessidade de um investimento maior para a solução proposta de Next Generation Firewall que combina hardware e software do fabricante Check Point.

Solução 03 - Locação de toda infraestrutura de Firewalls informadas na Solução nº 2, baseado em tecnologia mais atualizada.

a) Vantagens:

1) Somente seria necessário no orçamento mensal da empresa com valor fixo mais baixo do que seria o custo de uma compra efetiva.

b) Desvantagens:

1) Devido ao tipo dos equipamentos, softwares de gerência, softwares de segurança, incluindo o suporte e treinamento, a serem alugados e das condições previstas em contrato, a locação neste tipo de contrato não será tão vantajosa, pois quanto analisamos o cenário a longo prazo do valor do aluguel da solução adquirida. Isto acontece nos casos de infraestrutura que não são comuns no cotidiano, sendo que neste caso o seu valor de aquisição no mercado vale a pena devido a sua alta durabilidade.

2) Cada órgão tem as suas particularidades técnicas, ou seja, o tipo de infraestrutura que será solicitada, será exclusiva do TRE-RJ. Portanto, provavelmente a contratada terá que realizar um alto investimento para atender às rígidas condições técnicas e de funcionalidade deste tribunal. Portanto, não teremos empresas suficientes no mercado para atender a esta demanda, ao contrário das inúmeras revendas de fabricantes que poderão atender quando se trata de aquisição.

3) O risco de descontinuidade dos serviços decorrentes de descumprimento de contrato ou qualquer aspecto não previsto a priori, ensejaria paralisação da operação de toda comunicação de dados do TRE-RJ, pois nesta alternativa os equipamentos são de propriedade do fornecedor. Adicionalmente, o montante de equipamentos requeridos e a especificidades da demanda, dificultaria a adoção de medidas para suprir a necessidade emergencial em caso de rompimento contratual

Solução 04 -Aquisição de nova infraestrutura composta de 02 (dois) equipamentos appliances operando em cluster e 10 (dez) equipamentos appliances, com todos os hardwares, softwares e serviços de gerência integrados, baseado em tecnologia mais atualizada dos fabricantes **Palo Alto Networks**, **Cisco Sytems**, **Fortinet Inc**.

a) Vantagens:

1) Equipamentos mais modernos com padrões de segurança maior do que os atuais Firewalls em operação.

2) A nova infraestrutura de Firewalls que operará em Cluster, estará ajustada a nova realidade relativa ao incremento de carga, devido aos aumentos de velocidades que estes equipamentos suportarão, conforme descrito abaixo:

a) A mudança das velocidades dos 2 (dois) acessos à internet de 500 Mbps para 1 Gb para cada, até o final do ano (SEI: 2024.0.000002086-2)

b) 1 (um) acesso Lan-to-Lan de 1Gb interligando as sedes da Av. Presidente Wilson e Rua da Alfândega;

c) Aumento da velocidade da infraestrutura de ligação com o TSE de 60 Mbps para 150 Mbps;

d) A interligação da concentradora SD-WAN do novo Backbone das unidades judiciárias (SEI 2023.0.000033549-2) através de pelo menos 2 (duas) conexões através da rede local com velocidade de 10 Gb, podendo haver aumento destas conexões de 10 Gb,

3) Ampliar o número de portas de fibra-ótica, eliminando com isto as restrições de ampliações de novas infraestruturas.

4) Esta aquisição garantirá o devido suporte técnico seja local ou remoto com operação assistida e resposta a incidentes de segurança.

b) Desvantagens:

1) Necessidade de um investimento maior para a solução proposta de Next Generation Firewall que combina hardware e software dos fabricantes.

2) Entretanto, apesar destes fabricantes atuarem no mesmo segmento de segurança da informação, no combate a ameaças cibernéticas, cada um deles possui lógicas de funcionamento diferentes, ou seja, cada um possui sistema proprietário próprio, que precisa de anos para ser absorvido.

3) Podemos afirmar que apesar de alguns fabricantes de equipamentos afirmarem que seus produtos executam determinadas funcionalidades de acordo com os padrões definidos por instituições mundiais, na prática, é comum haver incompatibilidades técnicas ao optarmos por migrar para fabricantes distintos.

4) Alterar o fabricante de firewall pode trazer inúmeros impactos técnicos e operacionais com enormes prejuízos para o tribunal:

4.1. Curva de Aprendizado e Necessidade de Treinamento

4.1.1Curva de Aprendizado: A equipe de TI pode precisar de tempo para se familiarizar com a nova interface, funcionalidades e configurações do novo firewall. Isso pode resultar em uma queda na eficiência operacional durante o período de adaptação.

4.1.2 Necessidade de Treinamento: Será necessário investir em treinamento para a equipe nos níveis básicos, intermediário e avançado, o que pode aumentar os custos e tomar tempo que poderia ser usado em outras atividades.

4.1.2.1 Uma visão geral de diferentes cenários para a formação de especialista em firewall de um fabricante é a seguinte:

Formação Inicial: 1 a 2 anos.

Especialização Avançada: 2 a 4 anos.

Especialista Sênior: 5 a 7 anos.

Ressalvo, que esses tempos podem variar com a dedicação pessoal e oportunidades de trabalho específicas, mas fornecem uma visão geral de quanto tempo pode levar para formar um especialista em firewalls.

4.2. Interrupções no Serviço

4.2.1. **Downtime:** Durante a migração de um fabricante para outro, é comum que ocorram interrupções no serviço, o que pode afetar a disponibilidade de serviços críticos, especialmente em organizações que dependem de conectividade constante.

4.2.2 Incompatibilidade Temporária: Alguns serviços ou aplicativos podem enfrentar problemas de compatibilidade com o novo firewall até que sejam ajustados corretamente, o que pode causar falhas ou lentidão no sistema

4.3. Complexidade na Migração

4.3.1. Configurações e Políticas: Migrar regras, políticas de segurança e configurações de um fabricante de firewall para outro pode ser complexo. Ferramentas automatizadas nem sempre conseguem replicar configurações perfeitamente, exigindo ajustes manuais que podem ser demorados e suscetíveis a erros.

4.3.2. Problemas de Compatibilidade: Certos dispositivos ou softwares podem ser incompatíveis com o novo firewall de outro fabricante, exigindo modificações ou substituições adicionais na infraestrutura.

4.4. Impacto na Segurança

4.4.1. Perda de Funcionalidades Específicas: Cada fabricante de firewall oferece funcionalidades exclusivas. Ao trocar de fabricante, a organização pode perder funcionalidades ou capacidades que eram críticas para a segurança, aumentando os riscos de vulnerabilidades até que novas medidas sejam implementadas.

4.4.2. **Exposição Temporária a Riscos:** Durante a transição, pode haver um período em que as defesas não estão totalmente otimizadas, criando janelas de vulnerabilidade que podem ser exploradas por atacantes.

4.5. Custos Adicionais

4.5.1 Aquisição e Implementação: Além do custo de compra do equipamento de novo fabricante, há custos associados à instalação, configuração, e possível contratação de consultoria especializada para a transição.

4.5.2 Licenciamento e Suporte: Pode haver custos adicionais relacionados ao licenciamento de novas funcionalidades e suporte técnico especializado.

4.6. Mudança no Suporte Técnico

4.6.1 Dependência do Novo Fabricante: A organização passa a depender de um novo fornecedor para suporte técnico. Se o suporte oferecido pelo novo fabricante não for tão eficiente quanto o anterior, isso pode impactar a resolução de problemas e a agilidade na resposta a incidentes.

4.7. Integração com Outros Sistemas

4.7.1 Integração com Infraestrutura Existente: Com o novo firewall de outro fabricante existe a possibilidade de serem encontradas incompatibilidades na integração com os outros sistemas de segurança existentes, como os sistemas de detecção de intrusões, as soluções de monitoramento, ou a autenticação.

4.7.2 Mudanças na Arquitetura de Rede: Em alguns casos, a mudança de fabricante de firewall pode exigir alterações na arquitetura de rede para acomodar as novas tecnologias ou padrões de segurança, o que pode ser complexo e dispendioso.

B) SOLUÇÃO ESCOLHIDA

A escolha da melhor solução deverá ser concebida com base em requisitos técnicos e observar os objetivos e estratégias de negócio para o qual se propõe esta aquisição, bem como considerar as políticas de segurança, buscando as soluções estabelecidas nas normas informadas abaixo:

a) PORTARIA TSE, 456 de 13 de julho de 2021, que institui norma de uso aceitável de ativos de TI relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.

b) Resolução TSE nº 23.644 de 1º julho de 2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

c) PORTARIA TSE nº 455, DE 13 DE JULHO DE 2021, que institui norma de configuração segura de ambientes, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.

Além das normas acima, destacamos, também, as recomendações expedidas pelo Ministério da Economia, que indicam que o ciclo de vida de ativos de rede é de 5 (cinco) anos.

Foram considerados os seguintes aspectos:

a) A solução a ser adquirida deve prever a continuidade do atendimento aos princípios de segurança que já são suportados pela versão atual, garantindo a segurança da informação da Justiça Eleitoral Fluminense.

b) Não é vantajoso para a Administração, em razão do alto valor a ser despendido, realizar um novo contrato para manter equipamentos já defasados, ressaltando que toda a infraestrutura dos equipamentos está em uso neste Tribunal por mais de 5 (cinco) anos.

c) A solução adotada resultará em um ambiente de infraestrutura com equipamentos próprios, de forma a atender as necessidades específicas atuais e futuras deste Tribunal.

d) A solução escolhida manterá o ambiente das políticas de segurança da informação personalizadas para: usuários, grupos de usuários, servidores, estações de trabalho, portas, protocolos e aplicações.

e) Além de ampliação dos recursos da solução de segurança, há também a necessidade de expansão das funcionalidades, situação evidenciada pelas recentes recomendações de segurança, com o objetivo de se construir órgãos cada vez mais seguros e resilientes, fazendo frente às previsões de mercado quanto ao aumento dos ataques cibernéticos.

f) A solução a ser adquirida deve prever a continuidade do atendimento aos princípios de segurança que já são suportados pela versão atual, conforme abaixo:

f.1) Confidencialidade - o acesso para instalação, manutenção, configuração e desinstalação da ferramenta só deve ser permitido com uso de login e senha, no mínimo.

f.2) Disponibilidade - a solução deve garantir disponibilidade full-time quando as pré-condições para funcionamento estiverem sendo devidamente atendidas.

f.3) Integridade - a solução deve garantir que não haja risco de perda da integridade dos dados trafegados.

Considerando o que foi analisado o subitem V.1 e o que foi informado nos subitens I.1 e I.2 deste estudo preliminar, conclui-se que a melhor opção recai sobre a Solução 02 -Aquisição de nova infraestrutura composta de 02 (dois) equipamentos appliances operando em cluster e 10 (dez) equipamentos appliances, com todos os hardwares, softwares e serviços de gerência integrados, baseado em tecnologia mais atualizada do fabricante Check Point.

Justificativa em na escolha dos modelos dos Firewalls principais

Visando definir a melhor solução para substituição dos atuais Firewalls Principais 15.600, foram realizados análises sobre os modelos de equipamento Firewall Appliance CheckPoint que cumprissem com as nossas atuais necessidades, e com as previsões futuras que envolvem a expansão no quantitativo e nas velocidades dos circuitos de dados e serviços na Sede e nas Unidades Judiciárias.

Foi utilizada uma ferramenta da Checkpoint pela revenda a Contacta, empresa que presta suporte ao TRE relativo a Solução de Firewalls do TRE-RJ, que coletou dados trafegados na rede local de dados na Sede do TRE-RJ.

Foram coletados por alguns dias dados que nos informaram tecnicamente qual a opção de Firewall com as características mínimas necessárias para suprir a nossa atual e futura demanda. (Anexo I.1).

O objetivo principal da análise foi obter a melhor equação custo x benefício, assegurando o máximo retorno do capital investido, resultando na solução que ofereça maior confiabilidade e reduzindo custos não apenas na implantação, mas

principalmente na operação e na eventual ampliação da solução.

VI - DESCRIÇÃO COMPLETA DA SOLUÇÃO ESCOLHIDA [Art. 18, § 1º, inciso VII]

GRUPO	ITEM	DESCRIÇÃO	DETALHAMENTO	CATMAT/CATSER	QUANTIDADES
1	1	Firewall Principal	Equipamento Firewall modelo 9800 do tipo Applaince que operam em cluster	609340	2
	2	Licenças do Firewall I	Licenças do Firewall definido do item 1	21202	2
	3	Firewall Secundário	Equipamento Firewall modelo 1535 do tipo Applaince para eventos	609340	10
	4	Licenças do Firewall II	Licenças do Firewall definido do item 3	27740	10
	5	Suporte técnico para a Solução	Assistência técnica - hardware e Software da solução.	27740	1
	6	Treinamento	Configuração, administração e uso da ferramenta de gerenciamento do Firewall Check Point	27464	1
	7	Transceivers	TIPO: Transceivers 1000BASE-T RJ45	150812	8

PLANILHA 1

VII - ESTIMATIVA DO VALOR DA CONTRATAÇÃO [Art. 18, § 1º, inciso VI]

VII.1 Orçamento da empresa CONTACTA:

Equipamentos	Identificação do item	CUSTO
Hardware	Firewall Principal e Secundário	R$ 2.158.306,18
Software	Licenças dos Firewalls I	R$ 2.361.956,03
Treinamento	Treinamento das ferramentas de gerencia	R$ 52.715,43
Total		R$ 4.572.923,00

VIII - PARCELAMENTO DO OBJETO [Art. 18, § 1º, inciso VIII]

A presente aquisição será realizada em lote único com 7 itens a fim de que um único fornecedor seja o responsável por fornecer e integrar os componentes da solução, permitindo ainda simplificar e otimizar os processos de gerenciamento e definir claramente o responsável por eventual problema técnico causado por má implantação ou falhas de projeto.

O objeto será adjudicado a uma única licitante.

IX - RESULTADOS PRETENDIDOS/BENEFÍCIOS DIRETOS E INDIRETOS [Art. 18, § 1º, inciso IX]

IX.1 Benefícios Diretos:

IX.1.1 Elevação do nível de segurança de rede corporativa nos perímetros mais críticos, com o controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos.

IX.1.2 Elevação da disponibilidade da conectividade à Internet das unidades judiciárias à Rede de Dados do TRE-RJ, com a criação de políticas de proteção da rede contra ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização.

IX.1.3 Garantia de maior proteção às informações sensíveis deste órgão.

IX.1.4 Gerenciamento de incidentes, ataques cibernéticos e correlatos com a detecção de intrusos na rede e filtragens de conteúdos maliciosos, ao manter a rede protegida contra ameaças cibernéticas em tempo real e ter um maior controle de utilização da rede, a organização economiza significativamente em custos relacionados a incidentes de segurança, como recuperação de dados, perda de produtividade e danos à reputação.

IX.1.5 Garantia de acesso remoto seguro à rede administrativa e aos usuários, com controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos.

IX.1.6 Garantia de que a solução dos firewall sejam utilizados de acordo com as melhores práticas do fabricante e do mercado.

IX.1.7 Monitoração de eventos de segurança do ambiente de comunicação de dados do TRE-RJ.

IX.1.8 Suporte técnico qualificado para garantir que a solução permaneça com o seu funcionamento adequado de acordo com as melhores práticas.

IX.1.9. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº12.965/2014).

IX.2 Benefícios indiretos.

IX.2.1 Melhoria no nível de segurança da informação, uma rede de comunicação e de dados mais segura e eficiente, contribuindo para uma maior produtividade da equipe de TI e de toda a organização. Isso resulta em economia de tempo e recursos, bem como em uma utilização mais eficaz dos recursos de TI.

IX.2.2 Garantir entregas de serviços e aplicações cada vez com mais qualidade, em busca da satisfação dos clientes internos e externos da Justiça eleitoral Fluminense.

X - REQUISITOS DA CONTRATAÇÃO [Art. 18, § 1º, inciso III]

X.1. A solução de TIC objeto da licitação é comum, nos termos do art. 6º, inciso XIII, da Lei 14.133/2021. Os bens que se pretende contratar são encontrados facilmente no mercado nacional.

X.2. Neste sentido, a solução apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

XI – PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO [Art. 18, § 1º, incisos X e XI]

XI.1 Adequação de ambiente

XI.1.1 Infraestrutura tecnológica

Já existe a infraestrutura tecnológica que será realizada através dos switches adquiridos (SEI: 2022.0.000025446-1) para conexão com a solução adquirida.

XI.1.2 Infraestrutura elétrica

Será utilizada a infraestrutura elétrica disponível atualmente no Datacenter na sede da Presidente Wilson.

XI.1.3 Logística de implantação

A implantação da solução escolhida seguirá cronograma formulado pelo TRE-RJ que será detalhado no Termo de Referência.

XI.1.4 Espaço físico

Será utilizada o espaço físico disponível atualmente no Datacenter na sede da Presidente Wilson.

XI.1.5 Mobiliário

Será utilizada a infraestrutura de racks já instalada atualmente no Datacenter na sede da Presidente Wilson.

XI.2 Recursos humanos

Após a implantação da solução, a operação e o gerenciamento dos equipamentos adquiridos ficarão sob responsabilidade da Seção de Suporte às Redes Locais.

A Empresa Contratada será responsável por realizar os serviços de instalação, configurações necessárias na infraestrutura adquirida.

XI.3 Impactos administrativos

Não haverá impactos que impliquem em mudanças em processos de trabalho.

XI.4 Contratações correlatas e/ou interdependentes

Não há contratações correlatas ou interdependentes.

XII – COMPETÊNCIA ESPECÍFICA PARA A GESTÃO E FISCALIZAÇÃO DO CONTRATO:

Não será necessária competência específica dos servidores que atuarão na gestão e/ou fiscalização da prestação dos serviços ou recebimento do material.

XIII - CRITÉRIOS DE SUSTENTABILIDADE/REQUISITOS AMBIENTAIS [Art. 18, § 1º, inciso XII]

Para reduzir o impacto ambiental com a adoção da solução escolhida, foram estudados os seguintes requisitos:

a) Todos os bens permanentes de TI, ao final da vida útil, são disponibilizados para órgãos e entidades para reúso, seguindo um processo próprio de desfazimento realizado pela Sespeq que adota de um plano específico para tal fim.

XIV — INDICAÇÃO DA MODALIDADE DE LICITAÇÃO A SER UTILIZADA PARA A SELEÇÃO DO FORNECEDOR:

O fornecedor será selecionado por meio de licitação, na modalidade Pregão, sob a forma eletrônica, com a adoção do critério de julgamento pelo menor preço por grupo nos termos da Lei 14.133/2021.

XV - POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA [Art. 18, § 1º, inciso XIII]

A equipe de planejamento da contratação, após a conclusão destes Estudos Técnicos Preliminares, declara ser viável a aquisição dos itens aqui registrados.

XVI - DECLARAÇÃO SOBRE A RESTRIÇÃO DE ACESSO AOS ESTUDOS PRELIMINARES OU AO ORÇAMENTO DA CONTRATAÇÃO:

Trata-se de documento preparatório para licitação e deve ter acesso restrito até a publicação de Edital de Licitação (Art. 7º, da Lei 12.527/2011).

JOSE AMARO DOS SANTOS FILHO
CHEFE DA SEÇÃO DE SUPORTE ÀS REDES LOCAIS

Documento assinado eletronicamente em 18/09/2024, às 16:44, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

THEOGENES TERRA JUNIOR
ASSISTENTE I

Documento assinado eletronicamente em 18/09/2024, às 16:47, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

FELIPE DE MELLO SANTOS
CHEFE DA SEÇÃO DE INSTRUÇÃO DE COMPRAS

Documento assinado eletronicamente em 18/09/2024, às 16:54, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

ALBERTO CARMO DE ARAUJO
COORDENADOR(A) DE INFRAESTRUTURA

Documento assinado eletronicamente em 18/09/2024, às 17:06, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.