



PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO

ESTUDO

Estudo Técnico Preliminar - ETP Completo 16296896

**(para contratação de serviços e/ou aquisição de bens permanentes e de consumo por
licitação)**

Guia de suporte ao preenchimento do ETP: 15238786

1 – INTRODUÇÃO

A finalidade do presente expediente é demonstrar a viabilidade técnica e econômica da prorrogação da contratação de Serviço técnico para manutenção da solução de Proteção de Rede com características de *Next Generation Firewall (NGFW)* para o Tribunal Regional Federal da 6ª Região, conforme o Contrato nº 035/2020 firmado entre o TRF da 1ª Região e a empresa L8 Group S.A., que tem o TRF6 como parte interessada, bem como fornecer informações necessárias para subsidiar o respectivo planejamento da prorrogação contratual.

Ressalva-se que este TRF6 promoverá um novo processo licitatório visando a contratação de uma nova solução de firewall, de modo que a prorrogação ora pretendida será pelo período de 12 (doze) meses, podendo ser rescindida em menor período, mediante notificação prévia à Contratada, com antecedência de 30 (trinta) dias.

2 – DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

O presente estudo tem por objetivo demonstrar a viabilidade técnica e econômica da prestação de serviços técnicos para manutenção da solução de Proteção de Rede com características de *Next Generation Firewall (NGFW)* para o Tribunal Regional Federal da 6ª Região, conforme a manifestação do Diretor da Subsecretaria de Infraestrutura/SECTI/TRF6 neste sentido (0411294).

Destaca-se que atualmente os serviços de manutenção vem sendo prestado no âmbito do **Contrato nº 35/2020** (11284787/TRF1), celebrado pelo Tribunal Regional Federal da 1ª Região com a empresa **L8 Group**, cuja vigência expirará em **14/10/2023**. O fornecedor manifestou interesse na prorrogação do contrato, nos termos dos documentos (0447926, 0448328 e 0448332).

Cabe destacar que a solução de *Firewall* é um dispositivo composto de software e/ou hardware, que limita o acesso à rede. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados na rede. O firewall pode ser usado para ajudar a impedir que a rede ou um computador seja acessado sem autorização.

Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers. Com isso a solução de segurança da informação é um grande aliado no combate a vulnerabilidades, uma vez que é capaz de bloquear portas que, eventualmente, sejam usadas pelas ameaças digitais ou então bloquear acesso a programas não autorizados, é de suma importância para continuidade de negócio do TRF6, visto que na sua ausência, haveria enorme impacto na segurança dos serviços de infraestrutura para toda a Justiça Federal da Sexta Região (JF6).

3 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1 - Identificação das necessidades de Negócio da Área Requisitante

3.1.1. Alinhamento estratégico

3.1.1.1. Plano Estratégico de Tecnologia da Informação da Justiça Federal – PETI para 2021-2026, ambos aprovados pela resolução CJF-RES-2020/00685 de 15 de dezembro de 2020.

id. 01 - Aperfeiçoar e Assegurar a efetividade dos serviços de TI para a Justiça Federal.

id. 04 - Promover e fortalecer a segurança da informação digital na Justiça Federal.

3.1.1.2. Plano Diretor de Tecnologia da Informação da Justiça Federal da Primeira Região – PDTI-TRF1 2021/2023, aprovado pelo CGTI-JF1, PAe 0009898-93.2021.4.01.8000 - adotado como referência pelo TRF da 6ª Região.

PDTI-INIC-66 - Prover solução de segurança de acesso à internet (firewall) para o TRF6.

3.1.1.3. Plano de Contratação de Soluções de TI – PCSTI 2022 (14576250).

Aba "Prorrogações" - id 26948 - Serviços de instalação, configuração e treinamento de sistema - Firewall.

3.1.2. Requisitos de negócio

Id	Funcionalidades	Envolvidos
1.	<ol style="list-style-type: none">1. Prover alta disponibilidade e performance dos sistemas e aplicações.2. Prover segurança da informação.3. Prover suporte técnico para melhor utilização, implantação e configuração, bem como suporte preventivos e nos sistemas operacionais, equipamentos e aplicações da solução.	SECTI/SUINF/NUGTI
2.	<ol style="list-style-type: none">1. Prover um ambiente de processamento central (Data Center) com requisitos mínimos de segurança e de disponibilidade estabelecidos em normas nacionais e internacionais, que abrigue os equipamentos principais de processamento e de armazenamento de dados. de segurança e ativos de rede centrais, para maximizar a segurança e a disponibilidade dos serviços essenciais e de sistemas estratégicos do órgão.	SECTI/SUINF/NUGTI

3.	1. Validador de identidades. 2. Acesso Móvel. 3. Filtro de conteúdo. 4. Controle de Aplicações. 5. IPS – Sistema de Prevenção à Intrusão. 6. Inspeção SSL. 7. Emulação de Ameaças. 8. Firewall. 9. VPN - Rede Virtual Privada. 10. QoS – Qualidade de Serviço.	SECTI/SUINF/NUGTI
4.	1. Assegurar níveis de serviços adequados ao negócio.	SECTI/SUINF/NUGTI

3.2 - Macro Requisitos Tecnológicos da Solução de TIC

- 3.2.1.** Prover solução de segurança de acesso à internet (firewall) para a JF6.
- 3.2.2.** Prover segurança da informação.
- 3.2.3.** Garantir a continuidade da solução existente no ambiente da JF6.
- 3.2.4.** Assegurar efetividade dos serviços de TI para a Justiça Federal.

3.3 - Demais Requisitos

3.3.1. Requisitos Legais:

- 3.3.1.1. Resolução CNJ 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- 3.3.1.2. Resolução CJF 279/2013, que dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal - MCTI-JF no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus;
- 3.3.1.3. Instrução Normativa SGD/ME 1/2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal;
- 3.3.1.4. Resolução CJF 06/2008, que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus;
- 3.3.1.5. Portaria CJF-POR-2015/00104, de 6 de março de 2015 que dispõe sobre a aprovação do documento acessório comum "Política de Segurança para Desenvolvimento, Aquisição e Manutenção de sistemas", de que trata a Resolução 6, de 2008;
- 3.3.1.6. Resolução CJF 685/2020, que dispõe sobre o Plano Estratégico de Tecnologia da Informação da Justiça Federal, período 2021-2026;
- 3.3.1.7. Plano Diretor de Tecnologia da Informação da Justiça Federal da Primeira Região - PDTI-TRF1 2021/2023, aprovado pelo CGTI-JF1, conforme consta no PAe 0009898-93.2021.4.01.8000 - SEI;
- 3.3.1.8. Lei 10.520/2002, regulamentada pelo Decreto 10.024/2019, que dispões sobre o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;

3.3.1.9. Decreto 7.174/2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

3.3.1.10. Lei 8.666/1993, que regulamenta o art. 37 inciso XXI da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

3.3.1.11. Lei Complementar 123/2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. altera dispositivos das Leis 8.212 e 8.213 ambas de 24 de julho de 1991 da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei 5.452, de 1º de maio de 1943, da Lei 10.189, de 14 de fevereiro de 2001, da Lei Complementar 63, de 11 de janeiro de 1990. e revoga as Leis 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999;

3.3.1.12. Lei 13.709/2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3.3.2. Requisitos de Manutenção:

3.3.2.1. O plano de suporte deverá compreender a prestação de serviços de subscrição de licenças, suporte técnico e manutenção de hardware e software para todos os produtos (part-numbers) vinculados ao Account do CONTRATANTE, incluindo-se tanto hardware quanto software e também o serviço de emulação de arquivos - Threat Emulation Cloud Service. A contratação prevê o fornecimento do serviço pelo fabricante nas mesmas condições de prestação atuais, modelo de Suporte Collaborative Enterprise Premium.

3.3.2.2. Os serviços compreendem, entre outros:

3.3.2.2.1. Manutenção corretiva de hardware, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas do fabricante;

3.3.2.2.2. A identificação e correção de problemas de software ou em sua configuração;

3.3.2.2.3. Fornecimento e instalação de atualizações corretivas e evolutivas de software e firmware, incluindo pequenas atualizações de release, reparos de pequenos defeitos (bug fixing patches); 1.2.4. Orientação e esclarecimentos de dúvidas sobre instalação, configuração, manutenção e utilização dos produtos;

3.3.2.2.4. Planejamento, migração e acompanhamento de migração de versões de software;

3.3.2.2.5. Apoio em processos de recuperação de desastres (Disaster Recovery) que afetem os produtos;

3.3.2.2.6. Transferência de conhecimento acerca de melhores práticas indicadas pela fabricante;

3.3.2.2.7. Acesso à base de conhecimento da fabricante;

3.3.2.2.8. Execução de verificações de vulnerabilidades no software ou em sua configuração sempre que necessário;

3.3.2.2.9. Emissão de relatórios e realização de diagnósticos no ambiente.

3.3.2.3. A CONTRATADA deverá disponibilizar canal de atendimento para abertura de chamados técnicos, mediante número 0800 ou número local em Belo Horizonte/MG.

Adicionalmente, poderá ser disponibilizado serviço de abertura de chamado via site ou e-mail.

3.3.2.3.1. Para cada chamado técnico, a Contratada deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.

3.3.2.3.2 Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional, conforme abaixo:

3.3.2.3.2.1. Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;

3.3.2.3.2.2. Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema.

3.3.2.3.2.3. Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, troubleshooting ou utilização.

3.3.2.3.3. O nível de severidade será informado pelo CONTRATANTE no momento da abertura do chamado.

3.3.2.3.4. O CONTRATANTE poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade.

3.3.2.3.5. Os serviços de suporte e assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de atendimento inicial e solução do incidente:

3.3.2.3.5.1. Os chamados de Prioridade Alta deverão ser atendidos em até 30 (trinta) minutos e solucionados em até 2 (duas) horas;

3.3.2.3.5.2. Os chamados de Prioridade Média deverão ser atendidos em até 1 (uma) hora e solucionados em até 4 (quatro) horas;

3.3.2.3.5.3. Os chamados de Prioridade Baixa deverão ser atendidos em até 2 (duas) horas e solucionados em até 48 (quarenta e oito) horas.

3.3.2.3.6. O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte a partir da Central de Atendimento da CONTRATADA.

3.3.2.3.7. Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou a intervenção remota.

3.3.2.3.7.1. Caso não seja possível a intervenção remota, seja por impossibilidade de comunicação, seja por impossibilidade de análise do problema, um técnico da CONTRATADA deverá realizar o atendimento onsite, obrigatoriamente.

3.3.2.3.8. Entende-se por término do atendimento a ocorrência de um dos eventos abaixo relacionados:

3.3.2.3.8.1. Solução definitiva;

3.3.2.3.8.2. Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do CONTRATANTE;

3.3.2.3.8.3. Solução de contorno e escalonamento do chamado para o fabricante, em caso de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução. Para esses problemas, a CONTRATADA deverá restabelecer o ambiente, através de uma solução paliativa, informando o CONTRATANTE em

um prazo máximo de 24 (vinte e quatro) horas quando a solução definitiva será disponibilizada. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

3.3.2.3.9. O encerramento do chamado será dado por servidor do CONTRATANTE na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

3.3.2.3.10. Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos. 1.3.11. Em caso de falhas irreversíveis de hardware ou impossibilidade de solução pela assistência técnica, a CONTRATADA deverá providenciar a troca por equipamento idêntico.

3.3.2.3.11. Casos em que se tornará obrigatória a substituição de equipamentos pela CONTRATADA:

3.3.2.3.11.1. Falha de hardware e/ou software que interrompa o funcionamento do equipamento por mais de 12 (doze) horas consecutivas;

3.3.2.3.11.2. Inoperância do equipamento, por tempo superior a 2 (duas) horas, em 2 (duas) ocasiões separadas por, no máximo, um período de 60 (sessenta) dias corridos.

3.3.2.3.11.3. Por questão de segurança, os equipamentos e softwares nunca deverão ser removidos das dependências da CONTRATANTE sem a remoção de dados ou regras sigilosas.

3.3.2.3.12. No caso de troca do produto por defeito, não haverá qualquer ônus adicional para o CONTRATANTE.

3.3.2.4. Relativamente à manutenção corretiva de hardware e software:

3.3.2.4.1. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do CONTRATANTE, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);

3.3.2.4.2. Concluída a manutenção, a CONTRATADA fornecerá ao CONTRATANTE, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção.

3.3.2.4.3. Durante todo o período de vigência dos serviços, a CONTRATADA atualizará ou disponibilizará para download, sem ônus adicionais para o CONTRATANTE, os softwares necessários ao funcionamento da solução, fornecendo novas versões ou releases lançados. Os softwares tratados neste item incluem vacinas de antivírus/anti-malware, assinaturas do filtro de conteúdo web, software de gerenciamento, firmwares de bios e drivers.

3.3.2.4.4. A atualização ou disponibilização para download deverá ocorrer em um prazo máximo de 15 (quinze) dias úteis, contados da data de lançamento da nova versão ou release. Caso a nova versão ou release seja disponibilizada para download, deverá a CONTRATADA prestar o suporte necessário para a instalação e configuração da mesma.

3.3.2.4.5. Qualquer manutenção e/ou intervenção por solicitação da CONTRATADA ou do fabricante, mesmo não implicando em inoperância da solução ou alteração de suas características, deverá ser agendada e acordada previamente com o

CONTRATANTE.

3.3.2.5. Os serviços deverão ser prestados por equipe técnica qualificada pelo fabricante da solução.

3.3.2.6. A CONTRATADA não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.

3.3.2.7. O CONTRATANTE poderá acompanhar os chamados técnicos abertos pela CONTRATADA junto ao fabricante.

3.3.2.8. Os serviços deverão ser prestados por profissionais qualificados da fabricante ou empresa autorizada pela fabricante.

3.3.2.9. Os serviços de manutenção de hardware deverão ser prestados nas dependências do Tribunal Regional Federal da 6ª Região, situado na Avenida Álvares Cabral nº 1.805 - Bairro Santo Agostinho - CEP: 30.170-001 - Belo Horizonte - MG.

3.3.3. Requisitos de Capacitação:

3.3.3.1. Os serviços de suporte descritos nos requisitos de manutenção envolvem ainda transferência de conhecimento acerca de melhores práticas indicadas pela fabricante.

3.3.4. Requisitos Temporais:

3.3.4.1. O objeto deverá ser entregue no endereço do tribunal no prazo de até 15 (quinze) dias corridos contados da data de assinatura do contrato.

3.3.4.2. No caso de entrega em meio eletrônico, a CONTRADA deverá certificar-se do recebimento do objeto pelo órgão requisitante, dentro do prazo estabelecido no item anterior.

3.3.4.3. Prazo de entrega do plano de suporte para solução de firewall, será de no máximo, 15 (quinze) dias corridos a contar da data da assinatura do contrato.

3.3.4.4. Os serviços serão prestados pelo fornecedor ou fabricante, por um período de, no mínimo, 12 meses (plano anual).

3.3.4.5. Garantia integral, observada a previsão da Lei n.º 8.078/1990 sobre o tema, pelo período mínimo de 90 (noventa) dias, compreendendo defeitos e vícios de qualidade e quantidade, a contar da data do recebimento definitivo, pelo TRF6, em se tratando de defeitos ou vícios aparentes ou de fácil constatação; ou de sua evidência, nos casos de defeitos ou vícios ocultos.

3.3.4.6. Apresentar, no prazo máximo de 10 (dez) dias úteis, contados da assinatura do termo aditivo ao contrato, comprovante da prestação de garantia contratual.

3.3.5. Requisitos de Segurança:

3.3.5.1. Será exigida prestação de garantia, podendo o fornecedor optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, no montante equivalente a 5% (cinco por cento) do valor total do contrato.

3.3.5.2. Será exigida ainda Garantia integral, observada a previsão da Lei n.º 8.078/1990 sobre o tema, pelo período mínimo de 90 (noventa) dias, compreendendo defeitos e vícios de qualidade e quantidade, a contar da data do recebimento definitivo, pelo TRF6, em se tratando de defeitos ou vícios aparentes ou de fácil constatação; ou de sua evidência, nos casos de defeitos ou vícios ocultos.

3.3.6. Requisitos Sociais, Ambientais e Culturais:

3.3.6.1. De acordo com as normas vigentes relativas ao desenvolvimento sustentável nas licitações e contratações públicas, bem como o o Plano de Logística Sustentável da Justiça Federal da 1ª Região (RESOLUÇÃO PRESI 4/2016), em especial observando os

parágrafos e incisos do Art. 3º da referida resolução e o Art. 17 da Resolução Nº 201 de 03/03/2015, a equipe de planejamento entende que por se tratar de contratação onde não haverá oferta de produto por meio físico e nem mão de obra dedicada, não serem necessárias exigências editalícias ou contratuais referentes ao objeto desta contratação.

4 – LEVANTAMENTO DAS ALTERNATIVAS (CENÁRIOS POSSÍVEIS)

Cenário 1

Entidade	TRF6
Descrição	Prorrogação do Contrato 35/2020 (11284787/TRF1)
Fornecedor	L8 Group

Custo Total de Propriedade: Análise para o “Cenário 1”

	Descrição do Item	Quantidade	Valor unitário Mensal	Valor Mensal	Valor Total Anual (12 meses)
Valor estimado para a contratação, conforme o Termo de Apostilamento nº 1 (17214918/TRF1)	Plano de suporte para solução de firewall CheckPoint, incluindo subscrição de software, suporte técnico e manutenção de hardware pelo período de 12 (doze) meses.	02 unidades (1 cluster)	R\$ 17.657,06	R\$35.314,12	R\$423.769,50

**Valor unitário - para demonstrar a economicidade foram realizados os seguintes cálculos, a divisão do valor anual por 12 meses e o valor mensal pelo número de licenças do software, conforme o quantitativo adquirido.*

Cenário 2

Entidade	Justiça Federal - CE (0450897)
Descrição	Renovação de licenciamento de software para appliance Check Point 5600 pelo período de 12 (doze) meses

Custo Total de Propriedade: Análise para o “Cenário 1”

	Descrição do Item	Quantidade	Valor unitário mensal	Valor unitário Anual	Valor Total Anual
Valor estimado para a contratação	Renovação de licenciamento de software para appliance Check Point 5600 em alta disponibilidade e da solução de relatoria e correlação de eventos, garantia de atualização e funcionamento pelo período de 12 (doze) meses	02 Unidades (1 cluster)	R\$ 28.153,13	R\$56.306,26	R\$ 675.675,23
Total:					R\$ 675.675,23

SOLUÇÕES SIMILARES AO CENÁRIO 2

Órgão 1					
Nome do órgão/UASG	Defensoria Pública - CE (0450904)				
Nºda Compra	PE 20220017 - DPGE (0411288)				
Objeto	Serviço de renovação de licenciamento de software para appliance Check Point 5400 em alta disponibilidade e da solução de relatoria e correlação de eventos, garantia de atualização e funcionamento pelo período de 36 (trinta e seis) meses				
ID DO ITEM	DESCRIÇÃO	QUANTIDADES	*VALOR UNITÁRIO MENSAL	VALOR MENSAL	VALOR TOTAL (12 meses)
01	Serviço de renovação de licenciamento de software para appliance Check Point 5400 em alta disponibilidade e da solução de relatoria e correlação de eventos, garantia de atualização e funcionamento pelo período de 36 (trinta e seis) meses	1 Unidade (cluster)	R\$29.022,60	R\$29.022,60	R\$348.271,30
FORNECEDOR: NTSEC SOLUCOES EM TELEINFORMATICA LTDA.					
<i>*Valor unitário - para demonstrar a economicidade foram realizados os seguintes cálculos, a divisão do valor anual por 12 meses e o valor mensal pelo número de licenças do software, conforme o quantitativo adquirido.</i>					
Órgão 2					
Nome do órgão/UASG	BRB - Banco Regional de Brasília				
Nºda Compra	PE 078/2022 (0450907, 0450914 e 0450919)				
Objeto	Renovação da infraestrutura de firewalls do fabricante Check Point que o BRB possui, com módulos de expansão, treinamento e suporte especializado.				
ID DO ITEM	DESCRIÇÃO	QUANTIDADES	VALOR UNITÁRIO MENSAL	VALOR MENSAL	VALOR TOTAL (12 meses)

01	Renovação do licenciamento dos atuais equipamentos de firewall Check Point e módulos de expansão	2 (dois) appliances Check Point 15400 com SKU CPAP-SG15400-NGTP; 8 (oito) appliances Check Point 5800 com SKU CPAP-SG5800-NGTP. Serviços de suporte 24 x 7	R\$31.339,12	R\$313.391,25	R\$3.760.695,02
----	--------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------	---------------	-----------------

FORNECEDOR: NTSEC SOLUCOES EM TELEINFORMATICA LTDA.

***Valor unitário** - para demonstrar a economicidade foram realizados os seguintes cálculos, a divisão do valor anual por 12 meses e o valor mensal pelo número de appliances e serviços de suporte, conforme o quantitativo adquirido.

5 - ANÁLISE E COMPARATIVO DE CUSTOS DE PROPRIEDADE

Cenários	Valor Estimado (R\$)	Análise
1 . Renovação do Contrato 35/2020 (11284787)	R\$ 423.769,50	O valor deste cenário leva em consideração os valores constantes no Termo de Apostilamento nº 1 (17214918/TRF1) devido ao reajuste do valor conforme previsto em contrato. O cenário atende tecnicamente ao TRF6 e se mostra tecnicamente e economicamente viável, mesmo em se considerando o reajuste pleiteado pela contratada, conforme a proposta de prorrogação apresentada.
2 . Contratação de empresa especializada para prestação de serviços de manutenção e suporte para solução de Firewall pelo período de 12 (doze) meses	R\$ 675.675,23	O cenário atende a todos os requisitos de negócio e requisitos técnicos. Após análise de preços realizada com os órgãos públicos, foi observado que o cenário 01 é economicamente mais viável que o cenário 2, considerando os valores unitários coletados, conforme os quadros acima (Órgão 1 e Órgão 2) e Mapa Comparativo de Preços (0451587).

6 - DETALHAMENTO DAS ALTERNATIVAS EXISTENTES

Requisito	ID da Solução	Sim	Não	Não se Aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	Solução 1	X		
	Solução 2	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	Solução 1	X		

		Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro?		Solução 1			X
		Solução 2			X
A Solução é um software livre ou software público?		Solução 1		X	
		Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?		Solução 1			X
		Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)		Solução 1			X
		Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?		Solução 1			X
		Solução 2			X
7 – JUSTIFICATIVA DO CENÁRIO ESCOLHIDO					
Cenário	Cenário 1	Descrição	Prorrogação do Contrato 35/2020 pelo período de 12 meses		
Bens e Serviços que Compõem a Solução					
ID	Bem/Serviço		Estimativa		
01	Prorrogação do Contrato 35/2020		R\$ 423.769,50		
Alinhamento em Relação às Necessidades de Negócio e Macro Requisitos Tecnológicos					

A Justiça Federal da 6ª Região possui dados e documentos relevantes, além de fornecer serviços judiciais para os cidadãos e para as entidades da Administração Pública Federal. As atividades do Tribunal carecem de segurança tanto para com os servidores, quanto para com os usuários externos. A estrutura tecnológica da JF6 ainda está em construção, e o mercado encontra-se em constante crescimento e expansão, motivados principalmente pelo crescente volume de dados e um aumento considerável na quantidade de aplicações e recursos ofertados pela área de Tecnologia da Informação e Comunicação, tornando-se imprescindível que a mesma esteja disposta de forma estável, robusta e confiável. Ressalta-se também que boa parte destas informações são de natureza sensível ou crítica, comprovando ainda mais a necessidade de prover um nível elevado de segurança condizente com a natureza do Tribunal, pois camadas avançadas de proteção poderiam dotar a JF6 de uma infraestrutura de segurança mais robusta e confiável. A invasão do ambiente tecnológico do Tribunal ou o roubo/danificação de documentos sigilosos provocariam danos incalculáveis.

Firewall é um dispositivo composto de software e/ou hardware, que limita o acesso à rede. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados na rede. O firewall pode ser usado para ajudar a impedir que a rede ou um computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers. Com isso a solução de segurança da informação é um grande aliado no combate a vulnerabilidades, uma vez que é capaz de bloquear portas que, eventualmente, sejam usadas pelas ameaças digitais ou então bloquear acesso a programas não autorizados.

Cumprido neste ponto justificar a escolha do cenário 1 em detrimento dos demais cenários estudados no presente ETP.

Cenário 1:

Neste cenário foi avaliada a possibilidade de realização de prorrogação pelo período de 12 (doze) meses do Contrato nº 35/2020, relativamente à parte do contrato destinada ao TRF6, sendo este tecnicamente possível pois atende a todos os requisitos de negócio e técnicos.

Cenário 2:

Após realizar avaliação dos cenários 1 e 2 conclui-se que o cenário 2 é viável e atende a todos requisitos de negócio, porém, após análise dos valores de mercado (item 04 deste documento e conforme o Mapa Comparativo de Preços 0451587, foi constatado que o cenário 1 é mais viável economicamente.

Assim o cenário 1 foi escolhido como solução para esse estudo.

Benefícios a serem alcançados	
1	Manutenção e atualização do parque tecnológico para atender às necessidades da JF6, diminuindo riscos de indisponibilidades.
3	Garantia de suporte aos equipamentos, sistemas operacionais, softwares e aplicativos utilizados pela JF6.
5	Garantir disponibilidade e continuidade dos serviços que são imprescindíveis atualmente para o pleno desempenho das atividades da JF6.
6	Aplicação de proteções de segurança em sistemas e ativos de negócio.
7	Aplicação de controle sobre comunicações originadas e recebidas pelo Tribunal.
9	Controle de acesso a conteúdo de internet e Detecção e exclusão de ameaças virtuais.
10	Prevenção contra intrusão e ataques aos sistemas do Tribunal.

11	Disponibilidade de meios de acesso seguros para conexão com outros órgãos da Administração Pública.
12	Armazenar e gerenciar os logs de modo eficaz, permitindo a emissão automatizada de relatórios gerenciais e técnicos, essenciais às tomadas de decisão.

8 – NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE INTERNO PARA EXECUÇÃO CONTRATUAL

8.1. Não são necessárias adequações no ambiente, pois a solução já se encontra implantada no âmbito da JF6.

9 – RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

Recurso Material – 1

Infraestrutura básica do CPD local para manutenção da solução já instalada neste tribunal.

Quantidade	Quantidade necessária para suportar a solução.	Disponibilidade	<p>1. O tempo de execução dos serviços de infraestrutura não deverá ultrapassar os prazos definidos contratualmente para entrega dos equipamentos.</p> <p>2. As necessidades futuras, se houver, serão definidas com o apoio da área de TI.</p>
Ações para Obtenção do Recurso			1. Não se aplica, porquanto o Tribunal já possui a infraestrutura física e lógica necessária para a implantação da solução.
Responsáveis pela Obtenção do Recurso			SECTI/TRF6-MG

Recurso Material – 2

Contratação de garantia e suporte técnico.

Quantidade	A garantia e suporte técnico deverá ser de 12 (doze) meses.	Disponibilidade	1. Durante a vigência da prorrogação contratual.
------------	-------------------------------------------------------------	-----------------	--------------------------------------------------

9 – RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

Ações para Obtenção do Recurso

1. Definir os requisitos e critérios necessários para garantia em conjunto com a área técnica.
2. Deixar claro quais os critérios e responsabilidades da fornecedora da solução. e
3. Garantir que a empresa contratada tenha os requisitos necessários para atender à demanda do Tribunal devido ao tamanho de sua região.

Responsáveis pela Obtenção do Recurso

SESEI/DITEC/TRF1 - SECTI/TRF6
(conforme processo SEI nº 0033673-16.2021.4.01.8008 - MG)

Recursos Humanos – 1

Fiscal Técnico

Quantidade

01 titular e 01 substituto.

Formação

Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato.

Atribuições

Fiscalizar o contrato junto à Contratada do ponto de vista técnico, apoiar o gestor do contrato quanto às questões técnicas contratuais.

Recursos Humanos – 2

Gestor do Contrato

Quantidade

01 titular e 01 substituto.

Formação

Servidor com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato, indicado pela autoridade competente.

Atribuições

Iniciar o contrato, encaminhar ordem de serviço, monitorar a execução do contrato autorizar a emissão/pagamento de notas fiscais.

Recursos Humanos – 3

Preposto

Formação

Sólidos conhecimentos na solução para recebimento das demandas e acompanhamento da execução contratual.

Atribuições

Acompanhar a execução do contrato, atuar como interlocutor principal junto à CONTRATANTE, receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

Recursos Humanos – 4	
Equipe Técnica da Contratada	
Formação	Profissional(is) da Contratada devidamente capacitado(s) na solução de segurança.
Atribuições	Executar fielmente o contrato e efetuar, caso necessário, correções durante a execução contratual.
10 – ESTRATÉGIA DE CONTINUIDADE DA SOLUÇÃO EM CASO DE INTERRUPÇÃO CONTRATUAL	
Evento 1	
Execução inadequada do objeto contratado.	
Ação Preventiva	Fiscalizar o contrato e acompanhar a execução dos serviços evitando a descontinuidade da contratação, aplicando as sanções e glosas previstas no contrato.
Responsáveis	Gestor do contrato/NUGTI/SECTI/TRF6
Ação de Contingência	Rescisão contratual e convocação das próximas licitantes pela ordem de classificação no certame ou planejamento de nova contratação.
Responsáveis	Gestor do contrato/Diaco/Equipe de planejamento
Evento 2	
Falência da Empresa Contratada.	
Ação Preventiva	Planejamento de nova contratação
Responsáveis	Equipe de planejamento
Evento 3	
Encerramento abrupto do contrato.	
Ação de Contingência	Tomar as ações administrativas cabíveis em contrato e na legislação, informar o gestor do contrato das sanções administrativas previstas no contrato, informar a contratada sobre as sanções aplicáveis. Iniciar estudo de mercado e viabilidade de contratação de nova solução, via planejamento da contratação. Realizar novo processo licitatório.
Responsáveis	Gestor do contrato/Diaco/Equipe de Planejamento
Evento 4	
Não atendimento aos prazos preestabelecidos pelo Tribunal.	

Ação de Contingência	Executar as penalidades previstas no contrato. Não realizar o aceite dos serviços.
Responsáveis	Gestor do contrato/Diaco
Evento 5	
Prestação de serviços deficitária e/ou com nível de qualidade abaixo do previsto.	
Ação de Contingência	Avaliar a necessidade ou não de rescisão unilateral do Contrato. Rescisão contratual e convocação dos próximos participantes do certame. Realizar novo processo licitatório.
Responsáveis	Gestor do contrato/Diaco
Evento 6	
Proximidade do encerramento do Contrato.	
Ação de Contingência	Iniciar estudo de mercado e viabilidade de contratação de nova solução, via planejamento da contratação. Realizar novo processo licitatório.
Responsáveis	Gestor do contrato/Diaco/Equipe de planejamento
11 – DECLARAÇÃO DE VIABILIDADE	
<p>11.1. Os responsáveis pelo planejamento desta prorrogação contratual, ciente das regras e diretrizes da Resolução CNJ nº 182/2013, após a conclusão de todos os estudos técnicos preliminares aqui contidos, declaram ser viável a prorrogação da contratação pretendida.</p>	
12 – ASSINATURAS	
Diretor da Subsecretaria de Infraestrutura	
Nome: Heli Lopes Rios	Matrícula: TR 38
<p>O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da prorrogação. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, principalmente os técnicos, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a prorrogação proposta.</p>	
<p style="text-align: center;">Integrante Requisitante</p>	
Integrante Técnico	

Nome: Lucimar Ferreira da Silva

Matrícula: TR 271

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME nº 1/2019, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da prorrogação. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, principalmente os técnicos, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a prorrogação proposta.

Integrante Técnico



Documento assinado eletronicamente por **Heli Lopes Rios, Diretor de Subsecretaria**, em 12/09/2023, às 16:11, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Lucimar Ferreira da Silva, Técnico Judiciário**, em 12/09/2023, às 16:12, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site

[https://sei.trf6.jus.br/sei/controlador_externo.php?](https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código verificador **0456576** e o código CRC **F06BDD59**.