Estudo Técnico Preliminar - ETP - PGDF/SEGER/SUAG/EPC-OS10-2024

1 – INTRODUÇÃO

A presente análise tem por objetivo avaliar a viabilidade técnica e econômica de solução de segurança para rede de computadores (*firewall)* e serviços suplementares para a Procuradoria–Geral do Distrito Federal (PGDF)**,** bem como fornecer informações necessárias para subsidiar o respectivo processo.

2 – DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Solução de segurança para rede de computadores, compreendendo equipamentos do tipo *firewall* para o sítio principal e sítios remotos da PGDF, e logiciário relacionado, incluindo instalação, configuração, transferência de conhecimento e garantia, quando aplicáveis, visando atender a necessidade de garantir e monitorar a segurança da infraestrutura de Tecnologia da Informação da Procuradoria–Geral do Distrito Federal.

2.1 – CONTEXTUALIZAÇÃO

Por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), a PGDF firmou o Contrato de Aquisição de Bens pelo Distrito Federal nº 15/2020-PGDF (48527621), assinado em 20 de outubro de 2020, com vigência de 6 meses para fornecimento de solução de segurança para rede de computadores (*firewall*), com suporte e treinamento para operação da solução, restando a garantia pelo período de 36 meses, a partir da data de assinatura do Termo de Recebimento Definitivo, ocorrida em 19/05/2021 (62068446). Sendo assim, a sustentação da solução findou em 19/05/2024.

A solução fornecida à PGDF por meio do referido Contrato foi composta por:

- 02 equipamentos agregados (tipo 01), em alta disponibilidade, a serem instalados na sede do órgão – sítio principal;
- 02 equipamentos (tipo 02), a serem instalados em sítios remotos;
- 01 conjunto de softwares de gerenciamento de equipamentos e logs e caixa de areia (*sandbox*), instalados na sede do órgão – sítio principal; e
- 01 serviço Instalação e configuração dos equipamentos e logiciário relacionado.

Esses dispositivos em uso pela PGDF possuem módulos integrados e licenciados de controle de identidade e conscientização computacional, filtragem de endereços, controle de aplicações, inspeção *SSL* (*Secure Socket Layer* – Camada Segura de Soquete), prevenção de intrusões e ameaças, prevenção de perda de dados, conectividade por intermédio de *VPN* (*Virtual Private Network* – Rede Privada Virtual) dentre outras funcionalidades que caracterizam um *NGFW* (*Next Generation Firewall* – *Firewall* de Próxima Geração) – como inspeção na camada 7 do modelo *OSI* (*Open System Interconnection* – Interconexão de Sistemas Abertos).

Tendo por base o cenário atual e considerando a continuidade no atendimento às propriedades básicas da segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade), o prosseguimento do controle de restrições e do fluxo do tráfego entre redes distintas e possíveis modificações que ocorrem/ocorrerão nas redes de dados que servem à instituição, recomenda–se a aquisição de equipamentos, licenças e suporte técnico e/ou renovação de licenças e suporte técnico relacionado a solução de segurança para rede de computadores (*firewall*), conforme análise neste Estudo Técnico Preliminar da Contratação.

3 – DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1 – NECESSIDADES DE NEGÓCIO DA ÁREA REQUISITANTE

Id.	Requisitos
1.	Manter a segurança da rede de computadores da Procuradoria–Geral do Distrito Federal – PGDF
2.	Manter a efetividade da gestão da Segurança da Informação
3.	Manter a disponibilidade dos serviços providos pela PGDF
4.	Manter a prevenção contra ameaças externas à rede da PGDF

3.2 – MACRO REQUISITOS TECNOLÓGICOS DA SOLUÇÃO DE TI

Id.	Requisitos
1.	Permitir a adequação às necessidades da PGDF
2.	Permitir o controle do fluxo do tráfego entre redes distintas
3.	Permitir a inspeção do estado das conexões de rede
4.	Permitir a tradução de endereços para preservação da topologia da rede interna
5.	Permitir o controle do uso de aplicativos não autorizados ou potencialmente perigosos
6.	Permitir a inspeção do tráfego criptografado para aplicação de políticas de segurança e conformidade
7.	Permitir a análise dos padrões de tráfego em busca de atividades maliciosas
8.	Permitir a detecção de anomalias e comportamentos suspeitos
9.	Permitir a aplicação de políticas de segurança e conformidade
10.	Permitir o controle de acesso a recursos com base em identidades confiáveis

3.3 – DEMAIS REQUISITOS DA SOLUÇÃO	
Id.	**Requisitos**
1.	Fazer parte do catálogo de produtos comercializados e não ter sido descontinuado
2.	Não estar relacionada em listas *"end–of–sale"* e *"end–of–support"* do sítio do fabricante
3.	Continuar funcionando após o vencimento das licenças, mesmo que sem atualizações
4.	Ter uma interface intuitiva e amigável para a administração
5.	Ter uma única interface centralizada para gerenciar e monitorar os equipamentos
6.	Ter uma interface para monitoramento do tráfego de rede em tempo real e para a geração de relatórios
7.	Ter níveis de acesso para diferentes usuários e/ou grupos
8.	Ter módulos de auditoria para rastrear modificações realizadas
9.	Ter opção de *backup* das configurações dos equipamentos e/ou módulos
10.	Ter opção de agendar tarefas automáticas
11.	Ter opção de efetuar atualizações automáticas de *firmwares*, assinaturas de ameaças e atualizações críticas
12.	Permitir a integração com outras soluções de segurança de rede e/ou gerenciamento de informações
13.	Permitir o envio de alertas e notificações sobre atividades suspeitas e/ou violações de segurança
14.	Permitir o alinhamento de suas políticas com padrões regulatórios e a Política de Segurança da Informação e Comunicações (POSIC) da PGDF
15.	Permitir o monitoramento de licenças e serviços relacionados
16.	Possuir documentações e suporte técnico para solução de problemas e obtenção de orientações
17.	**Legais**
17.1.	Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018.
17.2.	Política de Segurança da Informação e Comunicações (POSIC) da PGDF - Portaria nº 356, de 16 de julho de 2018.
17.3.	Instrução Normativa SLTI/MPOG nº 94, de 23 de dezembro de 2022.
17.4.	Decreto nº 44.330, de 27 de setembro de 2023, que recepciona a IN 94/2022 no âmbito do GDF.
4 – LEVANTAMENTO DAS ALTERNATIVAS (CENÁRIOS POSSÍVEIS)	
4.1 – CENÁRIO 1	
Entidade	Procuradoria Geral do Distrito Federal - PGDF
Descrição	Manutenção da atual solução de segurança para rede de computadores – *firewall* – pela própria PGDF, sem a contratação de assistência técnica e/ou equipamento(s), consequentemente, renunciando aos módulos de filtragem de endereços, controle de aplicações, dentre outras funcionalidades da solução do tipo *Next Generation Firewall* (*NGFW*)
Fornecedor	–

Análise da Solução	Trata-se da manutenção da solução de segurança atual para a rede de computadores, adquirida por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), pela própria PGDF, renunciando recursos como filtragem de endereços, controle de aplicações e outras funcionalidades da solução de *Next Generation Firewall* (*NGFW*), composta por: • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do órgão – sítio principal; • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do Instituto de Pesquisa e Estatística do Distrito Federal – IPEDF – sítio de contingência; • 01 (um) conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*), instalados na sede do órgão – sítio principal. Nesse caso, os servidores da PGDF teriam que absorver a demanda e dar continuidade manutenção da solução de segurança. Contudo, a PGDF não dispõe de pessoal suficiente para atender às necessidades de suporte e de manutenção da solução de segurança. Há fatores críticos que dificultam a manutenção interna do sistema, como a especificidade e o desuso da tecnologia, o elevado custo de capacitação, a escassez de profissionais qualificados e os consequentes atrasos. O cenário apresenta as seguintes vantagens: • Economia de recursos – a manutenção da solução permite a economia de recursos financeiros; • Gestão simplificada – eliminação da complexidade de novas implementações; • Conhecimento prévio – supressão da necessidade de contratar serviços para treinamento de pessoal; • Histórico – preservação de registros históricos que podem ser posteriormente utilizados. O cenário apresenta as seguintes desvantagens: • Supressão de atualizações – a não contratação de assistência técnica extingue o acesso às atualizações de segurança. A rede da PGDF pode ficar exposta a novas ameaças e vulnerabilidades; • Supressão de assistência técnica – a não contratação de assistência técnica extingue o apoio do fabricante e/ou fornecedor da solução em caso de problemas, falhas e/ou incidentes de segurança relacionados aos equipamentos. A prestação de serviços pelo órgão pode ser prejudicada por tempos de inatividade prolongados e custos elevados de recuperação; • Regulamentações – a PGDF pode receber penalidades legais por descumprimento de regulamentos de segurança cibernética; • Eficácia reduzida – os equipamentos ficarão desatualizados e menos eficazes na proteção contra novas ameaças. A prestação de serviços pelo órgão pode ser prejudicada em razão de brechas na segurança; • Vulnerabilidades – a não contratação de assistência técnica torna o órgão vulnerável à ameaças diversas e incidentes de segurança. Custos relacionados à recuperação de dados e perda de produtividade podem ser maiores que a contratação de suporte especializado e/ou equipamentos. • Custos adicionais - custos envolvidos na capacitação/treinamento e nomeação de servidores para atuar na manutenção do sistema se segurança. A manutenção da solução de segurança atual para a rede de computadores da PGDF, prestada atualmente pelo próprio órgão, apresenta uma série de desafios significativos. A operação dos equipamentos e *softwares* instalados tanto na sede do órgão quanto no IPEDF, apresenta alta criticidade. A renúncia a recursos avançados de filtragem de endereços, controle de aplicações e outras funcionalidades de um *NGFW* impõe limitações consideráveis. Um dos principais desafios enfrentados pela PGDF é a necessidade de absorver internamente a demanda de suporte e manutenção da solução de segurança. A falta de pessoal suficiente e qualificado para atender a essas necessidades é um obstáculo crítico. A especificidade da tecnologia exige um elevado custo de capacitação, o que agrava ainda mais a situação. Atualmente, a PGDF passa por uma evasão de servidores, principalmente da área de tecnologia da informação, ocasionada pela grande disparidade de remuneração com os demais órgãos. A Subsecretaria de Tecnologia da Informação, que já teve um número considerável de servidores, agora conta apenas com um número reduzido, e nos próximos seis meses a previsão é que mais servidores já aprovados em outros concursos também deixem a Procuradoria. Sem uma equipe dedicada para cobrir os horários estendidos, qualquer problema técnico que ocorra fora do expediente compromete a operação do sistema e pode afetar diretamente as atividades da Procuradoria. A ausência de suporte constante aumenta o tempo de resposta e dificulta a resolução de falhas em tempo hábil, o que não só coloca em risco a continuidade dos serviços, mas também afeta a eficiência e a segurança das atividades jurídicas. Ademais, a carência de força de trabalho com conhecimento adequado na área de segurança e infraestrutura compromete a eficácia da solução de segurança. A escassez de pessoal capacitado para tomar medidas de proteção torna a rede de computadores da PGDF vulnerável a ataques e brechas de segurança. Além disso, a falta de suporte técnico qualificado pode resultar em tempos de resposta mais longos para resolver problemas críticos, afetando a continuidade dos serviços prestados pelo órgão. Desta forma, seria necessário um incremento no número de analistas aptos a dar continuidade ao serviço em questão. Posteriormente, esses servidores necessariamente precisariam de investimento adicional em treinamentos para garantir a manutenção da solução de segurança atual.

4.1.1 – CUSTO TOTAL DE PROPRIEDADE: ANÁLISE PARA O "CENÁRIO 1"

Item	Descrição	Valor (R$)
–	–	–
TOTAL GERAL		–

4.2 – CENÁRIO 2

Entidade	–

Descrição	Aquisição de servidores e/ou *appliances*, com características específicas de desempenho, para montagem de solução de segurança para rede de computadores – *firewall* – utilizando *software* de código aberto (*open–source*), tencionando substituir a atual solução
Fornecedor	–
Análise da Solução	Trata–se de aquisição de servidores e/ou *appliances* para a montagem de uma estrutura de segurança para a rede de computadores, utilizando software de código aberto (*open–source*), com vistas a substituir a atual solução adquirida por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), composta por: • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do órgão – sítio principal; • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do Instituto de Pesquisa e Estatística do Distrito Federal – IPEDF – sítio de contingência; • 01 (um) conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*), instalados na sede do órgão – sítio principal. O cenário apresenta as seguintes vantagens: • Flexibilidade – um so*ftware* de código aberto permite adaptações e personalizações conforme a necessidade do órgão; • Economia de recursos – embora haja a necessidade de aquisição de servidores e/ou *appliances*, o so*ftware* de código aberto pode reduzir custos de licenciamento; • Inovação – um so*ftware* de código aberto recebe atualizações da comunidade, garantindo melhoras contínuas; • Escalabilidade e integração – o modelo permite o crescimento da rede e a integração com diversas ferramentas e sistemas. O cenário apresenta as seguintes desvantagens: • Complexidade – um so*ftware* de código aberto mal configurado pode apresentar vulnerabilidades de segurança. É provável que o *hardening* (processos) para mitigar tentativas de ataque exija a necessidade de contratação de profissionais capacitados e/ou suporte técnico qualificado; • Suporte – o *software open–source* não possui assistência técnica tão abrangente quanto o oferecido por soluções de código fechado. Demandas específicas da PGDF podem exigir suporte imediato; • Recursos tecnológicos – um so*ftware* de código aberto, geralmente, necessita de funcionalidades mantidas por terceiros (prevenção de intrusões e ameaças, controle de aplicações, antivírus e filtragem de *URLs*). A possível descontinuação dessas funcionalidade(s) pode pode comprometer a segurança da rede. Outrossim, o *software open–source* padece de funcionalidades desejáveis; • Eficácia reduzida – as atualizações de segurança são fornecidas por uma comunidade de desenvolvedores. O so*ftware* pode ficar desatualizado e menos eficaz na proteção contra novas ameaças. A prestação de serviços pelo órgão pode ser prejudicada em razão de brechas na segurança; • Curva de aprendizado – um so*ftware* de código aberto pode exigir conhecimentos profundos de redes e segurança, aumentando a curva de aprendizado. É provável que seja necessária a contratação de profissionais capacitados e/ou suporte técnico qualificado para a operação da solução. Um software de código aberto mal configurado pode introduzir vulnerabilidades significativas na segurança. O processo de *hardening*, que envolve a redução de vulnerabilidades e proteção contra ataques, através da remoção de configurações padrão e aplicação de medidas de segurança, pode ser complexo e exigir a contratação de profissionais altamente capacitados ou suporte técnico qualificado. Isso pode aumentar os custos operacionais e a dependência de expertise externa. Além disso, o suporte oferecido para *software open–source* geralmente não é tão abrangente quanto o suporte disponível para soluções de código fechado. Em situações onde a PGDF necessita de suporte imediato, a falta de uma assistência técnica robusta pode resultar em atrasos na resolução de problemas críticos, comprometendo a segurança e a eficiência operacional. Outro ponto importante é a dependência de recursos tecnológicos mantidos por terceiros. Funcionalidades essenciais como prevenção de intrusões, controle de aplicações, antivírus e filtragem de *URLs* são frequentemente desenvolvidas e mantidas por comunidades ou empresas externas. A descontinuação dessas funcionalidades pode comprometer a segurança da rede, deixando-a vulnerável a novas ameaças. Além disso, o software de código aberto pode carecer de algumas funcionalidades desejáveis que são comuns em soluções proprietárias. As atualizações de segurança em *software* de código aberto são fornecidas por uma comunidade de desenvolvedores, o que pode resultar em atrasos na disponibilização de patches e correções. Isso pode deixar o *software* desatualizado e menos eficaz na proteção contra novas ameaças, aumentando o risco de brechas de segurança que podem prejudicar a prestação de serviços pelo órgão. Por fim, a curva de aprendizado associada ao uso de software de código aberto pode ser íngreme. A operação eficaz dessas soluções geralmente exige conhecimentos profundos de redes e segurança, o que pode aumentar a necessidade de contratação de profissionais capacitados ou suporte técnico qualificado. Isso não só eleva os custos, mas também pode retardar a implementação e a operação eficiente da solução. Embora o *software* de código aberto ofereça várias vantagens, como flexibilidade e economia de custos, as desvantagens relacionadas à complexidade, suporte, dependência de terceiros, eficácia reduzida e curva de aprendizado devem ser cuidadosamente avaliadas para garantir que a segurança da rede não seja comprometida.

4.2.1 – CUSTO TOTAL DE PROPRIEDADE: ANÁLISE PARA O "CENÁRIO 2"

Item	Descrição	Valor (R$)
–	–	–
TOTAL GERAL		–

4.3 – CENÁRIO 3

Entidade	–
Descrição	Aquisição de uma solução alternativa de segurança para a rede de computadores – *firewall* – com fornecimento de equipamentos, licenciamento de *softwares* e assistência técnica, objetivando substituir a atual solução.
Fornecedor	*Palo Alto Networks*, *Fortinet*, *Cisco*, *Check Point Software Technologies*, *SonicWall*, dentre outras
Análise da Solução	Trata-se da aquisição de uma solução alternativa de segurança para a rede de computadores, com vistas a substituir a atual solução adquirida por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), composta por: • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do órgão – sítio principal; • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do Instituto de Pesquisa e Estatística do Distrito Federal – IPEDF – sítio de contingência; • 01 (um) conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*), instalados na sede do órgão – sítio principal. O cenário apresenta as seguintes vantagens: • Tecnologia – a aquisição de uma nova solução permite a exploração de tecnologias e recursos mais recentes, com maior eficácia de proteção; • Funcionalidades – uma nova solução tende a oferecer recursos mais avançados, com maior eficácia contra ameaças; • Regulamentações – a PGDF pode se beneficiar com a capacidade da solução atender novas normas e regulamentos de segurança. O cenário apresenta as seguintes desvantagens: • Gastos – a contratação de nova solução de segurança envolve custos significativos. A opção pelo quadro resulta maior aporte de recursos públicos; • Implementação – a substituição dos dispositivos pode exigir tempo e esforço significativos para configuração, migração de políticas e testes; • Desperdício de recursos – os atuais equipamentos apresentam funcionamento adequado e atendem às demandas da PGDF. A contratação de uma nova solução pode ser considerada um desperdício de recursos públicos; • Suspensão dos serviços – a nova solução pode causar interrupções inesperadas na rede em razão da baixa maturidade do *software*/*firmware* de um equipamento novo; • Treinamento da equipe – uma nova solução de segurança pode apresentar uma interface ou funcionalidade diferente, dessa forma, é possível que haja a necessidade de treinamento para operação. Tecnologias mais recentes permitem a exploração de recursos avançados, proporcionando maior eficácia na proteção da rede. Soluções modernas tendem a oferecer funcionalidades mais avançadas, que são mais eficazes contra ameaças cibernéticas emergentes. Além disso, a nova solução pode ajudar a PGDF a cumprir regulamentações e normas de segurança atualizadas, garantindo que a instituição esteja em conformidade com os padrões exigidos. No entanto, a implementação de uma nova solução de segurança também apresenta desvantagens. Os gastos com a aquisição, implementação, operação e manutenção são uma preocupação significativa, pois a contratação de uma nova solução envolve um investimento considerável de recursos públicos. A implementação da nova solução pode exigir tempo e esforço significativos para configuração, migração de políticas e testes, o que pode causar interrupções nos serviços. Além disso, a substituição dos equipamentos atuais, que ainda funcionam adequadamente e atendem às demandas da PGDF, pode ser vista como um desperdício de recursos. Outra desvantagem é a possível suspensão dos serviços durante a transição para a nova solução, devido à baixa maturidade do *hardware* e/ou *software* dos novos equipamentos. Isso pode resultar em interrupções inesperadas na rede. Por fim, a nova solução pode apresentar uma interface ou funcionalidades diferentes, exigindo treinamento da equipe para garantir a operação eficaz, o que pode aumentar os custos e o tempo necessário para a adaptação.

4.3.1 – CUSTO TOTAL DE PROPRIEDADE: ANÁLISE PARA O "CENÁRIO 3"

Item	Descrição	Valor (R$)
–	–	–
TOTAL GERAL		–

4.4 – CENÁRIO 4	
Entidade	NCT Informática Ltda., Heimdallr Cybersecurity Ltda., Qualitek Tecnologia Ltda. – EPP
Descrição	Contratação de suporte para a atual solução de segurança para rede de computadores – *firewall,* sem atualização de *hardware* dos equipamentos.
Fornecedor	*Fortinet*
	Trata–se da contratação de assistência/suporte técnico para os elementos que compõem a atual solução de segurança para rede de computadores – *firewall* – com licenciamento de módulo(s) e ampliação do ciclo de garantia da solução do tipo *Next Generation Firewall* (*NGFW*) da empresa *Fortinet*, adquirida por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), composta por: • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do órgão – sítio principal; • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do Instituto de Pesquisa e Estatística do Distrito Federal – IPEDF – sítio de contingência; • 01 (um) conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*), instalados na sede

do órgão – sítio principal.

Esta perspectiva apresenta um cenário de contratação de assistência técnica para apoio à operação da atual solução de segurança para rede de computadores, sem atualização tecnológica dos equipamentos.

O cenário apresenta as seguintes vantagens:

- Suporte técnico – A contratação de período adicional de assistência/suporte técnico mantém a sustentação dos dispositivos da solução de segurança;
- Atualizações – A contratação de assistência/suporte técnico inclui as atualizações regulares de *software* e *firmware*. Tais melhoramentos são fundamentais para manutenção da segurança e do desempenho da solução, corrigindo vulnerabilidades e melhorando a funcionalidade da mesma;
- Substituições – A assistência/suporte técnico compreende uma política de substituição do dispositivo em caso de problema com o mesmo. Isso pode reduzir o impacto por tempos de inatividade prolongados e custos de recuperação;
- Regulamentações – A contratação colabora com a conformidade de regulamentos de segurança cibernética;

O cenário apresenta as seguintes desvantagens:

- Atualizações tecnológicas – Equipamentos mais antigos tornam–se menos eficazes na proteção contra ameaças. Se o ciclo de vida do produto está próximo do fim, o investimento em um novo dispositivo pode ser necessário para manter a segurança atualizada;
- Alternativas de Terceiros – Alguns fornecedores podem oferecer soluções de segurança a custos mais competitivos que as renovações de garantia do fabricante;
- Dependência tecnológica – O órgão pode se tornar dependente do fabricante da solução, limitando a flexibilidade para a adoção de novas soluções de segurança.

A opção pelo cenário de contratação de suporte para a atual solução de segurança para rede de computadores resulta em relativa economicidade a curto prazo, considerando a desnecessidade de aquisição de novos equipamentos e das etapas de instalação, configuração e treinamento para operação e manutenção dos dispositivos já existentes.

Cabe destacar que os **equipamentos mais antigos** podem se tornar menos eficazes na proteção contra novas ameaças, podendo ser necessário ter que investir em novos dispositivos para manter a segurança atualizada. É importante considerar também que os equipamentos instalados no sítio de contingência estão próximos do fim do ciclo de vida do produto (132847496), ***Product support expires: 17Aug2026***.

Análise da Solução

Para estabelecer os custos envolvidos na contratação, a equipe de planejamento realizou pesquisa de preços de acordo com o inciso VI, do §1º, art. 18 da Lei nº 14.133/2021:

Item	Descrição	Quantidade	Empresa 1 (141480578)	Empresa 2 (142571977)	Empresa 3 (142572158)
			Valor Unitário (R$)	Valor Unitário (R$)	Valor Unitário (R$)
1.	Suporte para 02 equipamentos até 17 de agosto de 2026 – sítio de contingência	02	36.524,48	40.979,34	35.600,00
2.	Suporte para 02 equipamentos por período de 36 meses – Sítio Principal	02	53.941,58	63.951,99	68.607,00
3.	Suporte para *softwares* de gerenciamento de equipamentos e *logs*, caixa de areia (*sandbox*) e gestão de usuários por período de 36 meses	01	181.538,69	145.551,53	213.117,60

Tabela 1. Valores de referência do cenário 4

A tabela abaixo apresenta planilha comparativa com os valores provenientes das propostas recebidas:

Item	Mediana (com valores discrepantes) (R$)	Mínimo (-50%) (R$)	Máximo (+50%) (R$)	Mediana Final (R$)	Média Final (R$)	Quantidade	Por Ano (/3 anos) (R$)	Valor Total (R$)
1.	36.524,48	18.262,24	54.786,72	36.524,48	37.701,27	2	12.174,83	73.048,96
2.	63.951,99	31.976,00	95.927,99	63.951,99	62.166,86	2	20.722,29	124.333,72
3.	181.538,69	90.769,35	272.308,04	181.538,69	180.069,27	1	60.023,09	180.069,27
TOTAL GERAL							**92.920,21**	**377.451,95**

Tabela 2. Planilha comparativa com valores de referência do cenário 4

4.4.1 – CUSTO TOTAL DE PROPRIEDADE: ANÁLISE PARA O "CENÁRIO 4"		
Item	**Descrição**	**Valor (R$)**
1.	Suporte para 02 equipamentos até 17 de agosto de 2026 – sítio de contingência	73.048,96
2.	Suporte para 02 equipamentos por período de 36 meses – sítio principal	124.333,72
3.	Suporte para *softwares* de gerenciamento de equipamentos e *logs*, caixa de areia (*sandbox*) e gestão de usuários por período de 36 meses	180.069,27
TOTAL GERAL		**377.451,95**

4.5 – CENÁRIO 5	
Entidade	NCT Informática Ltda., Heimdallr Cybersecurity Ltda., Qualitek Tecnologia Ltda. – EPP
Descrição	Contratação de suporte e atualização tecnológica para a atual solução de segurança para rede de computadores – *firewall,* com atualização de *hardware* dos equipamentos.
Fornecedor	*Fortinet*
	Trata–se da contratação de assistência/suporte técnico e atualização tecnológica para os elementos que compõem a atual solução de segurança para rede de computadores – *firewall* – com licenciamento de módulo(s) e ampliação do ciclo de garantia da solução do tipo *Next Generation Firewall* (*NGFW*) da empresa *Fortinet*, adquirida por intermédio do Pregão Eletrônico nº 04/2020 (00020-00045053/2019-01), composta por: • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do órgão – sítio principal; • 02 (dois) equipamentos agregados, em alta disponibilidade, instalados na sede do Instituto de Pesquisa e Estatística do Distrito Federal – IPEDF – sítio de contingência; • 01 (um) conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*), instalados na sede do órgão – sítio principal. Esta perspectiva apresenta um cenário de contratação de assistência técnica para apoio à operação da atual solução de segurança para rede de computadores, com atualização tecnológica dos equipamentos. O cenário apresenta as seguintes vantagens: • Suporte técnico – A contratação de um período adicional de assistência/suporte técnico assegura a continuidade no funcionamento dos dispositivos da solução de segurança; • Atualizações – A contratação de assistência/suporte técnico inclui atualizações regulares de *software* e *firmware*, essenciais para manter a segurança e o desempenho da solução, corrigindo vulnerabilidades e aprimorando suas funcionalidades; • Substituições – O suporte técnico abrange uma política de substituição dos dispositivos em caso de falha, minimizando o impacto de eventuais períodos de inatividade e os custos associados à recuperação; • Regulamentações – A contratação contribui para a conformidade com as normas e regulamentos de segurança cibernética; • Desempenho e Recursos – Os equipamentos instalados no site de contingência estão próximos do fim de seu ciclo de vida. Dispositivos mais modernos oferecem desempenho superior, o que pode otimizar a segurança e a eficiência da rede; • Suporte Estendido – A aquisição de equipamentos mais novos possibilita a contratação de um período mais longo de suporte técnico, o que pode reduzir os custos anuais com manutenção, suporte e atualizações; • Benefícios a Longo Prazo – A implementação dessas medidas resulta em vantagens contínuas, tanto em termos de segurança quanto de desempenho. O cenário apresenta as seguintes desvantagens: • Implementação – Substituir um dispositivo em término do ciclo de vida pode exigir tempo e esforço significativos para configurá–lo e usá–lo efetivamente (em razão de recursos diferentes ou avançados); • Alternativas de Terceiros – Alguns fornecedores podem oferecer soluções de segurança a custos mais competitivos que as renovações de garantia do fabricante; • Dependência tecnológica – O órgão pode se tornar dependente do fabricante da solução, limitando a flexibilidade para a adoção de novas soluções de segurança. A contratação de um período adicional de assistência e suporte técnico, juntamente com a atualização tecnológica, oferece diversos benefícios. Primeiramente, o suporte contínuo garante a operação e a eficácia dos dispositivos da solução de segurança. Além disso, inclui atualizações regulares de *software* e *firmware*, essenciais para manter a segurança e o desempenho da solução, corrigindo vulnerabilidades e aprimorando funcionalidades. Outra vantagem importante é a política de substituição dos dispositivos em caso de falhas, o que minimiza os impactos de períodos prolongados de inatividade e os custos de recuperação. A contratação também contribui para assegurar a conformidade com as regulamentações de segurança cibernética, um aspecto fundamental para a PGDF. Além disso, a atualização de equipamentos, especialmente aqueles próximos ao fim de seu ciclo de vida, melhora o desempenho e os recursos da rede, aumentando a segurança e a eficiência operacional. A aquisição de equipamentos mais modernos permite a contratação de um período mais longo de suporte técnico, o que pode resultar na redução dos gastos com manutenção, suporte e atualizações. Para estabelecer os custos envolvidos na contratação, a equipe de planejamento realizou pesquisa de preços de acordo com o inciso VI, do §1º, art. 18 da Lei nº 14.133/2021:

Item	Descrição	Quantidade	Empresa 1 (141480901)	Empresa 2 (142572031)	Empresa 3 (142572158)
			Valor Unitário (R$)	Valor Unitário (R$)	Valor Unitário (R$)
1.	Atualização tecnológica de 02 equipamentos (ID SEI 122228882 – *Replacement SKU: FG–100F*) com garantia de 60 meses – sítio de contingência	02	111.116,56	112.545,95	133.600,00
2.	Suporte para 02 equipamentos por período de 60 meses – sítio principal	02	89.324,84	106.399,98	114.394,50
3.	Suporte para *softwares* de gerenciamento de equipamentos e *logs*, caixa de areia (*sandbox*) e gestão de usuários por período de 60 meses	01	311.709,86	226.387,97	213.117,30

Tabela 3. Valores de referência do cenário 5

A tabela abaixo apresenta planilha comparativa com os valores provenientes das propostas recebidas:

Item	Mediana (com valores discrepantes)	Mínimo (-50%)	Máximo (+50%)	Mediana Final	Média Final	Quantidade	Por Ano (/5 anos) (R$)	Valor Total (R$)
1.	112.545,95	56.272,98	168.818,93	112.545,95	119.087,50	2	22.509,19	225.091,90
2.	106.399,98	53.199,99	159.599,97	106.399,98	103.373,11	2	20.674,62	206.746,22
3.	226.387,97	113.193,99	339.581,96	226.387,97	250.405,04	1	45.277,59	226.387,97
TOTAL GERAL =							**88.461,40**	**658.226,09**

Tabela 4. Planilha comparativa com valores de referência do cenário 5

4.5.1 – CUSTO TOTAL DE PROPRIEDADE: ANÁLISE PARA O "CENÁRIO 5"

Item	Descrição	Valor (R$)
1.	Atualização tecnológica de 02 equipamentos (122228882 – *Replacement SKU: FG–100F*) com garantia de 60 meses – sítio de contingência	225.091,90
2.	Suporte para 02 equipamentos por período de 60 meses – sítio principal	206.746,22
3.	Suporte para *softwares* de gerenciamento de equipamentos e *logs*, caixa de areia (*sandbox*) e gestão de usuários por período de 60 meses	226.387,97
TOTAL GERAL		**658.226,09**

5 – ANÁLISE COMPARATIVA DAS SOLUÇÕES

A decisão entre os cenários deve levar em conta não apenas os custos imediatos, mas também os benefícios a longo prazo relacionados à segurança e ao desempenho. A avaliação minuciosa dos requisitos e a comparação das soluções identificadas são fundamentais para uma escolha estratégica e fundamentada.

O quadro a seguir compara alguns dos requisitos encontrados nas soluções identificadas:

Requisitos		**Cenários**				
		Cenário 1	Cenário 2	Cenário 3	Cenário 4	Cenário 5
Negócio	Manter a segurança da rede de computadores da Procuradoria–Geral do Distrito Federal – PGDF	não atende	atende	atende	atende	atende
	Manter a efetividade da gestão da Segurança da Informação	não atende	atende	atende	atende	atende
	Manter a disponibilidade dos serviços providos pela PGDF	não atende	atende	atende	atende	atende
	Manter a prevenção contra ameaças externas à rede da PGDF	não atende	atende	atende	atende	atende
Tecnológico	Permitir a adequação às necessidades da PGDF	não atende	atende	atende	não atende	atende
	Permitir o controle do fluxo do tráfego entre redes distintas	atende	atende	atende	atende	atende
	Permitir a inspeção do estado das conexões de rede	atende	atende	atende	atende	atende
	Permitir a tradução de endereços para preservação da topologia da rede interna	atende	atende	atende	atende	atende
	Permitir o controle do uso de aplicativos não autorizados ou potencialmente perigosos	não atende	não atende	atende	atende	atende
	Permitir a inspeção do tráfego criptografado para aplicação de políticas de segurança e conformidade	atende	atende	atende	atende	atende
	Permitir a análise dos padrões de tráfego em busca de atividades maliciosas	não atende	não atende	atende	atende	atende
	Permitir a detecção de anomalias e comportamentos suspeitos	não atende	não atende	atende	atende	atende
	Permitir a aplicação de políticas de segurança e conformidade	não atende	não atende	atende	atende	atende
	Permitir o controle de acesso a recursos com base em identidades confiáveis	não atende	não atende	atende	atende	atende
Econômico	Princípio da Economicidade*	não se aplica	não se aplica	não atende	atende	atende
Resultado da Análise		**não viável**	**não viável**	**não viável**	**viável**	**viável**

*Princípio que objetiva a minimização dos gastos públicos, sem comprometimento dos padrões de qualidade. Refere–se à capacidade de uma instituição gerir adequadamente os recursos financeiros colocados à sua disposição.

5.1 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Os cenários **1**, **2**, **3** e **4** foram considerados e descartados, conforme registra–se abaixo:

- O **Cenário 1** resultaria em economicidade e possibilidade de alocação de recursos econômicos para outras necessidades críticas, no entanto, traz uma série de riscos significativos para a prestação de serviços pela PGDF. Dessa forma, em razão dos riscos significativos e considerando o impacto das desvantagens elencadas acima, opta–se pela eliminação deste cenário;
- O **Cenário 2** resultaria em economicidade (considerando apenas a necessidade de aquisição dos equipamentos) e possibilidade de personalização do *software* para execução de demandas específicas da PGDF, no entanto, traz complexidade para operação da solução e indisponibilidade de recursos técnicos necessários para manutenção da a segurança da rede e para a prestação de serviços pela PGDF. Desta maneira, considerando os riscos envolvidos dada a complexidade e indisponibilidade de alguns recursos para manutenção da segurança da rede, opta–se pela eliminação deste cenário.
- O **Cenário 3** resultaria em maior custo financeiro, considerando a necessidade de substituição de todos os equipamentos e da inevitabilidade da contratação das etapas de instalação, configuração e treinamento para operação, ensejando maior dispêndio de recursos públicos. O cenário ainda elimina a vantagem econômica da contratação de período de suporte técnico para o atual produto. Dessa forma, considerando os esforços necessários para a configuração, migração de políticas e testes, os esforços necessários para reinstalação de todos os clientes de rede privada virtual, a proteção do investimento anteriormente efetuado em dispositivos, a necessidade de transferência de conhecimento/treinamento para a operação da nova solução (o que pode ocasionar, inclusive, inúmeras brechas na segurança da rede), opta–se pela eliminação deste cenário;
- O **Cenário 4**, que analisa a contratação de suporte para a atual solução de segurança para rede de computadores (*firewall*) sem atualização de *hardware* dos equipamentos, apresenta vantagens e desvantagens tecnológicas e de negócio. No entanto, os equipamentos instalados no sítio de contingência da PGDF estão próximos do fim do ciclo de vida do produto (132847496), com expiração em **17 de agosto de 2026**. Dessa forma, a contratação descrita no presente cenário poderia incorrer em perda de eficácia na proteção contra ameaças, em razão da manutenção de produtos desatualizados e/ou sem suporte do fabricante.

6 – MAPA COMPARATIVO DOS CUSTOS TOTAIS DE PROPRIEDADE

Cenário	Estimativa de TCO ao longo dos anos					Total (R$)
	Ano 1 (R$)	Ano 2 (R$)	Ano 3 (R$)	Ano 4 (R$)	Ano 5 (R$)	
1. Manutenção da atual solução de segurança para rede de computadores – *firewall* – pela própria PGDF, sem a contratação de assistência técnica e/ou equipamento(s), consequentemente, renunciando aos módulos de filtragem de endereços, controle de aplicações, dentre outras funcionalidades da solução do tipo *Next Generation Firewall* (*NGFW*).	–	–	–	–	–	–
2. Aquisição de servidores e / o u *appliances*, com características específicas de desempenho, para montagem de solução de segurança para rede de computadores – *firewall* – u t i l i z a n d o *software* de código aberto (*open–source*), tencionando substituir a atual solução.	–	–	–	–	–	–
3 . Aquisição de uma solução alternativa de segurança para a rede de computadores – *firewall* – com fornecimento de equipamentos, licenciamento de *softwares* e assistência técnica, objetivando substituir a atual solução.	–	–	–	–	–	–
4 . Contratação de suporte para a atual solução de segurança para rede de computadores – *firewall,* sem atualização de *hardware* dos equipamentos.	125.817,33	125.817,33	125.817,33	–	–	**377.451,95**

5. Contratação de suporte e atualização tecnológica para a atual solução de segurança para rede de computadores – *firewall,* com atualização de *hardware* dos equipamentos.	131.645,21	131.645,21	131.645,21	131.645,21	131.645,21	**658.226,09**

7 – JUSTIFICATIVA DO CENÁRIO ESCOLHIDO

Cenário	Descrição
5	**7.1 – DA JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DA SOLUÇÃO** O "Cenário 5" apresenta uma solução mais robusta e eficiente em termos de segurança e desempenho, proporcionando maior estabilidade e proteção para a rede de computadores da PGDF, destacando-se como a opção mais vantajosa. As principais vantagens incluem: • **Suporte Técnico Contínuo**: Mantém a sustentação dos dispositivos da solução de segurança. • **Atualizações Regulares**: Inclui melhorias de software e firmware, fundamentais para corrigir vulnerabilidades e melhorar a funcionalidade. • **Política de Substituição**: Reduz o impacto de tempos de inatividade prolongados e custos de recuperação. • **Conformidade com Regulamentações**: Ajuda a garantir que a PGDF esteja em conformidade com normas de segurança cibernética. • **Desempenho Aprimorado**: Equipamentos mais recentes oferecem melhor desempenho e eficiência. • **Suporte Estendido**: Permite a contratação de períodos maiores de suporte técnico, resultando em custos anuais menores. A atual solução do tipo *Next Generation Firewall* (*NGFW*) da empresa *Fortinet* é composta por: • 02 equipamentos agregados, em alta disponibilidade, instalados na sede do órgão; • 02 equipamentos agregados, em alta disponibilidade, instalados na sede da Companhia de Planejamento do Distrito Federal; • 01 conjunto de *softwares* de gerenciamento de equipamentos e *logs* e caixa de areia (*sandbox*). Opta-se pela aquisição de um pacote de licenciamento que inclua módulos de prevenção contra intrusões e ameaças, controle de aplicativos, antivírus e filtragem de URLs (Uniform Resource Locator – Localizador Padrão de Recursos), atualização tecnológica dos equipamentos, além de software para análise de registros (logs) e garantia (assistência/suporte técnico) por 60 meses. Essa abordagem preserva parte dos dispositivos, moderniza os produtos cujo ciclo de vida se encerra em 17/08/2026 (122228882) e elimina a necessidade de treinamentos para operação. A análise da equipe de planejamento foi realizada de acordo com os seguintes critérios: • Aproveitamento de materiais, políticas e tecnologias padronizadas que visam, principalmente, garantir a segurança das informações; • Manutenção de solução de segurança com práticas e tecnologias modernas; • Padronização dos *firewalls* administradas pela Gerência de Segurança de Rede e Produção (Geseg), conforme art. 40, inc. V, alínea "a" da Lei 14.133/21 de 01 de Abril de 2021: *"Art. 15. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte: (...) V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;"* • Aproveitamento dos conhecimentos técnicos utilizados na manutenção e conservação dos atuais produtos, bem como o uso de insumos que atendam os atuais e futuros dispositivos; • Eliminação da pulverização de soluções, gerando heterogeneidade e garantindo a gerenciabilidade da solução; • Quantidade considerável de empresas credenciadas pelo fabricante dos equipamentos e capazes de fornecer o objeto e prestar os serviços desejados, não implicando em inexigibilidade de licitação; • Adequação às necessidades atuais da PGDF. Em relação aos demais cenários, alguns podem limitar, agregar os riscos durante e após a implantação: • Adoção de solução de segurança inadequada para as necessidades atuais da PGDF; • Redução da eficácia na proteção contra ameaças em virtude do ciclo de vida de um dos produtos estar próximo do fim e/ou adoção de solução de segurança com baixa maturidade do *software*/*firmware* dos equipamentos; • Aumento da exposição a novas ameaças e vulnerabilidades em virtude da desatualização do produto atual, da má configuração ou da complexidade de outra solução de segurança; • Incapacidade ou capacidade limitada de fornecer segurança de perímetro digital à PGDF, prejudicando a prestação de serviços pelo órgão e elevando custos de recuperação; • Necessidade de treinamento para operação de outra solução de segurança, com interfaces e/ou funcionalidades distintas e/ou contratação de profissionais capacitados e/ou suporte técnico qualificado para manter os novos produtos. Esses fatores combinados tornam o "Cenário 5" uma opção vantajosa, oferecendo segurança e desempenho aprimorados, com custos operacionais mais eficientes a longo prazo.

7.2 – DO PARCELAMENTO OU NÃO COM BASE NA JUSTIFICATIVA

A não divisão do objeto pretendido em vários grupos ocorre devido à possibilidade de prejuízos à Administração Pública, em razão dos riscos inerentes à execução e aos danos ao serviço demandado. Não há dúvidas de que, se o objeto for executado por diferentes contratados, ele poderá não ser prestado de forma integral ou satisfatória.

Os serviços solicitados exigem a prestação por profissionais capacitados e treinados especificamente para o desempenho dessas atividades. Considerando a indisponibilidade de mão de obra qualificada suficiente nos quadros da Administração para atender à demanda, torna-se necessária a contratação externa.

A decisão da equipe de planejamento foi fundamentada na necessidade de agrupar elementos correlatos em um único grupo, uma vez que estes estão intimamente relacionados entre si. Esse agrupamento visa minimizar os riscos e dificuldades associados à pluralidade de contratos independentes. Além disso, a consolidação contribui para um gerenciamento mais eficiente do contrato, além de gerar economia de escala.

7.3 – BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

Id.	Bem/Serviço	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1.	Atualização tecnológica de equipamentos com garantia de 60 meses – sítio de contingência	02	112.545,95	225.091,90
2.	Suporte para equipamentos por período de 60 meses – sítio principal	02	103.373,11	206.746,22
3.	Suporte para *softwares* de gerenciamento de equipamentos e *logs*, caixa de areia (*sandbox*) e gestão de usuários por período de 60 (sessenta) meses	01	226.387,97	226.387,97
TOTAL		05	442.307,03	**658.226,09**

7.4 – ALINHAMENTO EM RELAÇÃO AOS INSTRUMENTOS DE PLANEJAMENTO ADMINISTRATIVO

7.4.1 – ALINHAMENTO EM RELAÇÃO AO PAC

O objeto da contratação está previsto no Plano de Contratações Anual (PCA–PGDF 2024), conforme consta do documento SEI 132554353, anexado a este processo

7.4.2 – ALINHAMENTO EM RELAÇÃO AO PEI E AO PDTI

Objetivo Estratégico do Requisitante previsto no PEI	Necessidade do PDTI	Meta do PDTI	Ações previstas no PDTI
Gerar a transformação digital para a entrega de valor público ao cidadão.	NI12 Infraestrutura de TI adequada.	M50 – Adquirir e/ou renovar garantia de *firewall.*	A50.1 – Planejar aquisição de solução de *firewall*
			A50.2 – Selecionar o fornecedor para aquisição solução de *firewall*
			A50.3 – Instalar e configurar solução de *firewall*

7.5 – BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

7.5.1. Prevenção e proteção contra ameaças cibernéticas

7.5.2. Controle de acesso às redes de dados

7.5.3. Manutenção da segmentação e do desempenho das redes de dados

7.5.4. Manutenção do controle e da segurança do tráfego de dados

7.5.5. Manutenção dos recursos de registro e auditoria

7.5.6. Manutenção das políticas de segurança para atender as necessidades do órgão

7.5.7. Sustentação da gestão da Política de Segurança da Informação da instituição

8 – NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE INTERNO PARA EXECUÇÃO CONTRATUAL

8.1. A PGDF possui atualmente um centro de dados com dois ambientes interligados (principal e secundário). **Não são necessárias adequações iminentes no ambiente interno para execução contratual**.

9 – RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

9.1 – RECURSOS MATERIAIS E/OU TECNOLÓGICOS

9.1.1 – RECURSO 1

Tipo	*Hardware*
Identificação	*Switch L3* / Roteador
Descrição	Equipamento(s) para estabelecimento de Enlace de Dados – Rede de Área Metropolitana GDFNET
Quantidade	3 unidades
Ações para Obtenção do Recurso	**Responsáveis pela Obtenção do Recurso**
Uma unidade fornecida pela Subsecretaria de Tecnologia da Informação e Comunicação do GDF	SUTIC/SEPLAD
Uma unidade existente	SUTIC/PGDF
Duas unidades a serem adquiridas para substituição do equipamento existente	SUTIC/PGDF
9.1.2 – RECURSO 2	
Tipo	*Hardware*
Identificação	*Switch L3*
Descrição	Equipamento(s) de comutação (*switches*) para o topo de *rack* (*ToR*) e o núcleo (*CORE*)
Quantidade	4 unidades
Ações para Obtenção do Recurso	**Responsáveis pela Obtenção do Recurso**
Quatro unidades existentes	SUTIC/PGDF
Quatro unidades a serem adquiridas para substituição dos equipamentos existentes	SUTIC/PGDF
9.1.3 – RECURSO 3	
Tipo	*Hardware*
Identificação	Servidor
Descrição	Equipamento(s) para execução de programa(s) relacionado(s) e armazenagem de dados
Quantidade	1 unidade
Ações para Obtenção do Recurso	**Responsáveis pela Obtenção do Recurso**
Uma unidade existente	SUTIC/PGDF
A execução de programa(s) relacionado(s) e a armazenagem de dados serão realizadas no centro de dados a ser adquirido	SUTIC/PGDF
9.2 – RECURSOS HUMANOS	
9.2.1 – RECURSO 1	
Identificação	Técnico em Tecnologia da Informação
Definição	Profissional designado para realizar configurações de sistemas de informática, instalar equipamentos e verificar ocorrências na infraestrutura
Quantidade	1 profissional da Contratante 1 profissional da Contratada
Atribuições	Implementação e manutenção de infraestrutura, equipamentos de acesso e serviços de rede, aplicando normas de segurança e padrões técnicos
Formação	Curso técnico ou tecnólogo completo em tecnologia da informação
9.2.2 – RECURSO 2	

Identificação	Analista de Sistemas
Definição	Profissional designado para realizar a manutenção da estrutura física de computadores e servidores, da estrutura de rede de área local de computadores e de sistemas operacionais
Quantidade	1 profissional da Contratante 1 profissional da Contratada
Atribuições	Implementação, manutenção e ampliação das redes locais Configuração e manutenção da segurança de rede, aplicando normas de segurança e padrões técnicos Atualização de versões de aplicativos e configurações
Formação	Graduação completa em análise de sistemas e/ou áreas afins Desejável pós–graduação na área de redes de computadores

10 – DECLARAÇÃO DE VIABILIDADE

Declaramos que o **"Contratação de suporte e atualização tecnológica para a atual solução de segurança para rede de computadores – *firewall,* com atualização de *hardware* dos equipamentos"** é o **mais vantajoso para a administração pública,** considerando as necessidades atuais e futuras da rede da PGDF, bem como da eficácia da presente solução, torna imperiosa a contratação de período adicional de assistência/suporte técnico e atualização tecnológica de dispositivos de segurança para rede de computadores – *firewall*. A contratação de maior período de suporte técnico e atualização tecnológica de produtos torna–se vantajosa, tendo em vista que oferece maior estabilidade para o ambiente operacional.

Dentre os benefícios estão: a manutenção da proteção do perímetro digital; a compatibilidade de *hardware* e *software* com a atual solução; a desnecessidade de substituição de todos os equipamentos, considerando que alguns equipamentos estão próximos do fim do ciclo de vida do produto e outros não possuem anúncio de descontinuação iminente pelo fabricante; a dispensabilidade de efetuar treinamentos para operação; e a familiaridade dos usuários com os recursos presentes no produto em uso pela instituição.

Tal aquisição mantém a segurança cibernética e a proteção contra ameaças potenciais.

O presente ESTUDO TÉCNICO PRELIMINAR, considerando a fundamentação aduzida aos autos relativamente às necessidades a serem atendidas, ao alinhamento com o planejamento institucional, elaborado pelos integrantes técnico e requisitante em harmonia com o disposto na legislação que dispõe sobre contratos e licitações, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, **conclui pela VIABILIDADE DA CONTRATAÇÃO**.

11 – ASSINATURAS

O presente Estudo Técnico Preliminar (ETP) está em conformidade com o disposto no art. 18, inciso I da Lei nº 14.133, de 1º de abril de 2021 e com o art. 11 da Instrução Normativa nº 94, de 23 de dezembro de 2022, emitida pela Secretaria de Governo Digital, recepcionada, em seu art. 269–A, pelo Decreto 44.330, de 16 de março de 2023.

O ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação e tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização de Demanda (DFD), caracterizando a melhor solução para o atendimento ao interesse público.

11.1 – INTEGRANTES TÉCNICOS

Douglas Rafael Morais Kollar Integrante Técnico Matrícula: 226.096–4	**Ricardo Wagner de Melo** Integrante Técnico Matrícula: 40.532–9

11.2 – INTEGRANTE REQUISITANTE

Paulo Alves Pereira
Integrante Requisitante
Matrícula: 34.036-7

11.3 – AUTORIDADE MÁXIMA DA ÁREA DE TI

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

ADRIANA BORGES ARAÚJO
Subsecretária-Geral de Tecnologia da Informação Substituta
Matrícula: 247.072-1

Documento assinado eletronicamente por **DOUGLAS RAFAEL MORAIS KOLLAR - Matr.0226096-4**, **Integrante Técnico(a)**, em 29/01/2025, às 14:44, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **PAULO ALVES PEREIRA - Matr.0034036-7**, **Integrante Requisitante**, em 29/01/2025, às 15:48, conforme art. 10, §2º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Certificado ICP-Brasil Nº de Série do Certificado: 534516940790578335319370249 4.

Documento assinado eletronicamente por **RICARDO WAGNER DE MELO - Matr.0040532-9**, **Integrante Técnico(a)**, em 03/02/2025, às 15:11, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **LORENZA D'ONOFRIO CARNEIRO - Matr.0221656-6**, **Subsecretário(a)-Geral de Tecnologia da Informação**, em 03/02/2025, às 15:20, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **161539721** código CRC= **FA076984**.