AGENCIA NACIONAL DO PETROLEO - ANP - RJ

Estudo Técnico Preliminar 4/2026

1. Informações Básicas

Número do processo: 48610.201345/2026-74

2. Descrição da necessidade

A presente contratação tem por finalidade adquirir solução integrada de segurança e conectividade, composta pela substituição dos firewalls corporativos Fortinet 1500D por novos equipamentos do tipo Next Generation Firewall (NGFW), bem como pela implantação de solução de rede sem fio corporativa (WiFi) totalmente integrada ao ecossistema Fortinet utilizado pela ANP. A solução contempla:

- Implementação de firewalls NGFW com inspeção profunda de tráfego, prevenção de intrusões, controle de aplicações, Web Filter, AntiSpam, AntiMalware e VPN.
- Subscrições de segurança FortiGuard/UTP, suporte técnico especializado, atualizações e manutenção durante todo o período contratual.
- Integração total com FortiAnalyzerVM, FortiManager, FortiToken Mobile e FortiNAC, incluindo licenciamento para 1.600 dispositivos e 650 tokens.
- Consolidação e análise centralizada de logs, com maior capacidade de retenção e recursos aprimorados introduzidos nas versões mais recentes do FortiOS.
- Implantação de infraestrutura de rede sem fio com switches multigigabit PoE/PoE+ e Access Points corporativos gerenciados de forma nativa pelo firewall.
- Serviços profissionais de instalação, migração, configuração, documentação e operação assistida, garantindo o pleno funcionamento da solução integrada.

A contratação visa assegurar conectividade segura, moderna e de alto desempenho, com operação unificada de firewall, rede cabeada e rede sem fio, em conformidade com as necessidades institucionais da ANP.

2.1. Motivação/Justificativa

A contratação justificase pela necessidade de substituição imediata dos firewalls Fortinet 1500D, que se encontram em fim de ciclo de vida (EoL), deixando de receber atualizações críticas e impossibilitando a manutenção adequada da segurança perimetral da ANP. Conforme informado pelo fabricante:

- End of Order (EOO): 31/12/2021
- Última data para extensão de manutenção: 31/12/2025
- Expiração total de suporte (Product Support Expires): 31/12/2026
- Última versão de firmware suportada: FortiOS 7.2, incompatível com versões atuais (7.4+)
  .pdf) [TR_323031-...6-2026 (3) | PDF]

Essa limitação inviabiliza a aplicação de correções, atualizações de segurança e funcionalidades recentes, incluindo recursos avançados de análise e inteligência artificial introduzidos no FortiOS 7.4. A continuidade do uso desses equipamentos aumenta significativamente o risco cibernético, impactando diretamente a integridade, a disponibilidade e a confidencialidade das informações institucionais.

Além disso:

- O FortiAnalyzer atual encontra limitações de capacidade e funcionalidades devido às restrições dos firewalls 1500D, especialmente quanto à evolução tecnológica na análise e retenção de logs.
- A ANP possui parque Fortinet consolidado há mais de 10 anos (FortiAnalyzer, FortiManager, FortiToken, FortiGuard), cuja interoperabilidade depende da continuidade da mesma plataforma.
- A equipe técnica está capacitada e experiente na tecnologia Fortinet, reduzindo riscos operacionais, custos e curva de aprendizado.

Paralelamente, a organização necessita implementar rede sem fio corporativa moderna para suportar:

- Crescimento da demanda por mobilidade, dispositivos conectados e aplicações de alto desempenho.
- Integração nativa com o firewall para aplicação unificada de políticas de segurança, segmentação e autenticação (incluindo FortiNAC).
- Conectividade contínua, segura e de alta densidade em ambientes corporativos.

A implantação de switches multigigabit PoE/PoE+ e Access Points integrados ao Security Fabric elimina a necessidade de soluções paralelas, reduz pontos de falha, simplifica a administração e melhora a segurança e a governança da infraestrutura de TI.

A contratação também inclui serviços especializados de instalação, configuração, migração e operação assistida, essenciais para garantir implantação correta, mitigação de riscos e continuidade operacional.

Dessa forma, a solução proposta preserva investimentos anteriores, moderniza o ambiente tecnológico, reduz riscos de segurança e assegura a continuidade dos serviços críticos de TI da ANP.

3. Área requisitante

Área Requisitante	Responsável
Superintendência de Tecnologia da Informação	Daniella Christina Xavier de Oliveira

4. Necessidades de Negócio

4.1. A contratação da solução integrada de segurança e conectividade deve atender às seguintes necessidades de negócio, em conformidade com o Termo de Referência:

4.1.1. Manutenção e evolução da segurança perimetral

- Manter a segurança de borda da ANP com visibilidade completa de ativos, usuários, aplicações e tráfego, garantindo inspeção SSL, prevenção de intrusões (IPS), controle de aplicações, filtragem de conteúdo, proteção AntiMalware/AntiSpam e VPN corporativa.
- Assegurar continuidade operacional sem regressão funcional, incluindo migração e replicação das regras, objetos, rotas, políticas UTM e demais parâmetros existentes nos firewalls atuais, com aceites provisório e definitivo conforme procedimentos do TR.
- Sustentar mecanismos de autenticação forte e controle de acesso, incluindo OTP/MFA para 650 usuários e NAC para até 1.600 dispositivos, integrados nativamente ao ecossistema Fortinet (FortiToken, FortiNAC).
- Garantir suporte técnico 24x7, RMA e atualizações contínuas do fabricante ao longo de toda a vigência contratual, preservando a segurança, disponibilidade e integridade do ambiente.

4.1.2. Integração total dos componentes da solução

- Assegurar operação unificada entre firewall, switches, pontos de acesso, NAC, UTP, FortiAnalyzer e FortiToken, conforme modelo integrado Fortinet Security Fabric adotado pela ANP, evitando múltiplos fornecedores e reduzindo complexidade operacional.
- Centralizar políticas, autenticação, logs, relatórios e administração técnica no firewall e no FortiAnalyzerVM, garantindo coerência, auditoria e governança de segurança.

4.1.3. Conectividade segura e padronizada (rede cabeada + WiFi)

- Garantir uma rede WiFi corporativa integrada ao firewall, com redes corporativa e de visitantes submetidas a políticas de segurança centralizadas, autenticação adequada e segmentação conforme as diretrizes do TR.
- Evitar regressões funcionais na implantação da infraestrutura sem fio, assegurando instalação, configuração, documentação completa e operação assistida até a estabilização do ambiente.
- Sustentar desempenho, capacidade e disponibilidade da nova rede sem fio por meio de switches multigigabit PoE/PoE+ capazes de alimentar e suportar Access Points corporativos de alta performance.

4.1.4. Continuidade operacional e governança

- Assegurar alta disponibilidade, operação ininterrupta (24x7) e capacidade de atualização tecnológica contínua, garantindo proteção contra vulnerabilidades e evitando riscos associados ao fim de vida dos equipamentos atuais (1500D).
- Manter padronização tecnológica em Fortinet para preservar investimentos, reduzir riscos de interoperabilidade e garantir eficiência na operação e no suporte.
- Viabilizar controle e auditoria avançada por meio da ampliação da retenção de logs e da integração nativa com FortiAnalyzerVM, atendendo às necessidades institucionais de segurança, gestão e conformidade.

5. Necessidades Tecnológicas

5.1. NGFW Fortigate (3 unidades – “tipos I/II/III”) com requisitos de hardware/portas (RJ45/SFP/SFP+, DACs), TPM, fontes redundantes, HA ativo-ativo/ativo-passivo/clustering, certificações (p.ex., USGv6/IPv6, FCC/CE/UL/CB) e desempenho mínimo (throughput NGFW/IPS /Threat Protection, SSL inspection, sessões, CPS).

5.2. Serviços de instalação/implantação por item: plano de instalação, atualização de firmware estável/compatível, migração de políticas /objetos, suporte presencial (5 dias úteis) + remoto (25 dias úteis) após a virada, com documentação técnica completa (topologias, parâmetros, decisões).

5.3. Subscrições e licenças: UTP (FortiCare/IPS/AMP/WebFilter/Antispam/Sandbox, etc.) para os 3 firewalls; FortiNAC (licenças perpétuas, 1.600); FortiToken Mobile (650); FortiAnalyzerVM.

5.4. Switches multigigabit PoE/PoE+ com portas 5G/2.5G/10G, PoE bt/af/at, GBICs e desempenho compatível, além de certificações e operação fanless.

5.5. Access Points corporativos triband com WiFi 6/6E/7, OFDMA/MUMIMO, WPA3/802.1X, PoE 802.3at e integração ao Security Fabric.

5.6. Serviços de instalação/implantação, incluindo plano de instalação, firmware compatível, interligação óptica, documentação técnica e suporte presencial + remoto pós-implantação.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Requisitos Tecnológicos e Demais Requisitos

6.1.1. Os requisitos tecnológicos estão descritos no Termo de Referência.

6.2. Requisitos Legais

6.2.1. Conforme descrito no artigo 105 da PORTARIA Nº 265, DE 10 DE SETEMBRO DE 2020 - ANP, a Superintendência de Tecnologia da Informação - STI responde por todo o ambiente computacional da ANP, por meio do planejamento, projeto, aquisição, desenvolvimento, operacionalização, apoio e administração de equipamentos e programas de informática.

6.2.2. É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da Administração da ANP.

ALINHAMENTO AO PGC 2026	
DFD	**Descrição**
98/2025	Hardware de firewall (substituição das caixas atuais com aproveitamento das licenças)

6.3. Requisitos de Segurança

6.3.1. Devem ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela ANP, incluindo, mas não se limitando, ao que está definido na Política de Segurança da Informação e Comunicações e suas normas complementares, durante a execução dos serviços nas instalações da ANP.

6.3.2. Deve-se garantir a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionadas ao contrato e seus serviços, sendo legalmente responsabilizado quem causar perdas e danos à ANP e a terceiros.

6.3.3. A Contratada compromete-se a manter a confidencialidade das informações a que tiver acesso, formalizada por meio de um Termo de Compromisso de Manutenção de Sigilo, anexo ao Termo de Referência, mesmo após o término do contrato ou sua eventual rescisão.

6.3.4. A Contratada deve utilizar ferramentas de proteção e segurança da informação para evitar qualquer acesso não autorizado aos seus sistemas ou softwares, tanto aqueles sob sua responsabilidade direta quanto os disponibilizados à Contratante, mesmo que por meio de link.

6.3.5. As condições de manutenção de sigilo estão descritas no Termo de Compromisso de Manutenção de Sigilo, conforme modelo anexo ao Termo de Referência.

6.3.6. A Contratada deverá assinar o Termo de Compromisso de Manutenção de Sigilo.

6.3.7. A Contratada será responsabilizada pelo não cumprimento, por parte de seus profissionais, do Termo de Compromisso de Manutenção de Sigilo, bem como de todas as políticas e normas técnicas e administrativas da Contratada.

6.3.8. O tratamento de dados pessoais nesta contratação deve respeitar a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, ou legislação que a substitua.

6.4. Requisitos Temporais

6.4.1. O prazo de vigência da contratação é de 03 anos contado da data de vigência inicial do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

6.4.2. Início da execução do objeto: imediatamente após a data de vigência inicial do contrato.

6.4.3. Garantia onsite e suporte técnico pelo prazo de 36 (trinta e seis) meses, contados da emissão do Termo de Recebimento Definitivo.

6.4.4. O suporte técnico deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano.

7. Estimativa da demanda - quantidade de bens e serviços

Item	Especificação	CATMAT/ CATSER	Métrica ou Unidade de Medida	Qtde
01	Solução de Firewall Core – tipo I Next Generation Firewall Fortigate FG-901G Part Numbers e quantidades: Part Number: FG-901G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o Fortigate 901G com vigência de 36 meses. Part Number: FC-10-FG9H1-211-02-36 Quantidade: 1 unidade Upgrade do suporte para o Elite do FortiGate 901G com 36 meses de vigência Part Number: FC-10-FG9H1-204-02-36 Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo. Part Number: FN-TRAN-SFP+SR Quantidade: 20 unidades	618353	Unidade	1
02	Solução de Firewall Core – tipoII Next Generation Firewall Fortigate FG-701G Part Numbers e quantidades: Part Number : FG-701G Quantidade : 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-G7H1G-211-02-36 Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. Part Number: FC-10-G7H1G-204-02-36 Quantidade: 01 unidade SASE Secure Private Access, FortiTelemetry Cloud e 50 usuários de FortiSASE no starter kit Part Number: FC10G7H1G13290236	618353	Unidade	1

		Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo Part Number FN-TRAN-SFP+SR Quanitidade: 16 unidades			
	03	Solução de Firewall Core – tipo III Next Generation Firewall Fortigate FG-121G Part Number: FG-121G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-F121G-211-02-36 Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. FC-10-F121G-204-02-36 Quantidade: 01 unidade	618353	Unidade	1
	04	Serviço de Instalação da Solução de Firewall – tipo I – FG-901G	27103	Unidade	01
	05	Serviço de Instalação da Solução de Firewall – tipo II – FG-701G	27103	Unidade	01
	06	Serviço de Instalação da Solução de Firewall – tipo III – FG-121G	27103	Unidade	01
LOTE 01	07	Licença Unified Threat Protection (UTP) para Firewall Core – tipo I Fortigate FG901G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat Protection (UTP) Bundle para o FortiGate 901G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-FG9H0-950-02-36 Quantidade: 01 unidade	27502	mês	36
	08	Licença Unified Threat Protection (UTP) para Firewall Core – tipoII FG701G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat Protection (UTP) Bundle para o FortiGate 701G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-G7H0G-950-02-36 Quantidade: 01 unidade	27502	mês	36

09	Licença Unified Threat Protection (UTP) para Firewall Core – tipo III FG121G. Assinatura das funcionalidades de cybersegurança Fortinet UTP Bundle para o FortiGate 121G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência Part Number: FC-10-F121G-950-02-36 Quantidade: 01 unidade	27502	mês	36
10	FortiNAC para atender a 1.600 dispositivos FortiNAC-Subscription License FortiNAC Subscription PRO License for 1600 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response. Part Number:FC5-10-FNAC1-209-01-36 Quantidade: 6 unidades Part Number:FC6-10-FNAC1-209-01-36 Quantidade: 1 unidade Vigência de 36 meses	350949	Unidade (pack)	1600
11	FortiToken Mobile (FTM) One-Time Password (OTP) for 450 usuários Pacote com 100 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: FTM-ELIC-100 Quantidade: 04 unidades Pacote com 50 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: x FTM-ELIC-50 Quantidade: 01 unidade	350949	Unidade (pack)	450
12	FortiAnalyzer Virtual (VM) licença Perpétua com capacidade de armazenamento de 25GB de Logs por dia na capacidade de processamento de dados Upgrade para adicionar 25GB Log por dia na capacidade de processamento de dados no FortiAnalyzer VM Perpétuo Part Number: FAZ-VM-GB25 Quantidade: 01 unidade FortiAI Agentic - Ia Generativa com suporte a interações LLM para assistência nas análises de SOC, investigação de incidente, triagem e resposta para o FortiAnalyzer VM 36 meses de vigência. Part Number: FC5-10-LV0VM-1118-02-36 Quantidade: 01 unidade Suporte Elite para o FortiAnalyzer VM Perpétuo com 36 meses de vigência. Part Number:	350949	mês	36

		FC5-10-LV0VM-285-02-36 Quantidade: 01 unidade			
	13	Switch Multigigabit PoE/PoE+ FS-110G-FPOE - FortiSwitch 110G-FPOE com 2x 5G RJ45 com PoE bt, 8x 2.5G RJ45 com PoE af/at e 4x SFP+. Capacidade e 200W PoE. Part Number: FS-110G Quantidade: 11 unidades Suporte Elite para o FortiSwitch 110G-FPOE com vigência de 36 meses Part Number: FC-10-M10GF-284-02-36. Quantidade: 11 unidades	626881	unidade	11
	14	Access Point FAP-221K-N FortiAP 231K - Ponto de acesso indoor com suporte a Wi-fi 7 2x2 MIMO, antenas internas, interface RJ45 de 2.5G. Part Number: FAP-231K-N Quantidade: 25 unidades Suporte Elite para o FortiAP 231K com vigência de 36 meses Part Number: FC-10-P221K-284-02-36 Quantidade: 25 unidades	632687	unidade	25
	15	Instalação dos Switches e Access Points	27103	unidade	01

8. Levantamento de soluções

8.1. ANÁLISE DE SOLUÇÕES

8.1.1. Contexto Atual e Premissas de Avaliação

8.1.1.1. A ANP opera, desde 2013, sua arquitetura de segurança perimetral com equipamentos NGFW Fortinet Fortigate 1500D, adquiridos por meio do processo 48610.009268/201388. Esses equipamentos se tornaram o núcleo da proteção de borda, oferecendo inspeção profunda de pacotes (DPI), IPS, antivírus de borda, controle de aplicações, Web Filter, AntiSpam, VPN e inspeção SSL, sustentando operações críticas 24x7 e atendendo requisitos legais e regulatórios.

8.1.1.2. Ao longo de mais de uma década, todo o ecossistema de segurança da ANP foi padronizado na tecnologia Fortinet, incluindo FortiAnalyzer, FortiManager, FortiGuard, FortiNAC e FortiToken, com regras, políticas e fluxos internos totalmente integrados a essa plataforma. A equipe técnica também possui forte capacitação e experiência acumulada no ecossistema Fortinet.

8.1.1.3. Atualmente, a continuidade dessa arquitetura está comprometida pelo fim de ciclo de vida (EoL) do modelo Fortigate 1500D:

- EOO: 31/12/2021
- Última extensão de manutenção: 31/12/2025
- Expiração total de suporte: 31/12/2026
- Último firmware suportado: FortiOS 7.2 (incompatível com o FortiOS 7.4)

8.1.1.4. Esse cenário impede a aplicação de atualizações críticas, limita funcionalidades modernas e aumenta significativamente o risco cibernético.

8.1.1.5. Simultaneamente, a ANP necessita implementar rede sem fio corporativa, algo inexistente atualmente. O TR estabelecerá que a nova rede deve ser totalmente integrada ao firewall, permitindo gestão unificada, segmentação, autenticação centralizada, visibilidade e políticas de segurança fim a fim, utilizando switches multigigabit PoE/PoE+ e Access Points corporativos gerenciados pelo próprio firewall (Security Fabric).

8.1.1.6. Diante disso, todas as alternativas tecnológicas precisam considerar:

- continuidade do serviço público e mitigação de risco;
- integração nativa entre firewall, NAC, switches e APs;
- aderência ao parque Fortinet já implantado;
- redução do custo de transição e da curva de aprendizado;
- preservação das regras e políticas existentes;
- estabilidade operacional e simplificação administrativa.

8.1.1.7. A avaliação, portanto, deve tratar firewall + NAC + WiFi + switching como uma única solução integrada, pois é assim que a ANP opera hoje e como o TR definirá a solução desejada.

8.1.2. Alternativas Identificadas

8.1.2.1. Com base no levantamento técnico foram identificadas três alternativas integradas para evolução da solução de segurança perimetral + conectividade WiFi + switching, tratadas como um único conjunto tecnológico:

a) Evolução da solução integrada Fortinet atualmente em operação

Atualização tecnológica da solução existente, substituindo os firewalls 1500D por novos NGFW Fortigate compatíveis com o FortiOS atual, e implantando a rede sem fio com switches multigigabit PoE/PoE+ e Access Points corporativos da própria Fortinet, assegurando:

- gestão unificada pelo Security Fabric;
- políticas automatizadas e integração nativa com NAC e UTP;
- continuidade operacional sem regressão funcional;
- menor risco de implantação e curva de aprendizado;
- preservação de investimentos e componentes já existentes (Analyzer, Manager, Token, FortiGuard).

b) Aquisição de uma solução integrada de outro fabricante (NGFW + Switching + WiFi + NAC)

Adoção de uma plataforma completa de outro fabricante (ex.: Cisco, Aruba, Check Point, Palo Alto), desde que demonstre superioridade técnica e vantajosidade global. Envolve:

- substituição do ecossistema atual (firewalls, tokens, NAC, analyzer, switches e APs);
- migração manual de regras e políticas;
- perda da integração nativa existente;
- necessidade de requalificação da equipe;
- riscos de interoperabilidade e tempo de estabilização elevado.

c) Retorno a soluções fragmentadas (fabricantes múltiplos e integrações não nativas)

Aquisição de componentes separados (firewall de um fabricante, switches de outro, APs de outro, NAC isolado etc.), resultando em:

- múltiplas plataformas de gestão;
- maior risco operacional;
- perda de automação e telemetria integrada;
- necessidade de conectores terceiros;
- maior custo de suporte e implantação;
- visibilidade reduzida e segurança inconsistente.

Essa é a alternativa menos eficiente e mais custosa, contrariando diretrizes do TR que exigem integração completa e riscos reduzidos.

8.2. IDENTIFICAÇÃO DAS SOLUÇÕES

A tabela a seguir apresenta as alternativas integradas possíveis, considerando toda a solução como um único conjunto tecnológico:

Id	Descrição da Solução Integrada (Firewall + Switching + WiFi + NAC + UTP)
1	Evolução da solução integrada Fortinet atualmente em operação.
2	Adoção de solução integrada completa de outro fabricante (NGFW + NAC + WiFi + Switching).
3	Implementação de solução fragmentada com múltiplos fabricantes e integrações não nativas.

9. Análise comparativa de soluções

Requisitos	Cenário 1 Evolução Fortinet (solução integrada atualizada)	Cenário 2 Solução integrada completa de outro fabricante	Cenário 3 Solução fragmentada com múltiplos fabricantes
Negócio	Atende — mantém continuidade operacional 24×7, reduz risco, preserva regras existentes, integra WiFi, switching, firewall, NAC e UTP, conforme o modelo único definido no TR.	Atende — desde que justificada, mas com maior impacto operacional, curva de aprendizado e risco de transição.	**Não atende** — fragmenta a arquitetura, aumenta risco e complexidade, contradiz o modelo integrado exigido pelo TR.
Tecnológico	Atende — suporta expansão, atualiza firewall e WiFi, mantém integração nativa com NAC, Analyzer, Token e Security Fabric, usa hardware suportado, mantém gestão centralizada, não demanda requalificação de grande porte.	Atende — atende requisitos de capacidade e modernização, mas perde integração nativa, exige migração complexa e treinamento completo da equipe.	**Não atende** — perde integração, exige múltiplas ferramentas, compromete automação, aumenta risco e esforço técnico, e contraria requisitos de integração previstos no TR.
Resultado da Análise	**Viável**	**Viável** (com restrições e maior risco)	**Inviável**

10. Registro de soluções consideradas inviáveis

Cenário 2 – Inviável (Solução integrada de outro fabricante)

Esta alternativa não atende integralmente aos requisitos essenciais de negócio e tecnologia definidos no TR. Embora possa oferecer os componentes necessários, apresenta limitações de integração nativa com os demais elementos já existentes no ambiente da ANP, especialmente FortiAnalyzer, FortiManager, FortiToken e FortiNAC, que compõem o Security Fabric utilizado há mais de uma década.

A adoção de uma solução integrada de outro fabricante implica:

- perda da integração nativa com o firewall atualmente em uso e com os serviços correlatos;
- necessidade de requalificação completa da equipe;
- risco elevado na migração das regras de firewall, objetos e políticas UTM;
- aumento da complexidade operacional;
- perda de eficiência na aplicação centralizada de políticas de segurança;
- impacto direto na continuidade do serviço público.

Assim, por suprir apenas parcialmente as necessidades institucionais e criar riscos operacionais incompatíveis com o ambiente crítico da ANP, não apresenta condições de atender de forma adequada às demandas atuais nem futuras da organização.

Cenário 3 – Inviável (Solução fragmentada, com múltiplos fabricantes e integrações não nativas)

Esta alternativa não atende aos requisitos essenciais de negócio nem aos requisitos tecnológicos definidos no TR, pois contraria diretamente a necessidade de uma solução integrada, coesa e com gerenciamento unificado.

Uma arquitetura fragmentada implicaria:

- múltiplas interfaces de gerenciamento;
- ausência de integração nativa entre firewall, WiFi, switches, UTP, NAC, FTM e Analyzer;
- perda de automação e telemetria unificada;
- maior risco operacional e maior esforço contínuo da equipe;
- aumento expressivo da complexidade de configuração e suporte;
- redução da visibilidade de segurança e inconsistência na aplicação de políticas;
- dificultaria auditorias, conformidade e monitoramento.

Além disso, essa opção vai contra a abordagem prevista no TR, que exige que todos os componentes sejam parte de uma única solução integrada, com suporte unificado, atualizações consistentes e continuidade operacional.

Por esses motivos, a solução fragmentada não apresenta condições de suprir as demandas atuais nem futuras da ANP, sendo considerada tecnicamente inviável.

11. Análise comparativa de custos (TCO)

11.1. Cálculo dos custos totais de propriedade (TCO)

Solução Viável 1 – Cenário 1

Descrição: Evolução da solução integrada Fortinet atualmente em operação.

A solução considera a **aquisição de novos appliances Fortinet**, com garantia, licenciamento UTP (Unified Threat Protection), suporte premium e serviços especializados, conforme valores presentes nas propostas fornecidas. Os custos abaixo correspondem ao investimento necessário para atualização tecnológica da plataforma Fortinet, assegurando compatibilidade plena com o ambiente atual, continuidade operacional e reaproveitamento das políticas e integrações já existentes.

	Item	Especificação	CATMAT/ CATSER	Métrica o u Unidade de Medida	Qtde	Valor Unitário	Valor Total
	01	Solução de Firewall Core – tipo I Next Generation Firewall Fortigate FG-901G Part Numbers e quantidades: Part Number: FG-901G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o Fortigate 901G com vigência de 36 meses. Part Number: FC-10-FG9H1-211-02-36 Quantidade: 1 unidade Upgrade do suporte para o Elite do FortiGate 901G com 36 meses de vigência Part Number: FC-10-FG9H1-204-02-36 Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo. Part Number: FN-TRAN-SFP+SR Quantidade: 20 unidades	618353	Unidade	1	R$1.038.434,94	R$1.038.434,94
		Solução de Firewall Core – tipoII Next Generation Firewall Fortigate FG-701G Part Numbers e quantidades: Part Number : FG-701G Quantidade : 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-G7H1G-211-02-36					

02	Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. Part Number: FC-10-G7H1G-204-02-36 Quantidade: 01 unidade SASE Secure Private Access, FortiTelemetry Cloud e 50 usuários de FortiSASE no starter kit Part Number: FC10G7H1G13290236 Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo Part Number FN-TRAN-SFP+SR Quanitidade: 16 unidades	618353	Unidade	1	R$880.029,29	R$880.029,29
03	Solução de Firewall Core – tipo III Next Generation Firewall Fortigate FG-121G Part Number: FG-121G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-F121G-211-02-36 Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. FC-10-F121G-204-02-36 Quantidade: 01 unidade	618353	Unidade	1	R$95.810,43	R$95.810,43
04	Serviço de Instalação da Solução de Firewall – tipo I – FG-901G	27103	Unidade	01	R$51.200,00	R$51.200,00
05	Serviço de Instalação da Solução de Firewall – tipo II – FG-701G	27103	Unidade	01	R$49.840,00	R$49.840,00
06	Serviço de Instalação da Solução de Firewall – tipo III – FG-121G	27103	Unidade	01	R$46.000,00	R$46.000,00
	Licença Unified Threat Protection (UTP) para Firewall Core – tipo I Fortigate FG901G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat					

	07	Protection (UTP) Bundle para o FortiGate 901G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-FG9H0-950-02-36 Quantidade: 01 unidade	27502	mês	36	R$41.489,29	R$1.493.614,37
LOTE 01	08	Licença Unified Threat Protection (UTP) para Firewall Core – tipoII FG701G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat Protection (UTP) Bundle para o FortiGate 701G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-G7H0G-950-02-36 Quantidade: 01 unidade	27502	mês	36	R$32.157,85	R$1.157.682,67
	09	Licença Unified Threat Protection (UTP) para Firewall Core – tipo III FG121G. Assinatura das funcionalidades de cybersegurança Fortinet UTP Bundle para o FortiGate 121G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência Part Number: FC-10-F121G-950-02-36 Quantidade: 01 unidade	27502	mês	36	R$8.759,46	R$315.340,63
	10	FortiNAC para atender a 1.600 dispositivos FortiNAC-Subscription License FortiNAC Subscription PRO License for 1600 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response. Part Number:FC5-10-FNAC1-209-01-36 Quantidade: 6 unidades Part Number:FC6-10-FNAC1-209-01-36 Quantidade: 1 unidade Vigência de 36 meses	350949	Unidade (pack)	1600	R$513,53	R$821.649,66
	11	FortiToken Mobile (FTM) One-Time Password (OTP) for 450 usuários					

	Pacote com 100 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: FTM-ELIC-100 Quantidade: 04 unidades Pacote com 50 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: x FTM-ELIC-50 Quantidade: 01 unidade	350949	Unidade (pack)	450	R$780,93	R$351.417,24
12	FortiAnalyzer Virtual (VM) licença Perpétua com capacidade de armazenamento de 25GB de Logs por dia na capacidade de processamento de dados Upgrade para adicionar 25GB Log por dia na capacidade de processamento de dados no FortiAnalyzer VM Perpétuo Part Number: FAZ-VM-GB25 Quantidade: 01 unidade FortiAI Agentic - Ia Generativa com suporte a interações LLM para assistência nas análises de SOC, investigação de incidente, triagem e resposta para o FortiAnalyzer VM 36 meses de vigência. Part Number: FC5-10-LV0VM-1118-02-36 Quantidade: 01 unidade Suporte Elite para o FortiAnalyzer VM Perpétuo com 36 meses de vigência. Part Number: FC5-10-LV0VM-285-02-36 Quantidade: 01 unidade	350949	mês	36	R$22.465,09	R$808.743,31
13	Switch Multigigabit PoE/PoE+ FS-110G-FPOE - FortiSwitch 110G-FPOE com 2x 5G RJ45 com PoE bt, 8x 2.5G RJ45 com PoE af /at e 4x SFP+. Capacidade e 200W PoE. Part Number: FS-110G Quantidade: 11 unidades Suporte Elite para o FortiSwitch 110G-FPOE com vigência de 36 meses Part Number: FC-10-M10GF-284-02-36. Quantidade: 11 unidades	626881	unidade	11	R$30.743,94	R$338.183,31
14						

		Access Point FAP-221K-N FortiAP 231K - Ponto de acesso indoor com suporte a Wi-fi 7 2x2 MIMO, antenas internas, interface RJ45 de 2.5G. Part Number: FAP-231K-N Quantidade: 25 unidades Suporte Elite para o FortiAP 231K com vigência de 36 meses Part Number: FC-10-P221K-284-02-36 Quantidade: 25 unidades	632687	unidade	25	R$13.206,27	R$330.156,65
	15	Instalação dos Switches e Access Points	27103	unidade	01	R$47.840,00	R$47.840,00
Total						**-**	**R$7.825.942,50**

Fonte: Mapa de preços (SEI 6016163)

Cálculo do TCO do Cenário 1

A partir dos itens estruturais, o custo total inicial da solução, **sem considerar custos mensais**, é:

R$ 7.825.942,50 (sete milhões, oitocentos e vinte e cinco mil, novecentos e quarenta e dois reais e cinquenta centavos)

11.2. Mapa comparativo dos cálculos totais de propriedade (TCO)

MAPA DE PREÇOS

				STORAGEWAY		SOLOR		BRASILINE		2r Data		Columbia		MÉDIA	
Item	Especificação	Métrica ou Unidade de Medida	Qtde	Valor Unitário/Mensal	Valor Total	Valor Unitário/Mensal	Valor Total	Valor Unitário/Mensal	Valor Total	Valor Unitário/Mensal	Valor Total	Valor Unitário/Mensal	Valor Total	Valor Unitário/Mensal	Valor Total
1	Solução de Firewall Core – tipo I	Unidade	1	R$ 1.008.717,04	R$ 1.008.717,04	R$ 1.048.844,04	R$ 1.048.844,04	R$ 1.034.217,64	R$ 1.034.217,64	R$ 1.050.198,00	R$ 1.050.198,00	R$ 1.050.198,00	R$ 1.050.198,00	R$ 1.038.434,94	R$ 1.038.434,94
2	Solução de Firewall Core – tipo II	Unidade	1	R$ 827.160,62	R$ 827.160,62	R$ 896.145,82	R$ 896.145,82	R$ 864.151,99	R$ 864.151,99	R$ 906.344,00	R$ 906.344,00	R$ 906.344,00	R$ 906.344,00	R$ 880.029,29	R$ 880.029,29
3	Solução de Firewall Core – tipo III	Unidade	1	R$ 89.411,11	R$ 89.411,11	R$ 96.867,99	R$ 96.867,99	R$ 94.571,03	R$ 94.571,03	R$ 99.101,00	R$ 99.101,00	R$ 99.101,00	R$ 99.101,00	R$ 95.810,43	R$ 95.810,43
4	Serviço de Instalação da Solução de Firewall – tipo I	Unidade	1	R$ 48.800,00	R$ 48.800,00	R$ 53.300,00	R$ 53.300,00	R$ 52.000,00	R$ 52.000,00	R$ 50.700,00	R$ 50.700,00	R$ 51.200,00	R$ 51.200,00	R$ 51.200,00	R$ 51.200,00
5	Serviço de Instalação da Solução de Firewall – tipo II	Unidade	1	R$ 48.800,00	R$ 48.800,00	R$ 53.300,00	R$ 53.300,00	R$ 52.000,00	R$ 52.000,00	R$ 48.000,00	R$ 48.000,00	R$ 47.100,00	R$ 47.100,00	R$ 49.840,00	R$ 49.840,00
6	Serviço de Instalação da Solução de Firewall – tipo III	Unidade	1	R$ 45.200,00	R$ 45.200,00	R$ 45.000,00	R$ 45.000,00	R$ 49.900,00	R$ 49.900,00	R$ 44.100,00	R$ 44.100,00	R$ 45.800,00	R$ 45.800,00	R$ 46.000,00	R$ 46.000,00
7	Licença UTP para Firewall Tipo I, FortiGate FG-901G	Mês	36	R$ 38.817,46	R$ 1.397.428,56	R$ 42.961,00	R$ 1.546.596,00	R$ 41.491,98	R$ 1.493.711,28	R$ 42.088,00	R$ 1.515.168,00	R$ 42.088,00	R$ 1.515.168,00	R$ 41.489,29	R$ 1.493.614,37
8	Licença UTP para Firewall Tipo II Fortigate FG-701G	Mês	36	R$ 29.666,13	R$ 1.067.980,68	R$ 32.897,00	R$ 1.184.292,00	R$ 31.710,13	R$ 1.141.564,68	R$ 33.258,00	R$ 1.197.288,00	R$ 33.258,00	R$ 1.197.288,00	R$ 32.157,85	R$ 1.157.682,67
9	Licença UTP para Firewall Tipo III FortiGate FG-121G	Mês	36	R$ 7.974,92	R$ 287.097,12	R$ 8.894,00	R$ 320.184,00	R$ 8.524,39	R$ 306.878,05	R$ 9.202,00	R$ 331.272,00	R$ 9.202,00	R$ 331.272,00	R$ 8.759,46	R$ 315.340,63
10	FortiNAC para atender a 1.600 dispositivos	Dispositivo	1.600	R$ 492,54	R$ 788.069,96	R$ 517,35	R$ 827.752,00	R$ 511,40	R$ 818.244,34	R$ 523,18	R$ 837.091,00	R$ 523,18	R$ 837.091,00	R$ 513,53	R$ 821.649,66
11	FortiToken Mobile(FTM) One Time Password (OTP) for 450 usuários	Licenças	450	R$ 720,17	R$ 324.077,14	R$ 799,50	R$ 359.775,00	R$ 769,79	R$ 346.406,05	R$ 807,59	R$ 363.414,00	R$ 807,59	R$ 363.414,00	R$ 780,93	R$ 351.417,24
12	FortiAnalyzer Virtual (VM)	Mês	36	R$ 19.669,61	R$ 708.105,96	R$ 23.037,00	R$ 829.332,00	R$ 21.024,85	R$ 756.894,59	R$ 24.297,00	R$ 874.692,00	R$ 24.297,00	R$ 874.692,00	R$ 22.465,09	R$ 808.743,31
13	Switch Multigigabit PoE/PoE+ FS-110G-FPOE	Unidade	11	R$ 27.809,31	R$ 305.902,41	R$ 31.921,00	R$ 351.131,00	R$ 29.725,38	R$ 326.979,13	R$ 32.132,00	R$ 353.452,00	R$ 32.132,00	R$ 353.452,00	R$ 30.743,94	R$ 338.183,31
14	Access Point FAP-221K-N FortiAP 231K	Unidade	25	R$ 12.133,09	R$ 303.327,25	R$ 13.328,00	R$ 333.200,00	R$ 13.208,24	R$ 330.206,00	R$ 13.681,00	R$ 342.025,00	R$ 13.681,00	R$ 342.025,00	R$ 13.206,27	R$ 330.156,65
15	Instalação dos Switches e Access Points	Unidade	1	R$ 47.500,00	R$ 47.500,00	R$ 49.800,00	R$ 49.800,00	R$ 54.000,00	R$ 54.000,00	R$ 45.600,00	R$ 45.600,00	R$ 42.300,00	R$ 42.300,00	R$ 47.840,00	R$ 47.840,00
					R$ 7.297.577,85		R$ 7.995.519,85		R$ 7.721.724,78		R$ 8.058.445,00		R$ 8.056.445,00		R$ 7.825.942,50

12. Descrição da solução de TIC a ser contratada

A descrição completa da solução consta no item 3 do termo de referência n.º 36/2026-ANP, do qual esse documento faz parte.

13. Estimativa de custo total da contratação

Valor (R$): 7.825.942,50

Tabela com os valores:

Item	Especificação	CATMAT/ CATSER	Métrica o u Unidade de Medida	Qtde	Valor Unitário	Valor Total
01	Solução de Firewall Core – tipo I Next Generation Firewall Fortigate FG-901G Part Numbers e quantidades: Part Number: FG-901G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o Fortigate 901G com vigência de 36 meses. Part Number: FC-10-FG9H1-211-02-36 Quantidade: 1 unidade Upgrade do suporte para o Elite do FortiGate 901G com 36 meses de vigência Part Number: FC-10-FG9H1-204-02-36 Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo. Part Number: FN-TRAN-SFP+SR Quantidade: 20 unidades	618353	Unidade	1	R$1.038.434,94	R$1.038.434,94
02	Solução de Firewall Core – tipoII Next Generation Firewall Fortigate FG-701G Part Numbers e quantidades: Part Number : FG-701G Quantidade : 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-G7H1G-211-02-36 Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. Part Number: FC-10-G7H1G-204-02-36 Quantidade: 01 unidade SASE Secure Private Access, FortiTelemetry Cloud e 50 usuários de FortiSASE no starter kit	618353	Unidade	1	R$880.029,29	R$880.029,29

	Part Number: FC10G7H1G13290236 Quantidade: 01 unidade Transceivers do tipo 10GE SFP+ Short Range (300m) Multimodo Part Number FN-TRAN-SFP+SR Quanitidade: 16 unidades					
03	Solução de Firewall Core – tipo III Next Generation Firewall Fortigate FG-121G Part Number: FG-121G Quantidade: 01 unidade RMA prioritário de 4 horas para substituição para o FortiGate 701G com vigência de 36 meses. Part Number: FC-10-F121G-211-02-36 Quantidade: 01 unidade Upgrade do suporte para o Elite do FortiGate 701G com 36 meses de vigência. FC-10-F121G-204-02-36 Quantidade: 01 unidade	618353	Unidade	1	R$95.810,43	R$95.810,43
04	Serviço de Instalação da Solução de Firewall – tipo I – FG-901G	27103	Unidade	01	R$51.200,00	R$51.200,00
05	Serviço de Instalação da Solução de Firewall – tipo II – FG-701G	27103	Unidade	01	R$49.840,00	R$49.840,00
06	Serviço de Instalação da Solução de Firewall – tipo III – FG-121G	27103	Unidade	01	R$46.000,00	R$46.000,00
07	Licença Unified Threat Protection (UTP) para Firewall Core – tipo I Fortigate FG901G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat Protection (UTP) Bundle para o FortiGate 901G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-FG9H0-950-02-36 Quantidade: 01 unidade	27502	mês	36	R$41.489,29	R$1.493.614,37
	Licença Unified Threat Protection (UTP) para Firewall Core – tipoII					

LOTE 01		FG701G. Assinatura das funcionalides de cybersegurança Fortinet Unified Threat Protection (UTP) Bundle para o FortiGate 701G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência. Part Number: FC-10-G7H0G-950-02-36 Quantidade: 01 unidade					
	08		27502	mês	36	R$32.157,85	R$1.157.682,67
	09	Licença Unified Threat Protection (UTP) para Firewall Core – tipo III FG121G. Assinatura das funcionalidades de cybersegurança Fortinet UTP Bundle para o FortiGate 121G (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) com 36 meses de vigência Part Number: FC-10-F121G-950-02-36 Quantidade: 01 unidade	27502	mês	36	R$8.759,46	R$315.340,63
	10	FortiNAC para atender a 1.600 dispositivos FortiNAC-Subscription License FortiNAC Subscription PRO License for 1600 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response. Part Number:FC5-10-FNAC1-209-01-36 Quantidade: 6 unidades Part Number:FC6-10-FNAC1-209-01-36 Quantidade: 1 unidade Vigência de 36 meses	350949	Unidade (pack)	1600	R$513,53	R$821.649,66
	11	FortiToken Mobile (FTM) One-Time Password (OTP) for 450 usuários Pacote com 100 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: FTM-ELIC-100 Quantidade: 04 unidades Pacote com 50 FortiTokens Mobile (OTP) para iOS, Android, e dispositivos Windows. Part Number: x FTM-ELIC-50 Quantidade: 01 unidade	350949	Unidade (pack)	450	R$780,93	R$351.417,24

12	FortiAnalyzer Virtual (VM) licença Perpétua com capacidade de armazenamento de 25GB de Logs por dia na capacidade de processamento de dados Upgrade para adicionar 25GB Log por dia na capacidade de processamento de dados no FortiAnalyzer VM Perpétuo Part Number: FAZ-VM-GB25 Quantidade: 01 unidade FortiAI Agentic - Ia Generativa com suporte a interações LLM para assistência nas análises de SOC, investigação de incidente, triagem e resposta para o FortiAnalyzer VM 36 meses de vigência. Part Number: FC5-10-LV0VM-1118-02-36 Quantidade: 01 unidade Suporte Elite para o FortiAnalyzer VM Perpétuo com 36 meses de vigência. Part Number: FC5-10-LV0VM-285-02-36 Quantidade: 01 unidade	350949	mês	36	R$22.465,09	R$808.743,31
13	Switch Multigigabit PoE/PoE+ FS-110G-FPOE - FortiSwitch 110G-FPOE com 2x 5G RJ45 com PoE bt, 8x 2.5G RJ45 com PoE af /at e 4x SFP+. Capacidade e 200W PoE. Part Number: FS-110G Quantidade: 11 unidades Suporte Elite para o FortiSwitch 110G-FPOE com vigência de 36 meses Part Number: FC-10-M10GF-284-02-36. Quantidade: 11 unidades	626881	unidade	11	R$30.743,94	R$338.183,31
14	Access Point FAP-221K-N FortiAP 231K - Ponto de acesso indoor com suporte a Wi-fi 7 2x2 MIMO, antenas internas, interface RJ45 de 2.5G. Part Number: FAP-231K-N Quantidade: 25 unidades Suporte Elite para o FortiAP 231K com vigência de 36 meses Part Number: FC-10-P221K-284-02-36 Quantidade: 25 unidades	632687	unidade	25	R$13.206,27	R$330.156,65
15	Instalação dos Switches e Access Points	27103	unidade	01	R$47.840,00	R$47.840,00

Total						**-**	**R$7.825.942,50**

14. Justificativa técnica da escolha da solução

14.1. Fundamentação Técnica e Aderência aos Objetivos

14.1.1. A aquisição e implantação da solução integrada de segurança perimetral (NGFW) e conectividade sem fio corporativa (WiFi) com equipamentos Fortinet é essencial para garantir estabilidade, segurança, desempenho e continuidade dos serviços de TIC da organização. A proposta contempla infraestrutura de firewall de última geração, switches multigigabit e Access Points corporativos, todos nativamente integrados ao ecossistema Fortinet, além de serviços especializados de instalação, migração, documentação e operação assistida.

14.1.2. A adoção desse modelo assegura:

- Continuidade operacional 24x7 da segurança perimetral e da conectividade corporativa.
- Capacidade ampliada, atualização de firmwares e suporte do fabricante, garantindo tratamento de vulnerabilidades e conformidade técnica.
- Gestão centralizada via Security Fabric, permitindo telemetria unificada, políticas coerentes, correlação de eventos e administração simplificada.
- Implantação assistida por especialistas, reduzindo riscos durante a transição e acelerando a estabilização do ambiente.
- Preservação do investimento já realizado no ecossistema Fortinet, evitando retrabalho, reescrita massiva de regras e múltiplos consoles de administração.
- Atendimento aos prazos e condições contratuais de entrega, garantia e validade das licenças, em aderência aos requisitos operacionais definidos.

14.1.3. A solução proposta inclui suporte por 36 meses, operação assistida, documentação completa e componentes de última geração com suporte a 2.4/5/6 GHz, PoE/PoE+, uplinks de 10 Gbps, WPA3, 802.1X e integração nativa com o firewall, assegurando arquitetura coerente e desempenho compatível com as necessidades atuais e futuras.

14.2. Do Parcelamento da Contratação Decorrente de Aspectos Técnicos

14.2.1. Opção pelo não parcelamento (integração técnica como premissa)

A análise de viabilidade demonstra que não parcelar o objeto é a prática mais adequada sob o ponto de vista técnicooperacional. A divisão entre hardware, software, firmwares, serviços de instalação/configuração/migração/treinamento, switches, APs e interconexões resultaria em:

- perda da coerência arquitetural;
- maior complexidade operacional;
- riscos adicionais de incompatibilidade;
- fragmentação da responsabilidade técnica;
- dificuldades de diagnóstico unificado, suporte e operação assistida;
- aumento de janelas de risco em um ambiente crítico de operação contínua.

Na solução em questão, todos os componentes — NGFW, switching, WiFi, licenças, segurança, integração, telemetria, operação assistida — atuam de forma conjunta e dependente, formando uma única solução integrada de segurança e conectividade corporativa.

14.2.1.1. Viabilidade técnica e indivisibilidade funcional

Embora seja tecnicamente possível adquirir os componentes separadamente, o cenário concreto exige implantação integrada para assegurar:

- coerência arquitetural;
- segurança ponta a ponta;
- desempenho adequado;
- aplicação consistente de políticas;
- telemetria e gestão centralizadas.

Os serviços descritos no escopo — instalação, atualização de firmwares, migração de parâmetros, criação de regras/VPNs, energização PoE, validação de cobertura WiFi, testes e operação assistida — demonstram que hardware, licenças e serviços funcionam de maneira interdependente.

Por isso, o parcelamento comprometeria a governança do projeto e ampliaria o risco de falhas técnicas.

14.2.1.2. Organização do objeto e precificação

A discriminação por itens nas propostas serve exclusivamente à correta precificação (equipamentos, licenças, serviços e suporte), sem descaracterizar a unidade técnica da solução.
Durante a execução, todos os componentes devem operar integrados para entregar o resultado esperado:

- segurança perimetral avançada (NGFW + HA + UTM/IPS/VPN)
- conectividade WiFi corporativa moderna e segura
- telemetria unificada e administração centralizada
- operação assistida e documentação

Assim, o objeto deve ser conduzido como solução única, ainda que sua precificação seja detalhada.

14.2.1.3. Competitividade e vantajosidade

O não parcelamento não restringe a competitividade, pois diversos integradores e parceiros certificados ofertam soluções completas Fortinet (appliances + licenças + switches + APs + serviços).

Pelo contrário, a contratação coesa:

- concentra responsabilidade técnica;
- reduz litígios;
- evita incompatibilidades entre fabricantes;
- melhora o SLA e o suporte;
- diminui o TCO;
- reduz riscos operacionais;
- garante aderência plena às políticas do fabricante.

As propostas apresentadas já incluem prazos de entrega, garantias, licenças e condições de suporte de 36 meses, reforçando a pertinência da contratação integrada.

15. Justificativa econômica da escolha da solução

15. Justificativa Econômica da Escolha da Solução

15.1. Justificativa Econômica da Solução Integrada

A solução selecionada engloba a aquisição de firewalls NGFW, switches multigigabit, Access Points corporativos, licenças, suporte FortiCare e serviços especializados (instalação, migração, documentação e operação assistida), todos integrantes do ecossistema Fortinet. Esse conjunto integrado garante continuidade operacional, previsibilidade de custos e redução de riscos de indisponibilidade, assegurando eficiência econômica ao longo do ciclo de vida da infraestrutura.

A escolha da arquitetura unificada reduz gastos recorrentes com múltiplos fabricantes, elimina investimentos adicionais em plataformas de gerenciamento paralelas, diminui o esforço técnico das equipes internas e reduz o risco financeiro associado a falhas, incompatibilidades ou retrabalhos.

15.1.1. Análise Econômica por TCO (Total Cost of Ownership)

A decisão não se restringe ao custo inicial de aquisição. O TCO total considera custos diretos e indiretos ao longo de todo o ciclo de vida, incluindo:

a) Custos de operação e capacitação

A adoção da solução integrada Fortinet aproveita a maturidade já existente no ambiente, reduzindo:

- tempo de aprendizado;
- necessidade de treinamentos extensivos;
- custos operacionais (N1/N2/N3) de sustentação;
- despesas com reengenharia de regras, objetos e políticas de segurança.

b) Custos recorrentes de suporte e atualização

As propostas incluem:

- suporte FortiCare;
- atualizações de firmware;
- assinaturas de UTP/IPS/Antivírus/filtragens;
- garantia e substituição de componentes.

Esses custos já estão precificados e alinhados aos prazos do fabricante, garantindo previsibilidade financeira.

c) Custos de integração e compatibilidade

A solução integrada evita:

- recriação massiva de VPNs, regras, objetos e políticas;
- necessidade de reestruturação de toda a arquitetura de segurança;
- custos ocultos de migração para fabricante distinto.

Assim, o TCO da solução integrada é substancialmente inferior ao de alternativas fragmentadas ou baseadas em nova plataforma.

15.1.2. Comparação Econômica entre Alternativas Avaliadas

Consideradas as alternativas levantadas no ETP (evolução Fortinet, mudança de fabricante ou aquisição fragmentada), a solução integrada apresenta vantagens econômicas claras:

- Menor CAPEX/OPEX agregado, pois aproveita ferramentas e expertise já estabelecidas.
- Custos de transição reduzidos, sem necessidade de reescrever políticas ou redesenhar todo o ambiente.
- Menor curva de aprendizado, garantindo rápida estabilização.
- Entrega acelerada, com benefícios antecipados e menor risco de indisponibilidade.
- Eliminação de retrabalho e duplicidade de ferramentas, reduzindo custos indiretos.

Além disso, a solução integrada minimiza incidentes, reduz tempo de resolução de falhas e diminui intervenções corretivas — fatores que reduzem significativamente o TCO em ambientes críticos 24x7.

15.1.3. Alinhamento à Responsabilidade Fiscal e à Eficiência

A adoção da solução integrada é economicamente responsável, conforme os princípios da Administração Pública, porque:

- garante previsibilidade dos dispêndios durante todo o ciclo de vida;
- reduz riscos de transição, indisponibilidade e despesas inesperadas;
- evita contratações redundantes e fragmentadas;
- preserva investimentos anteriores e expande capacidades com menor custo marginal.

Assim, a solução atende aos princípios de economicidade, eficiência, motivação e continuidade dos serviços públicos essenciais.

15.1.4. Catálogo de Soluções de TIC

A solução pretendida não possui equivalente padronizado no Catálogo de Soluções de TIC do Governo Digital no formato requisitado.

Assim, a contratação permanece fundamentada no presente ETP e nos termos de referência específicos, cujas condições técnicas e econômicas estão descritas detalhadamente nas propostas anexas.

15.2. Justificativa Econômica da Integração (Switching + WiFi + Firewall)

A integração de switches multigigabit, Access Points corporativos e firewall Fortinet reduz o TCO por:

- eliminar plataformas de gerenciamento adicionais;
- evitar incompatibilidades entre fabricantes;
- consolidar suporte e responsabilidade técnica em um único fornecedor;
- otimizar PoE, uplinks, políticas de segurança e operação assistida;
- reduzir esforço interno de operação e troubleshooting;
- evitar gastos com consultorias independentes;
- assegurar atualizações, suporte e substituição de hardware por 36 meses.

A padronização da rede reduz custos diretos e indiretos, melhora a previsibilidade financeira e assegura continuidade operacional, mitigando riscos de falhas em ambiente crítico.

15.3. Do Parcelamento sob a Ótica Econômica

15.3.1. Desvantagens do Fracionamento (Gestão e Fiscalização)

O fracionamento entre diferentes fornecedores (firewall, switches, APs, acessórios ópticos, instalação, operação assistida) traria impactos econômicos negativos:

- pulverização das responsabilidades;
- ampliação de custos administrativos e transacionais;
- sobreposição de garantias e disputas entre fornecedores;
- maior risco de incompatibilidade técnica;
- fiscalização mais custosa e menos eficiente;
- aumento do tempo de resposta em incidentes.

Em ambiente crítico 24x7, tais fatores ampliariam riscos operacionais e custos indiretos.

15.3.2. Perda de Ganho de Escala e Sinergias

O fracionamento comprometeria:

- ganho de escala na aquisição de hardware e serviços;
- uniformização de GBICs, acessórios e peças;
- treinamento único e otimizado;
- integração de ferramentas de gestão;
- logística e implantação coordenada.

Isso elevaria:

- CAPEX total;
- OPEX operacional;
- custos administrativos e contratuais;
- tempo de estabilização do ambiente.

A solução integrada maximiza o efeito de escala e reduz custos indiretos ao longo de todo o ciclo de vida.

16. Benefícios a serem alcançados com a contratação

16. Objetivos da Contratação

A contratação da solução integrada de segurança perimetral (NGFW), switching e WiFi corporativo tem como objetivos:

16.1. Reforçar a capacidade e o desempenho da segurança da informação

i. Ampliar a capacidade de processamento e inspeção de tráfego, garantindo desempenho compatível com o crescimento da demanda por serviços digitais e maior volume de dados.
ii. Modernizar a segurança perimetral com tecnologia atual de mercado, adotando firewalls de próxima geração com inspeção profunda, análise avançada de ameaças e políticas unificadas.
iii. Mitigar riscos associados a hardware/software obsoletos, reduzindo falhas operacionais e aumentando a confiabilidade da infraestrutura.
iv. Eliminação de vulnerabilidades por meio de assinaturas atualizadas, inteligência global de ameaças e mecanismos modernos de detecção e proteção.
v. Proteger serviços essenciais de TIC que dependem de VPNs, autenticação, filtragem e conectividade segura, garantindo comunicação confiável entre ambientes internos e externos.
vi. Adotar arquitetura integrada e definida por software, combinando IPS, filtragem web, antivírus, controle de aplicações, análise comportamental e balanceamento em plataforma única.
vii. Elevar a maturidade de segurança com princípios equivalentes ao modelo Zero Trust, incluindo microsegmentação, controle granular, inspeção contínua e validação permanente de identidade.

16.2. Garantir alta disponibilidade, continuidade e resiliência

i. Assegurar alta disponibilidade (HA) com capacidade de assumir operações automaticamente em caso de falhas, reduzindo indisponibilidades.
ii. Aumentar a disponibilidade dos serviços de TIC, garantindo resistência a picos de tráfego e ataques sem degradação significativa de desempenho.
iii. Permitir janelas de manutenção sem impacto, graças à redundância e à maior capacidade da solução.
iv. Melhorar a resiliência da infraestrutura, permitindo rápida ativação de novos serviços e expansão modular conforme o crescimento institucional.
v. Preparar o ambiente para expansão pelos próximos cinco anos, evitando substituições disruptivas e preservando investimentos realizados.

16.3. Modernizar e estruturar a rede WiFi corporativa

i. Implementar uma rede WiFi corporativa robusta, inexistente até o momento, com equipamentos modernos e de alto desempenho.
ii. Adotar WiFi 6/6E, garantindo conectividade rápida, estável e resiliente para usuários e sistemas.
iii. Assegurar continuidade operacional da rede sem fio, com implantação assistida, configuração padronizada e boas práticas do fabricante.
iv. Garantir expansão futura da rede WiFi, permitindo crescimento sem interrupções significativas.
v. Reduzir riscos de falhas e aumentar a vida útil da solução WiFi, adotando hardware novo e com suporte oficial de 36 meses.
vi. Garantir compatibilidade com novos padrões e políticas, assegurando longevidade e capacidade de atualização.
vii. Fortalecer a segurança da mobilidade, com WPA3, 802.1X, segmentação, criptografia moderna e controles dinâmicos por usuário /dispositivo.
viii. Oferecer conectividade estável para serviços corporativos críticos, garantindo mobilidade com qualidade e baixa latência.

16.4. Integrar toda a infraestrutura em gestão centralizada

i. Unificar a administração da infraestrutura de segurança, switching e WiFi em uma única plataforma (Security Fabric), eliminando dependência de múltiplos consoles.
ii. Simplificar a gestão operacional, com automação de políticas, relatórios integrados e diagnóstico avançado.
iii. Melhorar o tempo de resposta a incidentes, com telemetria unificada e correlação automática de eventos.
iv. Aumentar a escalabilidade da solução, permitindo evolução ordenada, controlada e segura da infraestrutura.
v. Viabilizar integrações com ambientes híbridos e multicloud, mantendo políticas unificadas, conformidade com a LGPD e governança centralizada.

16.5. Fortalecer governança, conformidade e planejamento de longo prazo

i. Aprimorar governança de TIC, com arquitetura padronizada, consolidação de plataformas e redução de soluções fragmentadas.
ii. Garantir aderência regulatória, facilitando controles, auditorias e aplicação de políticas corporativas.
iii. Preparar a infraestrutura para expansão futura, sem necessidade de trocas abruptas ou reestruturação profunda.

17. Providências a serem Adotadas

17.1. Após a assinatura do contrato deverá ser realizada reunião inicial com representantes da CONTRATANTE e da CONTRATADA, para alinhamento das condições para o início da prestação dos serviços.

17.2. Após a assinatura do contrato, deverá ser realizada reunião entre os representantes da Contratante e da CONTRATADA para alinhar as formas e os prazos para execução dos serviços relacionados à solução.

17.3. Antes da entrega dos equipamentos, o fiscal técnico deverá verificar a disponibilidade de local para instalação dos novos equipamentos, incluindo compatibilidade de cabos e tomadas elétricas e lógicas com os equipamentos.

17.4. As administrações dos locais de entrega devem ser avisados com antecedência sobre a data prevista para entrega dos equipamentos.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Após análise técnica, econômica, operacional e de riscos, concluise que a contratação da solução integrada de segurança perimetral, switching e WiFi corporativo é plenamente viável e adequada às necessidades institucionais. A proposta atende aos requisitos de negócio e aos objetivos tecnológicos da organização, alinhandose aos princípios de economicidade, continuidade, eficiência e governança previstos na Lei nº 14.133/2021 e na IN SGD/ME nº 94/2022.

A manutenção e evolução da plataforma Fortinet — já consolidada no ambiente — e sua integração direta com os switches multigigabit e Access Points corporativos garantem coerência arquitetural, baixa complexidade de transição, menor risco operacional e melhor aproveitamento dos investimentos realizados. Essa abordagem reduz significativamente custos de migração, treinamento e suporte, ao mesmo tempo em que simplifica a administração com gestão unificada via Security Fabric.

A solução integrada assegura alta disponibilidade, resiliência, eficiência operacional e continuidade dos serviços críticos, oferecendo escalabilidade para os próximos anos, compatibilidade com tecnologias emergentes e robusto fortalecimento da postura de segurança da informação. A arquitetura proposta reduz vulnerabilidades, diminui a probabilidade de falhas e garante operação estável 24×7, atendendo plenamente aos requisitos técnicos e estratégicos da organização.

Dessa forma, a contratação demonstra-se tecnicamente adequada, economicamente vantajosa e operacionalmente alinhada às necessidades presentes e futuras, recomendando-se seu prosseguimento conforme os parâmetros estabelecidos neste ETP.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Despacho: Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 94/2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento.

DAVID FERNANDES FRANCA

Integrante Requisitante

Assinou eletronicamente em 17/06/2026 às 15:22:58.

Despacho: Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 94/2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento.

RODRIGO RIBEIRO AFFONSO ALVES

Integrante Técnico

Assinou eletronicamente em 17/06/2026 às 15:25:48.

Despacho: Aprovo o ETP Digital e atesto sua conformidade, nos termos do §2º do art. 11 da IN SGD/ME nº 94/2022.

DANIELLA CHRISTINA XAVIER DE OLIVEIRA

Superintendente de TI

Assinou eletronicamente em 17/06/2026 às 15:11:47.