

INST. FED. DE SÃO PAULO/CAMPUS CAPIVARI

Estudo Técnico Preliminar 25/2025

1. Informações Básicas

Número do processo: 23430.001033.2025-79

2. Descrição da necessidade

Renovação de Licença do Firewall Forcepoint NGFW 1105 - Vencimento em 07/07/2025

1. Objeto da Contratação

A presente contratação tem como objeto a **Renovação de Licença do Firewall Forcepoint NGFW 1105**, vencida em **07 de julho de 2025**. Esta renovação é imperativa para a manutenção da segurança perimetral da rede institucional do IFSP - Campus Capivari, garantindo a continuidade e a integridade dos serviços de Tecnologia da Informação.

2. Justificativa da Necessidade

A segurança da informação é um pilar fundamental para a continuidade das atividades-fim deste órgão. A infraestrutura de rede, que suporta sistemas críticos como SUAP, e-mail institucional e bases de dados acadêmicas, depende intrinsecamente de uma robusta defesa contra ameaças cibernéticas. O firewall Forcepoint NGFW 1105 é o principal componente dessa defesa, atuando como barreira digital entre as redes internas confiáveis e a internet.

2.1. Funções Essenciais do Firewall para a Organização:

- **Controle de Acesso:** Filtra conexões e permite ou bloqueia tráfego com base em políticas de segurança predefinidas, controlando o acesso a recursos críticos da rede.
- **Proteção Perimetral:** Atua como a primeira linha de defesa contra ameaças externas, monitorando todo o tráfego de entrada e saída e prevenindo acessos não autorizados.
- **Monitoramento e Auditoria:** Registra conexões e tentativas de acesso, gerando logs detalhados essenciais para análise de segurança e auditoria forense.

2.2. A Evolução para Next Generation Firewall (NGFW) e Sua Relevância:

O Forcepoint NGFW 1105, sendo um firewall de próxima geração, incorpora funcionalidades avançadas cruciais para a proteção contra o cenário atual de ameaças, tais como:

- **Inspecção Profunda de Pacotes (DPI):** Analisa o conteúdo dos pacotes de dados, não apenas os cabeçalhos, para identificar ameaças ocultas.
- **Prevenção contra Intrusões (IPS):** Detecta e impede tentativas de invasão e exploração de vulnerabilidades.
- **Filtro de Aplicações e Protocolos:** Permite o controle granular sobre quais aplicações e protocolos podem ser utilizados na rede, reduzindo a superfície de ataque.
- **Deteção de Ameaças Avançadas e Integração com Threat Intelligence:** Utiliza inteligência sobre ameaças para identificar e mitigar ataques emergentes e persistentes.

3. Situação-Problema e Consequências da Não Contratação

A não renovação das licenças do Forcepoint NGFW 1105, vencida em **07 de julho de 2025**, acarretará na **exposição crítica da infraestrutura de TI**, comprometendo severamente a segurança perimetral da rede institucional. Este cenário gera uma série de problemas derivados de alto impacto:

3.1. Segurança Comprometida:

- Vulnerabilidades de segurança descobertas após o vencimento da licença não serão corrigidas pelo fabricante.
- A base de assinaturas de ameaças ficará obsoleta, impossibilitando a detecção e mitigação de novos malwares e ataques.
- Perda da capacidade de enfrentamento de novas modalidades de ataques cibernéticos emergentes.

3.2. Risco Operacional Elevado:

- O equipamento está em período de **End of Life (EoL)**, o que significa que não há mais desenvolvimento de novas funcionalidades e o suporte do fabricante se torna limitado (apenas correções críticas).
- Em caso de falha crítica de hardware, a falta de suporte técnico especializado e a impossibilidade de recuperação de configurações podem resultar em indisponibilidade prolongada (superior a 72 horas) dos sistemas.
- O prazo definido para o término do suporte do fabricante para o equipamento EoL agrava o risco de falhas irrecuperáveis.

3.3. Não Conformidade Regulatória:

A ausência de uma solução de segurança de rede atualizada e suportada implica em:

- **Descumprimento do Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação - PNSI):** A PNSI estabelece princípios e diretrizes para a governança da segurança da informação em órgãos e entidades da administração pública federal, e a ausência de um firewall com licenças ativas e suporte técnico viola diretamente essas diretrizes.
- **Inadequação às medidas de proteção exigidas pela LGPD (Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais):** A LGPD exige a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Um firewall sem licença e suporte representa uma falha crítica nessas medidas.
- **Violação da Política Institucional de Segurança da Informação:** A política interna de segurança do IFSP Campus Capivari estabelece requisitos mínimos de proteção que seriam violados.

3.4. Impacto Acadêmico e Administrativo:

- **Vulnerabilidade de Sistemas Críticos:** Sistemas essenciais como o Sistema Unificado de Administração Pública (SUAP), e-mail institucional e bibliotecas digitais ficariam expostos, com risco de interrupção e comprometimento de dados.
- **Comprometimento de Atividades-Fim:** Pesquisas, acesso a bases científicas, processos administrativos e financeiros seriam diretamente impactados pela instabilidade e insegurança da rede.
- **Exposição de Dados Sensíveis:** Informações administrativas, financeiras e acadêmicas poderiam ser acessadas indevidamente, gerando prejuízos incalculáveis.

4. Consequências da Não Contratação (Síntese Executiva)

A não renovação das licenças do firewall resultará na inoperabilidade do equipamento em sua capacidade de proteção perimetral, cessando as atualizações de segurança e o suporte técnico essencial. Isso exporá a infraestrutura de TI a ataques cibernéticos, com potencial para:

- **Interrupção dos serviços:** Paralisação de sistemas essenciais ao funcionamento do órgão.
- **Perda ou vazamento de dados:** Comprometimento de informações sensíveis, incluindo dados pessoais, com implicações legais e reputacionais.
- **Danos à imagem institucional:** Perda de confiança da comunidade acadêmica, parceiros e sociedade em geral.
- **Sanções e multas:** Em razão do descumprimento de leis como a LGPD e o Decreto nº 9.637/2018.
- **Custos de recuperação:** Gastos adicionais e imprevisíveis para recuperação de sistemas e dados após um incidente de segurança.

A contratação, portanto, não se trata de uma mera aquisição de licenças, mas sim da **garantia da continuidade das operações, da proteção de dados críticos e da conformidade legal e normativa da instituição.**

5. Público-Alvo e Benefícios da Contratação

5.1. Identificação do Público-Alvo (Beneficiários Diretos e Indiretos):

A interrupção dos serviços de segurança impacta diretamente:

- **Beneficiários Diretos:**
 - **800+ usuários da comunidade acadêmica:** Servidores docentes, técnico-administrativos, estudantes e terceirizados, que dependem da infraestrutura de TI para suas atividades diárias.
 - **200+ dispositivos institucionais:** Conectados à rede e que necessitam de proteção contínua.
 - **Equipe de TI:** Responsável pela gestão da infraestrutura de segurança, que perderia suas ferramentas de monitoramento e defesa.
 - **Gestores administrativos:** Que dependem da disponibilidade e segurança dos sistemas institucionais.
- **Beneficiários Indiretos:**
 - Comunidade externa que acessa serviços digitais do órgão [ESPECIFICAR: nome do órgão, se aplicável].
 - Parceiros institucionais que mantêm conectividade com a rede.
 - Órgãos de controle que fiscalizam a conformidade de segurança.
 - A sociedade em geral, beneficiária dos serviços educacionais protegidos.

5.2. Valor a Ser Entregue à Organização (Benefícios da Contratação):

A renovação das licenças não apenas mitiga os riscos, mas agrega valor significativo em diversas frentes:

- **Valor Estratégico Institucional:**
 - Proteção continuada da missão educacional, garantindo que atividades de ensino, pesquisa e extensão permaneçam seguras e disponíveis.
 - Conformidade regulatória assegurada, atendendo integralmente aos normativos federais e institucionais, evitando sanções e multas.

- Reputação e credibilidade preservadas, mantendo a confiança da comunidade acadêmica e da sociedade.
- **Valor Operacional:**
 - Continuidade garantida com alta disponibilidade (99,5%+) dos sistemas críticos.
 - Proteção atualizada e defesa em tempo real contra ameaças emergentes.
 - Gestão centralizada e administração unificada das políticas de segurança.
- **Valor Econômico-Financeiro:**
 - Economia significativa de **R\$ 140.000+** (estimado) ao evitar a substituição completa do equipamento em razão do EoL, pois a renovação da licença prolonga a vida útil da solução existente.
 - Otimização do Retorno sobre o Investimento (ROI) em **350%+** comparado à aquisição de uma nova solução.
 - Prevenção de custos adicionais de **R\$ 200.000+** (estimado) em possíveis incidentes de segurança, interrupções e recuperação de dados.
- **Valor Social:**
 - Criação e manutenção de um ambiente educacional seguro para mais de 800 usuários.
 - Preservação do patrimônio digital, incluindo mais de 10 anos de produção acadêmica digitalizada.
 - Garantia da continuidade educacional sem interrupções no processo de ensino-aprendizagem.

6. Urgência e Criticalidade

O **prazo limite para a contratação é setembro de 2025**, em virtude do iminente vencimento das licenças do firewall Forcepoint NGFW 1105. Considerando o tempo necessário para um processo licitatório completo, estima-se um tempo disponível de apenas **3 meses** para a sua conclusão. Diante disso, a contratação é classificada como **URGENTE E INADIÁVEL**, requerendo prioridade máxima no planejamento e execução.

3. Área requisitante

Área Requisitante	Responsável
CTI-CPV	Junio Rodrigues de Oliveira

4. Necessidades de Negócio

4.1 Metas de Negócio

META PRIMÁRIA: Manter a **segurança perimetral da rede institucional** em conformidade com os padrões de segurança da informação exigidos para instituições federais de ensino.

METAS SECUNDÁRIAS:

- Garantir **99,5% de disponibilidade** dos sistemas críticos institucionais
- Manter **conformidade integral** com normativos de segurança da informação
- Assegurar **proteção adequada** de dados pessoais conforme LGPD
- Preservar a **reputação institucional** quanto à segurança cibernética

4.2 Objetivos Estratégicos

OBJETIVO 1: CONTINUIDADE OPERACIONAL

- **O QUE:** Manter operação ininterrupta dos serviços de TI críticos
- **COMO:** Renovação das licenças de suporte e garantia do firewall
- **RESULTADO ESPERADO:** Zero interrupções por falhas de segurança

OBJETIVO 2: CONFORMIDADE REGULATÓRIA

- **O QUE:** Atender integralmente aos normativos de segurança
- **COMO:** Manutenção de proteções atualizadas e suporte técnico
- **RESULTADO ESPERADO:** Zero não conformidades em auditorias

OBJETIVO 3: PROTEÇÃO PATRIMONIAL

- **O QUE:** Proteger ativos informacionais da instituição
- **COMO:** Defesa perimetral atualizada contra ameaças
- **RESULTADO ESPERADO:** Zero incidentes com perda de dados

OBJETIVO 4: OTIMIZAÇÃO DE RECURSOS

- **O QUE:** Maximizar aproveitamento de investimentos existentes
- **COMO:** Extensão da vida útil do equipamento durante período EoL
- **RESULTADO ESPERADO:** Economia de 78% versus substituição

4.3 Resultados de Negócio Esperados

CURTO PRAZO (0-6 meses):

- Licenças renovadas e operacionais
- Atualizações de segurança aplicadas
- Suporte técnico restabelecido

MÉDIO PRAZO (6-18 meses):

- Proteção contra ameaças emergentes mantida
- Conformidade regulatória consolidada
- Confiança da comunidade preservada

LONGO PRAZO (18-36 meses):

- Segurança institucional garantida durante período EoL
- Planejamento para futura substituição estabelecido
- ROI maximizado do investimento em infraestrutura
-

4.4 Definição do Objeto (O QUE)

OBJETO DA CONTRATAÇÃO: A solução deve prover **licenciamento de software de segurança perimetral** que garanta:

- **Atualizações automáticas** de assinaturas de ameaças e patches de segurança
- **Suporte técnico especializado** 24x7 do fabricante
- **Garantia de hardware** com substituição acelerada em caso de falha
- **Capacidades de gerenciamento** centralizado de políticas de segurança
- **Proteção para ambientes híbridos** incluindo acesso a serviços em nuvem

INDEPENDENTEMENTE DA TECNOLOGIA EMPREGADA, a solução deve assegurar continuidade da proteção perimetral durante o período de End of Life do equipamento existente.

5. Necessidades Tecnológicas

5.1 Padrões Tecnológicos Institucionais

ARQUITETURA DE SEGURANÇA ESTABELECIDA:

- **Firewall perimetral único:** Forcepoint NGFW 1105 como elemento central
- **Integração com Active Directory:** Autenticação centralizada de usuários
- **Políticas de segurança consolidadas:** 3+ anos de configurações refinadas
- **Monitoramento centralizado:** Integração com ferramentas de SIEM

METODOLOGIAS E PROCESSOS DEFINIDOS:

- **Gestão de incidentes:** Procedimentos padronizados para resposta a ameaças
- **Backup de configurações:** Rotinas automatizadas de preservação de políticas
- **Atualizações de segurança:** Processos de aplicação de patches validados
- **Auditoria e compliance:** Relatórios regulares de conformidade

5.2 Infraestrutura Computacional Existente

CAPACIDADE INSTALADA:

- **Rede backbone:** Gigabit Ethernet com redundância
- **Servidor de gerenciamento:** Dedicated management appliance
- **Integração de rede:** VLANs segmentadas por função organizacional

- **Conectividade externa:** Links redundantes para Internet e RNP

COMPETÊNCIAS DA EQUIPE:

- **Administradores certificados:** Profissionais com experiência em Forcepoint
- **Conhecimento consolidado:** 3+ anos de operação do ambiente atual
- **Procedimentos documentados:** Runbooks e documentação técnica atualizada
- **Treinamento especializado:** Equipe capacitada nas funcionalidades específicas

5.3 Cuidados com Segurança da Informação

POLÍTICAS DE SEGURANÇA IMPLEMENTADAS:

- **Classificação de informações:** Dados públicos, internos, confidenciais e secretos
- **Controle de acesso:** Princípio do menor privilégio aplicado
- **Gestão de logs:** Retenção e análise de registros de segurança
- **Resposta a incidentes:** Plano de contingência para ameaças

BOAS PRÁTICAS ESTABELECIDAS:

- **Defesa em profundidade:** Múltiplas camadas de proteção implementadas
- **Monitoramento contínuo:** Supervisão 24x7 de eventos de segurança
- **Atualizações regulares:** Janelas de manutenção estabelecidas
- **Testes de segurança:** Avaliações periódicas de vulnerabilidades

5.4 Decisões Estratégicas de TIC

HISTÓRICO DE DECISÕES:

- **2022:** Implementação do Forcepoint NGFW 1105 como solução perimetral
- **2023-2024:** Consolidação de políticas e procedimentos operacionais
- **2025:** Decisão de manter investimento durante período EoL

PROJETOS FUTUROS:

- **2028:** Planejamento para substituição por solução de próxima geração
- **Integração cloud:** Expansão para proteção de workloads em nuvem
- **Zero Trust:** Evolução para arquitetura de confiança zero

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

6.1 Requisitos Internos Funcionais

RF01 - ATUALIZAÇÕES DE SEGURANÇA

- **Descrição:** Fornecimento automático de assinaturas de ameaças atualizadas
- **Criticidade:** OBRIGATÓRIO
- **Justificativa:** Essencial para proteção contra ameaças emergentes

RF02 - SUPORTE TÉCNICO ESPECIALIZADO

- **Descrição:** Acesso 24x7 ao suporte técnico do fabricante
- **Criticidade:** OBRIGATÓRIO
- **Justificativa:** Necessário para resolução de incidentes críticos

RF03 - GERENCIAMENTO CENTRALIZADO

- **Descrição:** Interface unificada para administração de políticas
- **Criticidade:** OBRIGATÓRIO
- **Justificativa:** Fundamental para eficiência operacional

RF04 - PROTEÇÃO PARA NUVEM

- **Descrição:** Capacidade de inspeção e controle de tráfego para serviços cloud
- **Criticidade:** OBRIGATÓRIO

- **Justificativa:** Atender demandas de transformação digital

6.2 Requisitos Internos Não Funcionais

RNF01 - DISPONIBILIDADE

- **Descrição:** Disponibilidade mínima de 99,5% do serviço
- **Métrica:** Uptime mensal $\geq 99,5\%$
- **Justificativa:** Garantir continuidade dos serviços acadêmicos

RNF02 - DESEMPENHO

- **Descrição:** Tempo de resposta para resolução de incidentes
- **Métrica:** ≤ 4 horas para incidentes críticos
- **Justificativa:** Minimizar impacto de falhas operacionais

RNF03 - SEGURANÇA

- **Descrição:** Atualizações de segurança aplicadas automaticamente
- **Métrica:** 100% das atualizações críticas em $\leq 24h$
- **Justificativa:** Manter proteção atualizada continuamente

RNF04 - USABILIDADE

- **Descrição:** Interface de gerenciamento intuitiva e acessível
- **Métrica:** Compatibilidade com padrões de acessibilidade web
- **Justificativa:** Facilitar operação pela equipe técnica

RNF05 - AUDITABILIDADE

- **Descrição:** Geração de logs detalhados e relatórios de conformidade
- **Métrica:** Retenção de logs por 12+ meses
- **Justificativa:** Atender requisitos de auditoria e compliance

6.3 Requisitos Externos

RE01 - CONFORMIDADE LEGAL (LGPD)

- **Descrição:** Atendimento aos requisitos de proteção de dados pessoais
- **Base Legal:** Lei nº 13.709/2018
- **Obrigatoriedade:** Mandatório para órgãos públicos

RE02 - POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

- **Descrição:** Conformidade com diretrizes de segurança cibernética
- **Base Legal:** Decreto nº 9.637/2018
- **Obrigatoriedade:** Mandatório para órgãos federais

RE03 - GESTÃO DE SEGURANÇA DA INFORMAÇÃO

- **Descrição:** Implementação de controles de segurança adequados
- **Base Legal:** Instrução Normativa GSI/PR nº 1/2008
- **Obrigatoriedade:** Mandatório para administração federal

RE04 - CONTRATAÇÕES SUSTENTÁVEIS

- **Descrição:** Critérios de sustentabilidade ambiental e social
- **Base Legal:** Decreto nº 10.024/2019
- **Obrigatoriedade:** Mandatório para contratações públicas

RE05 - ACESSIBILIDADE DIGITAL

- **Descrição:** Conformidade com padrões de acessibilidade
- **Base Legal:** Lei nº 13.146/2015 e Decreto nº 5.296/2004
- **Obrigatoriedade:** Mandatório para serviços públicos digitais

7. Estimativa da demanda - quantidade de bens e serviços

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

7.1 Descrição Detalhada dos Itens

ITEM ÚNICO: Licenciamento de software para firewall Forcepoint NGFW 1105

COMPOSIÇÃO DO LICENCIAMENTO:

Componente	Quantidade	Período	Justificativa
Essential Support	1 licença	33 meses	Suporte e atualizações críticas
Advanced RMA Warranty	1 licença	33 meses	Garantia com substituição acelerada
Cloud Access & Network Security	1 licença	33 meses	Proteção para ambientes híbridos
Management Center	1 licença	33 meses	Gerenciamento centralizado

7.2 Memorial de Cálculo das Quantidades

7.2.1 Método de Cálculo Adotado

BASE DE CÁLCULO: Equipamento único existente na infraestrutura

JUSTIFICATIVA QUANTITATIVA:

- 1 appliance Forcepoint NGFW 1105 instalado e operacional
- 1 conjunto de licenças necessário por equipamento
- Não há redundância ativa que exija licenciamento adicional

8. Levantamento de soluções

8. LEVANTAMENTO DE SOLUÇÕES

8.1 Metodologia de Levantamento

O levantamento de soluções foi realizado considerando as **características específicas** da infraestrutura existente e os **requisitos técnicos** identificados nas seções anteriores.

CRITÉRIOS DE SELEÇÃO DE SOLUÇÕES:

- Compatibilidade com equipamento Forcepoint NGFW 1105 existente
- Atendimento aos requisitos funcionais e não funcionais
- Disponibilidade no mercado nacional
- Conformidade com normativos de segurança

8.2 Soluções Identificadas

8.2.1 SOLUÇÃO A: Renovação de Licenças Originais Forcepoint

DESCRIÇÃO: Renovação das licenças existentes diretamente com partners autorizados Forcepoint **CARACTERÍSTICAS:**

- Essential Support para atualizações e suporte técnico
- Advanced RMA Warranty para substituição acelerada
- Cloud Access & Network Security para proteção híbrida
- Management Center para gerenciamento centralizado **ADEQUAÇÃO: TOTALMENTE ADEQUADA**

8.2.2 SOLUÇÃO B: Substituição por Novo Firewall

DESCRIÇÃO: Aquisição de novo appliance firewall de próxima geração **CARACTERÍSTICAS:**

- Novo hardware com garantia total
- Licenças incluídas por período determinado
- Migração de configurações necessária
- Descarte do equipamento atual **ADEQUAÇÃO:** TECNICAMENTE VIÁVEL, ECONOMICAMENTE INVIÁVEL

8.2.3 SOLUÇÃO C: Migração para Firewall Cloud/Virtual

DESCRIÇÃO: Substituição por solução de firewall virtualizada ou baseada em nuvem **CARACTERÍSTICAS:**

- Infraestrutura como serviço (IaaS)
- Escalabilidade automática
- Migração completa de arquitetura necessária
- Dependência de conectividade externa **ADEQUAÇÃO:** INADEQUADA PARA O CONTEXTO ATUAL

8.2.4 SOLUÇÃO D: Operação Sem Licenças de Suporte

DESCRIÇÃO: Manter equipamento operacional sem renovação de licenças **CARACTERÍSTICAS:**

- Funcionamento básico do hardware
- Sem atualizações de segurança
- Sem suporte técnico do fabricante
- Sem garantia de substituição **ADEQUAÇÃO:** INACEITÁVEL POR RISCOS DE SEGURANÇA

9. Análise comparativa de soluções

9. ANÁLISE COMPARATIVA DE SOLUÇÕES

9.1 Matriz de Comparação

Critério	Peso	Sol. A (Ren.)	Sol. B (Subst)	Sol. C (Cloud)	Sol. D (Sem Lic)
Atendimento aos Requisitos	25%	10	9	6	2
Custo Total (TCO)	20%	10	3	5	10
Tempo de Implementação	15%	10	4	3	10
Riscos Técnicos	15%	9	6	7	1
Conformidade Regulatória	15%	10	9	7	1
Aproveitamento de Investimentos	10%	10	2	2	8
PONTUAÇÃO TOTAL	100%	9,6	5,8	5,4	4,7

9.2 Análise Detalhada por Solução

9.2 .1. SOLUÇÃO A: Renovação de Licenças (ESCOLHIDA)

VANTAGENS:

- Aproveitamento integral do investimento existente
- Continuidade operacional sem interrupções
- Equipe técnica já capacitada
- Configurações e políticas preservadas
- Menor custo total de propriedade
- Implementação imediata

DESVANTAGENS:

- Equipamento em período End of Life
- Limitação temporal da solução (36 meses)

9.2 .2. SOLUÇÃO B: Substituição por Novo Firewall**VANTAGENS:**

- Hardware novo com garantia completa
- Tecnologia atualizada
- Vida útil estendida

DESVANTAGENS:

- Custo 4,5x maior (R\$ 180.000+)
- Necessidade de migração complexa
- Risco de interrupção durante transição
- Perda do investimento em treinamento
- Tempo de implementação prolongado

9.2 .3. SOLUÇÃO C: Migração para Cloud**VANTAGENS:**

- Escalabilidade automática
- Atualizações automáticas

DESVANTAGENS:

- Dependência de conectividade externa
- Mudança radical de arquitetura
- Custos recorrentes elevados
- Complexidade de migração
- Questões de soberania de dados

9.2 .4 SOLUÇÃO D: Operação Sem Licenças**VANTAGENS:**

- Sem custos imediatos

DESVANTAGENS:

- Exposição crítica a vulnerabilidades
- Não conformidade regulatória
- Ausência de suporte técnico
- Risco reputacional inaceitável

10. Registro de soluções consideradas inviáveis

10 REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

10.1 SOLUÇÃO INVIÁVEL 1: Firewall Open Source

DESCRIÇÃO: Implementação de solução baseada em software livre (pfSense, OPNsense)

MOTIVOS DE INVIABILIDADE:

- **Suporte limitado:** Sem suporte comercial 24x7 adequado
- **Complexidade de migração:** Necessidade de reconfiguração completa
- **Capacidades limitadas:** Funcionalidades inferiores ao NGFW atual
- **Risco operacional:** Dependência de conhecimento técnico específico interno

10.2 SOLUÇÃO INVIÁVEL 2: Múltiplos Firewalls de Menor Porte

DESCRIÇÃO: Substituição por vários appliances de menor capacidade

MOTIVOS DE INVIABILIDADE:

- **Complexidade de gestão:** Múltiplos pontos de administração
- **Custo elevado:** Licenciamento múltiplo mais caro
- **Arquitetura inadequada:** Não atende ao design de rede atual
- **Overhead operacional:** Aumento significativo da carga de trabalho

10.3 SOLUÇÃO INVIÁVEL 3: Solução Híbrida Multi-Vendor

DESCRIÇÃO: Combinação de equipamentos de diferentes fabricantes

MOTIVOS DE INVIABILIDADE:

- **Incompatibilidade:** Diferentes interfaces e metodologias de gestão
- **Complexidade técnica:** Integração complexa entre soluções
- **Suporte fragmentado:** Múltiplos contratos de suporte necessários
- **Custos elevados:** Soma de licenciamentos distintos

10.4 SOLUÇÃO INVIÁVEL 4: Postergação da Decisão

DESCRIÇÃO: Adiar a contratação para exercício seguinte

MOTIVOS DE INVIABILIDADE:

- **Prazo crítico:** Vencimento das licenças em setembro/2025
- **Risco de segurança:** Exposição desnecessária a vulnerabilidades
- **Não conformidade:** Violação de normativos de segurança
- **Impacto operacional:** Possível interrupção de serviços críticos

11. Análise comparativa de custos (TCO)

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

11.1 Metodologia de Cálculo do TCO

PERÍODO DE ANÁLISE: 36 meses (2025-2028) COMPONENTES DO TCO:

- Custos de aquisição/licenciamento
- Custos de implementação
- Custos operacionais
- Custos de descontinuação
- Custos de oportunidade

11.2 TCO da Solução A: Renovação de Licenças

Componente de Custo	Valor (R\$)	Justificativa
Licenças (36 meses)	40.000,00	Renovação das 4 licenças essenciais
Implementação	0,00	Ativação automática, sem custos adicionais
Operação	0,00	Equipe interna já capacitada
Manutenção	0,00	Incluída nas licenças de suporte
Descontinuação	0,00	Não aplicável no período
TOTAL TCO	30.784,20	R\$ 855,12/mês

11.3 TCO da Solução B: Substituição por Novo Firewall

Componente de Custo	Valor (R\$)	Justificativa
Novo Equipamento (ESTIMADO)	120.000,00	Appliance NGFW equivalente
Licenças (36 meses)(ESTIMADO)	45.000,00	Licenciamento para novo equipamento
Implementação (ESTIMADO)	15.000,00	Migração, configuração, testes
Treinamento(ESTIMADO)	8.000,00	Capacitação da equipe
Descarte(ESTIMADO)	2.000,00	Descomissionamento do equipamento atual
TOTAL TCO	190.000,00	R\$ 5.277,78/mês

11.4 TCO da Solução C: Migração para Cloud

Componente de Custo	Valor (R\$)	Justificativa
Serviço Cloud (36 meses)(ESTIMADO)	108.000,00	R\$ 3.000/mês por capacidade equivalente
Implementação (ESTIMADO)	25.000,00	Migração complexa de arquitetura
Conectividade (ESTIMADO)	36.000,00	Enlaces dedicados adicionais
Treinamento (ESTIMADO)	12.000,00	Nova plataforma para equipe
Descarte (ESTIMADO)	2.000,00	Descomissionamento
TOTAL TCO	183.000,00	R\$ 5.083,33/mês

11.5 Comparativo de TCO

Solução	TCO 36 meses	TCO Mensal	Economia vs Sol. A
A - Renovação	R\$ 30.784,20	R\$ 1.111,11	-
B - Substituição	R\$ 190.000,00	R\$ 5.277,78	-R\$ 150.000,00
C - Cloud	R\$ 183.000,00	R\$ 5.083,33	-R\$ 143.000,00

CONCLUSÃO TCO: A Solução A apresenta **economia de 78-79%** comparada às alternativas.

12. Descrição da solução de TIC a ser contratada

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

12.1 Caracterização Geral da Solução

NATUREZA: Licenciamento de software de segurança para firewall de próxima geração

MODELO: Renovação de licenças para equipamento Forcepoint NGFW 1105 existente

MODALIDADE: Licenciamento por subscrição com duração de 36 meses

ARQUITETURA: Appliance físico on-premises com gerenciamento centralizado

12.2 Componentes da Solução

12.2.1 Essential Support

FUNÇÃO: Base de suporte técnico e atualizações de segurança

CARACTERÍSTICAS:

- Atualizações automáticas de assinaturas de ameaças
- Patches de segurança críticos
- Suporte técnico 24x7x365 do fabricante
- Acesso à base de conhecimento técnica
- Suporte remoto e via portal web

12.2.2 Advanced RMA (Return Merchandise Authorization) Warranty

FUNÇÃO: Garantia estendida com substituição acelerada de hardware

CARACTERÍSTICAS:

- Substituição de hardware em 4-8 horas úteis
- Equipamento de reposição pré-configurado
- Logística reversa incluída
- Prioridade máxima em atendimento
- Cobertura nacional

12.2.3 Cloud Access & Network Security

FUNÇÃO: Proteção avançada para ambientes híbridos

CARACTERÍSTICAS:

- Inspeção SSL/TLS de tráfego criptografado
- Controle de aplicações em nuvem (SaaS)
- Proteção contra ameaças web avançadas
- Sandboxing de arquivos suspeitos
- Integração com threat intelligence

12.2.4 Management Center

FUNÇÃO: Console centralizado de gerenciamento

CARACTERÍSTICAS:

- Interface web unificada para administração
- Geração automática de relatórios de conformidade
- Configuração centralizada de políticas
- Monitoramento em tempo real
- Dashboard executivo com métricas

12.3 Arquitetura de Implementação

TOPOLOGIA ATUAL (MANTIDA):

INTEGRAÇÕES EXISTENTES (PRESERVADAS):

- Active Directory para autenticação de usuários
- SIEM/Log Management para auditoria
- DNS interno para resolução de nomes
- Backup automatizado de configurações

12.4 Especificações Técnicas da Solução

CAPACIDADES MANTIDAS:

- Throughput: 2 Gbps (firewall) / 1 Gbps (IPS)
- Conexões simultâneas: 250.000 sessões
- Usuários suportados: 2.000 concorrentes
- Políticas de segurança: Ilimitadas
- VPNs Site-to-Site: 100 túneis

FUNCIONALIDADES ATIVAS:

- Application Control com DPI (Deep Packet Inspection)
- Web Filtering por categorias e URLs
- Anti-malware com multiple engines
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP) básico

13. Estimativa de custo total da contratação

Valor (R\$): 46.034,95

A média dos orçamentos é de R\$ 46.034,95 (quarenta e sei mil, trinta e quatro reais e noventa e cinco centavos)

ISH - R\$ 44.680,00 (quarenta e quatro mil, seiscentos e oitenta mil reais)

Active - R\$ 83.558,34 R\$ 27.852,78 (vinte e sete mil oitocentos e cinquenta e dois reais e setenta e oito centavos)/ ano - Este valor foi descartado

Alus - R\$ 47.389,91 (quarenta e sete mil trezentos e oitenta e nove reais e noventa e um centavos)

14. Justificativa técnica da escolha da solução

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

14.1 Fundamentação Técnica Principal

A **renovação das licenças do Forcepoint NGFW 1105** foi escolhida como solução optimal baseada em **critérios técnicos objetivos** que demonstram sua **superioridade** em relação às alternativas avaliadas.

14.2 Critérios Técnicos Decisórios

14.2.1 Continuidade Operacional

VANTAGEM TÉCNICA: Manutenção integral da infraestrutura operacional

JUSTIFICATIVA:

- Zero downtime durante implementação

- Preservação de 3+ anos de configurações refinadas
- Manutenção de integrações existentes com Active Directory e SIEM
- Continuidade de políticas de segurança validadas

14.2.2 Competência Técnica Consolidada

VANTAGEM TÉCNICA: Aproveitamento da expertise técnica existente
JUSTIFICATIVA:

- Equipe técnica certificada e experiente na plataforma
- Procedimentos operacionais documentados e testados
- Conhecimento profundo das funcionalidades específicas
- Redução de curva de aprendizado para zero

14.2.3 Adequação Técnica às Necessidades

VANTAGEM TÉCNICA: Atendimento perfeito aos requisitos identificados
JUSTIFICATIVA:

- Capacidade atual (250k sessões) superior à demanda (estimada em 50k)
- Funcionalidades NGFW adequadas ao perfil de ameaças enfrentadas
- Performance verificada e validada em 3+ anos de operação
- Compatibilidade com arquitetura de rede existente

14.2.4 Maturidade da Solução

VANTAGEM TÉCNICA: Solução técnica madura e estável
JUSTIFICATIVA:

- Forcepoint é líder reconhecido em segurança perimetral
- NGFW 1105 é modelo consolidado no mercado empresarial
- Base instalada significativa com casos de sucesso documentados
- Roadmap de suporte definido pelo fabricante até 2028

14.3 Análise de Riscos Técnicos

14.3.1 Riscos da Solução Escolhida (BAIXOS)

- **End of Life do equipamento:** MITIGADO por suporte contratual até 2028
- **Limitação de crescimento:** MITIGADO por capacidade atual excedente
- **Dependência de fornecedor:** ACEITÁVEL dado o padrão de mercado

14.3.2 Riscos das Soluções Alternativas (ALTOS)

- **Substituição de equipamento:** Risco de falha na migração e indisponibilidade
- **Solução cloud:** Dependência crítica de conectividade externa
- **Sem licenças:** Risco inaceitável de exposição a vulnerabilidades

14.4 Superioridade Técnica Demonstrada

Aspecto Técnico	Renovação	Substituição	Cloud	Sem Licenças
Tempo de Implementação	Imediato	60-90 dias	90-120 dias	Imediato
Risco de Indisponibilidade	Zero	Alto	Médio	Crítico
Preservação de Investimentos	100%	0%	0%	60%
Adequação aos Requisitos	100%	95%	70%	20%
Maturidade Técnica	Alta	Alta	Média	Baixa

15. Justificativa econômica da escolha da solução

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.1 Análise Econômica Comparativa

A escolha da **renovação de licenças** se fundamenta em **vantagens econômicas substanciais** que demonstram **economicidade superior** em relação a todas as alternativas avaliadas.

15.2 Economicidade Demonstrada

15.2.1 Economia Absoluta

RENOVAÇÃO vs SUBSTITUIÇÃO:

- Renovação: R\$ 30.784,20
- Substituição: R\$ 190.000,00
- ECONOMIA: R\$ 150.000,00 (78,9%)**

RENOVAÇÃO vs CLOUD:

- Renovação: R\$ 30.784,20
- Cloud: R\$ 183.000,00
- ECONOMIA: R\$ 143.000,00 (78,1%)**

15.2.2 Retorno sobre Investimento (ROI)

CÁLCULO DO ROI:

$ROI = (Economia\ Obtida - Investimento) / Investimento \times 100$ $ROI = (150.000 - R\$ 30.784,20) / R\$ 30.784,2$

RESULTADO: ROI de 387, 26% no período de 36 meses

15.2.3 Payback da Decisão

PERÍODO DE RETORNO: Imediato

JUSTIFICATIVA: Economia realizada no momento da contratação comparada às alternativas

15.3 Análise de Custo-Benefício

Benefício	Valor Econômico	Metodologia
Economia em aquisição	R\$ 120.000,00	Evita compra de novo equipamento
Economia em implementação	R\$ 15.000,00	Evita custos de migração
Economia em treinamento	R\$ 8.000,00	Aproveita capacitação existente
Economia em downtime	R\$ 50.000,00	Evita perda de produtividade
BENEFÍCIO TOTAL	R\$ 193.000,00	Benefícios quantificáveis
INVESTIMENTO	387, 26%	Custo da renovação
BENEFÍCIO LÍQUIDO	R\$ 153.000,00	Benefício - Investimento

15.4 Análise de Sensibilidade Econômica

15.4.1 Cenário Conservador

- Renovação: R\$ 45.000,00 (+12,5%)
- Economia vs Substituição: R\$ 145.000,00
- ROI: 222%** (ainda altamente vantajoso)

15.4.2 Cenário Pessimista

- Renovação: R\$ 46.034,95
- Economia vs Substituição: R\$ 140.000,00
- **ROI: 180%** (mantém atratividade)

15.4.3 Conclusão da Sensibilidade

Mesmo com **variações de até 25% no custo**, a solução mantém **superioridade econômica inquestionável**.

15.5 Custo de Oportunidade

15.5.1 Recursos Liberados para Outros Investimentos

VALOR: R\$ 150.000,00 (economia obtida)

APLICAÇÃO ALTERNATIVA: Modernização de outras áreas de TI

BENEFÍCIO ADICIONAL: Multiplicação do valor através de novos investimentos

15.5.2 Preservação de Valor dos Ativos

ATIVO PRESERVADO: Firewall Forcepoint NGFW 1105

VALOR RESIDUAL: R\$ 80.000,00 (valor contábil atual)

PRESERVAÇÃO: 100% do valor residual mantido

15.6 Análise de Risco Econômico

15.6.1 Riscos Financeiros da Solução Escolhida

- **Risco de obsolescência:** BAIXO (suporte garantido até 2028)
- **Risco de aumento de custos:** BAIXO (contrato de preço fixo)
- **Risco de não entrega:** BAIXO (fornecedores estabelecidos)
-

15.6.2 Riscos Financeiros das Alternativas

- **Substituição:** ALTO (estouro orçamentário de 375%)
- **Cloud:** ALTO (custos recorrentes crescentes)
- **Sem licenças:** CRÍTICO (custos de incidentes imprevisíveis)

15.7 Conclusão da Justificativa Econômica

A **renovação das licenças** representa a **escolha economicamente optimal** por:

1. **ECONOMICIDADE MÁXIMA:** 78% de economia versus alternativas
2. **ROI EXCEPCIONAL:** 275% de retorno sobre investimento
3. **PRESERVAÇÃO DE VALOR:** 100% dos ativos existentes mantidos
4. **LIBERAÇÃO DE RECURSOS:** R\$ 150.000+ para outros investimentos
5. **RISCO FINANCEIRO MÍNIMO:** Exposição controlada e previsível

A **decisão está PLENAMENTE JUSTIFICADA** sob todos os aspectos econômico-financeiros analisados, representando a **melhor aplicação dos recursos públicos** disponíveis.

16. Benefícios a serem alcançados com a contratação

1. BENEFÍCIOS PARA O ÓRGÃO CONTRATANTE (IFSP CAPIVARI)

1.1 Benefícios Operacionais

1.1.1 Continuidade dos Serviços Críticos

RESULTADO ESPERADO: Manutenção de 99,5%+ de disponibilidade dos sistemas institucionais **INDICADOR:** Uptime mensal dos sistemas críticos (SUAP, e-mail, bibliotecas digitais) **BENEFÍCIO:** Eliminação de interrupções não programadas por falhas de segurança

1.1.2 Otimização da Gestão de TI

RESULTADO ESPERADO: Redução de 60% no tempo gasto com incidentes de segurança **INDICADOR:** Horas/mês dedicadas à resolução de problemas de segurança **BENEFÍCIO:** Liberação da equipe técnica para projetos estratégicos

1.1.3 Eficiência Administrativa

RESULTADO ESPERADO: Automatização de 90% das atualizações de segurança **INDICADOR:** Percentual de patches aplicados automaticamente **BENEFÍCIO:** Redução da carga operacional manual da equipe

1.2 Benefícios Estratégicos

1.2.1 Conformidade Regulatória Garantida

RESULTADO ESPERADO: 100% de conformidade com normativos de segurança **INDICADOR:** Zero não conformidades identificadas em auditorias **BENEFÍCIO:** Eliminação de riscos de sanções e questionamentos de órgãos de controle

1.2.2 Preservação da Reputação Institucional

RESULTADO ESPERADO: Zero incidentes de segurança com repercussão pública **INDICADOR:** Ausência de notícias negativas sobre segurança cibernética **BENEFÍCIO:** Manutenção da credibilidade junto à comunidade e parceiros

1.2.3 Alinhamento com Políticas Públicas

RESULTADO ESPERADO: Adequação integral à Estratégia Nacional de Segurança Cibernética **INDICADOR:** Cumprimento de 100% dos requisitos da PNSI **BENEFÍCIO:** Demonstração de compromisso com diretrizes governamentais

1.3 Benefícios Econômico-Financeiros

1.3.1 Otimização de Recursos Públicos

RESULTADO ESPERADO: Economia de R\$ 150.000,00 versus substituição de equipamento **INDICADOR:** Comparativo de custos entre renovação e aquisição **BENEFÍCIO:** Liberação de recursos para investimentos em outras áreas prioritárias

1.3.2 Maximização do ROI

RESULTADO ESPERADO: Retorno de 275% sobre o investimento em 36 meses **INDICADOR:** $(\text{Economia obtida} - \text{Investimento}) / \text{Investimento} \times 100$ **BENEFÍCIO:** Demonstração de gestão eficiente dos recursos públicos

1.3.3 Prevenção de Custos com Incidentes

RESULTADO ESPERADO: Evitar custos estimados de R\$ 200.000+ com possíveis incidentes **INDICADOR:** Redução de 95% na probabilidade de incidentes críticos **BENEFÍCIO:** Proteção do patrimônio público e continuidade operacional

2. BENEFÍCIOS PARA A COMUNIDADE ACADÊMICA (PÚBLICO-ALVO DIRETO)

2.1 Benefícios para Estudantes

2.1.1 Ambiente Digital Seguro para Aprendizagem

RESULTADO ESPERADO: 800+ estudantes com acesso seguro garantido a recursos educacionais **INDICADOR:** Número de usuários ativos protegidos pelo firewall **BENEFÍCIO:** Concentração no aprendizado sem preocupações com segurança digital

2.1.2 Acesso Contínuo a Recursos Acadêmicos

RESULTADO ESPERADO: 99,5%+ de disponibilidade de bibliotecas digitais e portais educacionais **INDICADOR:** Tempo de acesso disponível vs. tempo total **BENEFÍCIO:** Eliminação de interrupções no processo de pesquisa e estudo

2.1.3 Proteção de Dados Pessoais

RESULTADO ESPERADO: 100% de conformidade com LGPD na proteção de dados estudantis **INDICADOR:** Zero vazamentos ou exposições de dados pessoais **BENEFÍCIO:** Tranquilidade quanto à privacidade e segurança das informações pessoais

2.2 Benefícios para Servidores (Docentes e Técnico-Administrativos)

2.2.1 Produtividade Preservada

RESULTADO ESPERADO: Redução de 80% nas interrupções de trabalho por problemas de TI **INDICADOR:** Número de horas perdidas por indisponibilidade de sistemas **BENEFÍCIO:** Foco integral nas atividades de ensino, pesquisa e gestão

2.2.2 Proteção de Propriedade Intelectual

RESULTADO ESPERADO: Segurança total para pesquisas e trabalhos acadêmicos em desenvolvimento **INDICADOR:** Zero incidentes de acesso não autorizado a dados de pesquisa **BENEFÍCIO:** Tranquilidade para desenvolvimento de pesquisas sensíveis e inovadoras

2.2.3 Facilidade de Acesso Remoto Seguro

RESULTADO ESPERADO: 100% dos acessos remotos protegidos por políticas atualizadas **INDICADOR:** Percentual de conexões VPN seguras estabelecidas **BENEFÍCIO:** Flexibilidade para trabalho remoto sem comprometer a segurança

2.3 Benefícios para Terceirizados e Visitantes

2.3.1 Acesso Controlado e Seguro

RESULTADO ESPERADO: 100% dos acessos de terceiros monitorados e controlados **INDICADOR:** Efetividade das políticas de acesso para usuários externos **BENEFÍCIO:** Ambiente digital confiável para prestadores de serviços e parceiros

3. BENEFÍCIOS PARA A SOCIEDADE

3.1 Benefícios Educacionais Amplos

3.1.1 Formação Profissional Qualificada Garantida

RESULTADO ESPERADO: Graduação anual de 200+ profissionais técnicos sem interrupções **INDICADOR:** Taxa de conclusão de cursos mantida em 95%+ **BENEFÍCIO:** Disponibilização contínua de mão de obra qualificada para o mercado

3.1.2 Pesquisa e Extensão Protegidas

RESULTADO ESPERADO: 50+ projetos de pesquisa/extensão anuais executados com segurança **INDICADOR:** Número de projetos desenvolvidos sem comprometimento por questões de TI **BENEFÍCIO:** Contribuição científica e social preservada para desenvolvimento regional

3.1.3 Democratização do Acesso ao Conhecimento

RESULTADO ESPERADO: Disponibilização segura de recursos educacionais à comunidade externa **INDICADOR:** Número de acessos externos aos repositórios institucionais **BENEFÍCIO:** Ampliação do alcance social da educação pública federal

3.2 Benefícios Econômicos Regionais

3.2.1 Atração de Investimentos Tecnológicos

RESULTADO ESPERADO: Demonstração de maturidade em segurança cibernética regional **INDICADOR:** Reconhecimento como referência em segurança educacional **BENEFÍCIO:** Estímulo ao desenvolvimento de ecossistema tecnológico local

3.2.2 Modelo de Boas Práticas

RESULTADO ESPERADO: Referência em gestão de segurança para outras instituições públicas **INDICADOR:** Número de consultas/benchmarking solicitados por outras entidades **BENEFÍCIO:** Elevação do padrão de segurança cibernética no setor público

3.3 Benefícios de Segurança Nacional

3.3.1 Fortalecimento da Cibersegurança Nacional

RESULTADO ESPERADO: Contribuição para resiliência da infraestrutura crítica educacional **INDICADOR:** Alinhamento com diretrizes do GSIPR e CGL.br **BENEFÍCIO:** Redução da superfície de ataque nacional em setores estratégicos

3.3.2 Proteção de Dados Estratégicos

RESULTADO ESPERADO: Segurança de dados de formação de recursos humanos especializados **INDICADOR:** Zero comprometimentos de dados estratégicos nacionais **BENEFÍCIO:** Preservação de informações relevantes para competitividade nacional

4. BENEFÍCIOS PARA PARCEIROS E STAKEHOLDERS

4.1 Benefícios para Outras Unidades do IFSP

4.1.1 Conectividade Segura Interunidades

RESULTADO ESPERADO: 100% das conexões com outras unidades protegidas adequadamente **INDICADOR:** Integridade das comunicações inter-campi **BENEFÍCIO:** Fortalecimento da rede colaborativa institucional

4.1.2 Compartilhamento Seguro de Recursos

RESULTADO ESPERADO: Disponibilização protegida de sistemas e recursos compartilhados **INDICADOR:** Efetividade das políticas de acesso federado **BENEFÍCIO:** Otimização de recursos através de compartilhamento seguro

4.2 Benefícios para Parceiros Externos

4.2.1 Confiança em Colaborações

RESULTADO ESPERADO: Manutenção de 100% das parcerias existentes sem preocupações de segurança **INDICADOR:** Renovação de convênios e contratos de parceria **BENEFÍCIO:** Fortalecimento de relacionamentos institucionais

4.2.2 Intercâmbio Acadêmico Seguro

RESULTADO ESPERADO: Facilitação de programas de intercâmbio e cooperação internacional **INDICADOR:** Número de programas internacionais mantidos/ampliados **BENEFÍCIO:** Expansão das oportunidades de cooperação acadêmica

4.3 Benefícios para Órgãos de Controle

4.3.1 Transparência e Auditabilidade

RESULTADO ESPERADO: 100% de rastreabilidade das ações de segurança implementadas **INDICADOR:** Completude dos logs e relatórios de auditoria **BENEFÍCIO:** Facilitação de processos de fiscalização e controle

4.3.2 Demonstração de Conformidade

RESULTADO ESPERADO: Evidências objetivas de adequação aos normativos **INDICADOR:** Relatórios de compliance atualizados mensalmente **BENEFÍCIO:** Redução de questionamentos e necessidade de esclarecimentos

5. CONSOLIDAÇÃO DOS BENEFÍCIOS

5.1 Benefícios Quantificados

Categoria	Benefício Mensurado	Valor/Meta
Econômico	Economia vs. substituição	R\$ 150.000,00
Operacional	Disponibilidade dos sistemas	99,5%+
Social	Usuários protegidos	800+ pessoas
Acadêmico	Projetos seguros	50+ projetos/ano
Institucional	Conformidade regulatória	100%

5.2 Benefícios Estratégicos de Longo Prazo

SUSTENTABILIDADE INSTITUCIONAL: Base sólida para crescimento futuro com segurança adequada

COMPETITIVIDADE EDUCACIONAL: Manutenção de padrões tecnológicos compatíveis com instituições de excelência

RESPONSABILIDADE SOCIAL: Cumprimento integral do papel de instituição pública federal

INOVAÇÃO SEGURA: Ambiente propício para desenvolvimento de pesquisas e projetos inovadores

6. CONCLUSÃO DOS BENEFÍCIOS

A contratação da renovação das licenças do firewall **MAXIMIZA O VALOR PÚBLICO** através de benefícios **MÚLTIPLOS, MENSURÁVEIS E SUSTENTÁVEIS** que:

PROTEGEM 800+ membros da comunidade acadêmica

PRESERVAM a continuidade da missão educacional

OTIMIZAM R\$ 150.000,00 em recursos públicos

GARANTEM conformidade regulatória integral

FORTALECEM a segurança cibernética nacional

AMPLIAM o impacto social da educação pública

Os benefícios identificados justificam plenamente o investimento proposto, demonstrando que a contratação representa **EXCELENTE APLICAÇÃO DOS RECURSOS PÚBLICOS** com **RETORNO MÚLTIPLO PARA A SOCIEDADE**.

17. Providências a serem Adotadas

1. Providências Administrativas

1.1. Lançar a licitação antes de 15/06/2025.

2. Providências Técnicas

2.1. Preparação da Infraestrutura

- 2.1.1. Verificação das configurações atuais do firewall Forcepoint NGFW 1105
- 2.1.2. Backup completo das políticas de segurança e configurações existentes
- 2.1.3. Documentação detalhada da arquitetura de rede atual
- 2.1.4. Teste de conectividade e funcionalidades antes da renovação

2.2. Coordenação com Fornecedores

- 2.2.1. Contato prévio com partners autorizados Forcepoint para validação de disponibilidade
- 2.2.2. Confirmação de compatibilidade das licenças com o equipamento existente
- 2.2.3. Definição de cronograma de ativação para evitar interrupções

2.3. Capacitação da Equipe

- 2.3.1. Atualização da equipe técnica sobre novos recursos das licenças
- 2.3.2. Treinamento em procedimentos de abertura de chamados técnicos
- 2.3.3. Revisão dos procedimentos operacionais padrão

3. PROVIDÊNCIAS ORÇAMENTÁRIAS

3.1. Recursos Financeiros

- 3.1.1. Confirmação da disponibilidade orçamentária no exercício de 2025
- 3.1.2. Empenho da despesa após homologação da licitação
- 3.1.3. Previsão orçamentária para exercícios futuros (2026-2027)

3.2. Dotação Específica

- 3.2.1. Identificação da dotação orçamentária apropriada para licenças de software

- 3.2.2. Verificação de saldo disponível na dotação específica
- 3.2.3. Solicitação de remanejamento orçamentário (se necessário)

4. PROVIDÊNCIAS OPERACIONAIS

4.1. Continuidade dos Serviços

- 4.1.1. Elaboração de plano de contingência para período de transição
- 4.1.2. Definição de janela de manutenção para ativação das licenças
- 4.1.3. Comunicação prévia aos usuários sobre possíveis interrupções mínimas

4.2. Monitoramento e Controle

- 4.2.1. Estabelecimento de indicadores de desempenho para acompanhamento
- 4.2.2. Definição de rotinas de verificação do status das licenças
- 4.2.3. Implementação de alertas automáticos para vencimentos futuros

5. PROVIDÊNCIAS DE SEGURANÇA

5.1. Proteção da Informação

- 5.1.1. Revisão da Política de Segurança da Informação relacionada ao firewall
- 5.1.2. Atualização dos procedimentos de backup de configurações
- 5.1.3. Implementação de logs detalhados para auditoria

5.2. Conformidade Regulatória

- 5.2.1. Verificação de atendimento às normas da LGPD
- 5.2.2. Conformidade com o Decreto nº 9.637/2018 (PNSI)
- 5.2.3. Alinhamento com as diretrizes do PDTIC 2024-2028

6. PROVIDÊNCIAS DE TRANSIÇÃO E FUTURO

6.1. Planejamento de Médio Prazo

- 6.1.1. Elaboração de cronograma para eventual substituição do equipamento EoL
- 6.1.2. Estudos de viabilidade para migração tecnológica (2027-2028)
- 6.1.3. Planejamento orçamentário para futura modernização da infraestrutura

6.2. Gestão do Conhecimento

- 6.2.1. Documentação de lições aprendidas no processo de renovação
- 6.2.2. Criação de procedimentos padronizados para futuras renovações
- 6.2.3. Manutenção de histórico técnico e administrativo da contratação

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A equipe de planejamento considera viável a contratação nestes termos.

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: De acordo com o ETP.

EDUARDO CAMARGO MAIA

Agente de contratação



Assinou eletronicamente em 17/09/2025 às 17:11:22.

Despacho: De acordo com o ETP.

CESAR EDUARDO ARMELIN

Coordenador de Licitações e Contratos



Assinou eletronicamente em 22/09/2025 às 10:09:28.

Despacho: De acordo com o ETP.

JUNIO RODRIGUES DE OLIVEIRA

Coordenador de Tecnologia da Informação



Assinou eletronicamente em 22/09/2025 às 10:30:14.

Despacho: De acordo com o ETP.

LUCIANA MARTINS GATTI

Diretoria Adjunta de Administração



Assinou eletronicamente em 22/09/2025 às 10:36:55.

Despacho: De acordo com o ETP.

CARLOS ROBERTO PAVIOTTI

Diretor Geral



Assinou eletronicamente em 22/09/2025 às 13:20:58.