

UFRS-UNIVERSIDADE FEDERAL DO RS/RS

Estudo Técnico Preliminar 150/2025

1. Informações Básicas

Número do processo: 23078.528115/2025-22

2. Descrição da necessidade

O presente estudo técnico tem por objetivo identificar e analisar cenários para a renovação do licenciamento da solução de firewall de próxima geração (*Next-Generation Firewall* – NGFW) em produção na infraestrutura de Tecnologia da Informação e Comunicação (TIC) da Universidade Federal do Rio Grande do Sul (UFRGS), bem como na aquisição de solução de NGFW para a composição de um cenário de Alta Disponibilidade (*High Availability* – HA).

2.1. Contextualização e Continuidade Operacional:

A infraestrutura de rede da UFRGS sustenta diversos serviços essenciais e sistemas estratégicos necessários ao funcionamento diário das atividades de ensino, pesquisa, extensão e administração. A indisponibilidade do acesso à internet ou o comprometimento do perímetro de segurança resultaria na paralisação das operações da Universidade. Dessa forma, a implementação de uma arquitetura de Alta Disponibilidade mediante a aquisição de um equipamento de *firewall* (FG-1801F) é imperativa para eliminar ponto único de falha. Em caso de falha física ou manutenção do equipamento principal, o equipamento secundário assume o tráfego instantaneamente, garantindo a continuidade ininterrupta dos serviços.

2.2. Mitigação de Riscos e Proteção de Dados (LGPD)

O ambiente cibernético atual exige controles de segurança dinâmicos e proativos. A renovação do licenciamento do NGFW (*Enterprise Protection*) garante o funcionamento de mecanismos avançados de defesa, tais como o Sistema de Prevenção de Intrusões (IPS), a prevenção de *malware* baseada em inteligência artificial em tempo real, o controle de aplicações corporativas e a Prevenção contra a Perda de Dados (DLP). A manutenção ininterrupta destas assinaturas de segurança é uma medida técnica de salvaguarda indispensável para mitigar o risco de invasões e vazamentos, assegurando a conformidade da universidade à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD).

2.3. Rastreabilidade e Gestão de Incidentes

De forma complementar à proteção de borda, a renovação do licenciamento da plataforma de gestão de *logs* (FortiAnalyzer), garantindo a ingestão de 100 GB/dia e armazenamento sem limitações, atende à necessidade de prover visibilidade centralizada. Esse componente é fundamental para subsidiar as atividades de auditoria técnica e apoiar as rotinas de detecção e resposta a incidentes cibernéticos, permitindo a investigação forense retroativa e a identificação precisa de anomalias na rede.

2.4. Alinhamento Estratégico e Normativo

A contratação da solução integrada de NGFW (hardware, licenciamento e serviços de implementação) encontra-se alinhada aos objetivos estratégicos definidos no Plano Diretor de Tecnologia da

Informação e Comunicação (PDTIC) da UFRGS. Ademais, a presente necessidade observa os princípios de segurança (confidencialidade, integridade, disponibilidade e autenticidade) estabelecidos na Política de Segurança da Informação (PSI) interna e nas diretrizes de melhores práticas como a ISO /IEC 27001 e o *NIST Cybersecurity Framework*. Por fim, atende ao art. 18, inciso I, da Lei nº 14.133 /2021 e à Instrução Normativa SGD/ME nº 94/2022, assegurando a proteção contínua dos ativos e informações sob a custódia do Estado.

2.5. Modelo de Prestação do Serviço e Avaliação de Deslocamento

Em cumprimento ao disposto no § 4º do art. 40 da Lei nº 14.133/2021, que determina a avaliação sobre a necessidade de deslocamento de técnico ou disponibilização de unidade física de prestação de serviços, define-se que, para a presente contratação, não será exigida a disponibilização de unidade física de prestação de serviços (filial ou escritório) localizada em distância específica ou no município sede da universidade.

No entanto, dadas as características de hardware da solução e a criticidade do ambiente de rede, é obrigatório o deslocamento de técnico(s) especializado(s) da Contratada para realizar a instalação física de equipamentos no *Datacenter* da instituição. Ficará a encargo exclusivo da Contratada — tanto na implantação inicial quanto nas substituições decorrentes de acionamento de garantia ou falha de hardware (RMA) — o envio de profissionais e o custeio de todas as despesas de deslocamento para as atividades de desinstalação do equipamento defeituoso, fixação em rack, organização de cabeamento, energização e ativação física do *appliance* de NGFW.

Uma vez concluída a etapa de instalação física presencial, os serviços subsequentes de configuração lógica, integração, atualização de *firmware* e o suporte técnico continuado poderão ser prestados de forma remota, garantindo a agilidade e a eficiência operacional requeridas para a gestão da segurança da informação.

Por fim, a aquisição da solução de NGFW e licenças associadas configura-se como requisito essencial para o fortalecimento da segurança cibernética, a redução de riscos institucionais e a garantia da continuidade dos serviços de TIC, assegurando a proteção das atividades de ensino, pesquisa, extensão e gestão administrativa da Universidade.

3. Área requisitante

Área Requisitante	Responsável
Departamento de Segurança da Informação - DSINF/CPD	Arthur Boos Jr

4. Necessidades de Negócio

A UFRGS atua como um polo crítico de ensino, pesquisa e extensão. Suas operações e a prestação de serviços essenciais à sociedade dependem da alta disponibilidade (*High Availability* - HA), integridade e confidencialidade da infraestrutura de TIC. Diante do complexo cenário de ameaças cibernéticas, a proteção do perímetro de rede e a gestão unificada de ameaças ultrapassam a condição de mero requisito operacional e assumem a posição de pilar estratégico de governança institucional.

Nesse contexto, a necessidade de contratação de uma solução de NGFW e a renovação do parque de segurança em produção visam viabilizar o crescimento tecnológico, com segurança e capacidade de auditoria. As necessidades de negócio motivadoras deste ETP possuem fundamentação no

fortalecimento da infraestrutura de segurança e desdobram-se no seguinte objetivo macro e seus respectivos requisitos:

4.1. Garantia de Continuidade Operacional e Alta Disponibilidade (HA)

A infraestrutura tecnológica da Universidade sustenta o acesso a sistemas acadêmicos, financeiros e administrativos vitais para o funcionamento da instituição. O negócio exige a eliminação de pontos únicos de falha (*Single Point of Failure* - SPOF) na borda da rede. A aquisição de um novo *appliance* FortiGate FG-1801F (Item 1) permite a composição de um *cluster* em Alta Disponibilidade (HA) com o equipamento de mesmo modelo já em operação. Essa arquitetura garante que, em caso de falha física ou necessidade de manutenção em um dos *appliances*, o tráfego seja assumido instantaneamente pelo outro, assegurando operações ininterruptas.

4.2. Mitigar Riscos e Ameaças Cibernéticas

Reduzir o risco de ataques cibernéticos, como *ransomware*, invasões, roubo e sequestro de dados e ataques de negação de serviço (DDoS), com potencial crítico de paralisar as operações acadêmicas e administrativas.

4.3. Garantir a Continuidade dos Serviços

Assegurar a estabilidade e a disponibilidade contínua da rede e dos sistemas críticos, dada a essencialidade dos serviços prestados e a alta dependência da comunidade acadêmica em relação aos recursos de TIC.

4.4. Cumprir Exigências Regulatórias

Alcançar a conformidade com a legislação vigente e com as políticas de governança, com destaque para a LGPD, a Política de Segurança da Informação (PSI) e as diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

4.5. Proteger Dados e Ativos Críticos

Assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações digitais geradas pelas atividades de ensino, pesquisa e extensão, bem como o resguardo dos dados pessoais sob custódia, classificados como ativos críticos da UFRGS.

4.6. Prevenir Uso Indevido de Infraestrutura

Impedir o uso de recursos tecnológicos e de rede, como *links* de internet, para fins ilícitos, como o *download* de conteúdos protegidos por direitos autorais ou a participação em ataques DDoS.

5. Necessidades Tecnológicas

Para dar resposta aos requisitos de negócio, à continuidade dos serviços essenciais e à proteção do perímetro de rede da Universidade, a solução tecnológica a contratar deverá contemplar as seguintes capacidades e componentes:

5.1. Arquitetura de Resiliência e Processamento (Hardware e HA)

Para garantir a resiliência da infraestrutura de rede e evitar a interrupção de serviços, é tecnologicamente imperativa a expansão da capacidade de processamento através da aquisição de 1 (um) *appliance* físico FortiGate FG-1801F (Item 1).

- **Alta Disponibilidade:** Este equipamento operará em conjunto com o *appliance* idêntico já existente na instituição, formando um *cluster* de Alta Disponibilidade.
- **Padronização Tecnológica:** A indicação do modelo exato é uma necessidade técnica estrita para garantir a compatibilidade de *hardware* e *firmware* exigida para o funcionamento do *cluster* HA ativo-passivo ou ativo-ativo, garantindo a sincronização de sessões e o *failover* imediato sem perda de pacotes.

5.2. Inspeção Profunda e Defesa Ativa de Perímetro (Licenciamento NGFW)

O tráfego de rede atual (que inclui túneis encriptados e tráfego aplicativo complexo) não pode ser protegido por *firewalls* tradicionais baseados apenas em portas e protocolos. A topologia necessita da aquisição e renovação dos pacotes de licenciamento *Enterprise Protection* (Itens 3 e 4) por 60 meses para habilitar as seguintes tecnologias no *cluster*:

- Prevenção Baseada em Inteligência Artificial: Capacidade de *AI-based Inline Malware Prevention* e *Advanced Malware Protection* para bloquear ameaças de dia zero (*zero-day*) em tempo real.
- Controle Granular e Proteção de Dados: Ativação de *App Control* (para gerir o uso de aplicações não homologadas), *Inline CASB Database* e DLP (*Data Loss Prevention*), controles tecnológicos essenciais para mitigar fugas de dados e assegurar o cumprimento das exigências de privacidade.
- Higiene da Superfície de Ataque: Funcionalidades de IPS (*Intrusion Prevention System*), filtro de URL/DNS/Vídeo e *Anti-spam*, garantindo o monitoramento e a filtragem proativa do tráfego que entra e sai da universidade.

5.3. Telemetria, Retenção de Logs e Correlação de Eventos

A arquitetura de segurança exige uma plataforma centralizada de telemetria que suporte as operações diárias da equipe de Tratamento e Resposta a Incidentes.

- Ingestão e Armazenamento: É necessária a renovação do licenciamento da máquina virtual FortiAnalyzer FAZ-VM-GB-100 (Item 5) já em produção, garantindo a capacidade técnica de ingestão de até 100 GB/dia de *logs*.
- Ecossistema Integrado: A integração nativa (*Security Fabric*) entre os *firewalls* (Itens 1, 3 e 4) e o FortiAnalyzer (Item 5) é uma exigência tecnológica para garantir que não existam estrangulamentos na exportação de *logs* e para permitir o armazenamento ilimitado das trilhas de auditoria durante os 60 meses do contrato, possibilitando a investigação forense retroativa.

5.4. Serviços de Implementação, Integração e Mitigação de Falhas

A inserção destes componentes numa rede de grande escala requer conhecimentos avançados de engenharia de redes e segurança cibernética.

- Implementação Especializada: É necessária a contratação de serviços profissionais de instalação, configuração e implementação (Item 2), abrangendo a instalação física no *datacenter* (montagem em *rack*, cabeamento), a configuração lógica (migração de regras, ativação do HA, afinação do IPS e integração com o FortiAnalyzer).
- Suporte e Garantia de Substituição: Para sustentar a operação a longo prazo, a infraestrutura requer um contrato unificado de manutenção e suporte 24 horas por dia, 7 dias por semana (Item 6), cobrindo todos os equipamentos e licenças por 60 meses. Face à importância da topologia de borda, é uma exigência tecnológica que qualquer falha de *hardware* seja suprimida pela substituição por modelo igual num prazo máximo de 1 (um) dia útil (*RMA*).

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

A presente contratação deverá estar em conformidade com as seguintes normativas e legislações (ou correspondentes em caso de atualização/substituição/revogação):

I. Plano de Desenvolvimento Institucional da UFRGS (PDI);

II. Política de Segurança da Informação (PSIUFRGS);

III. Política de Uso de Recursos de TI da UFRGS;

IV. Lei Federal nº 14.133/2021: estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

V. Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022: Dispõe sobre o processo de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP;

VI. Instrução Normativa SEGES /ME Nº 65, de 7 de julho de 2021: Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

VII. Decreto Nº 10.947, de 25 de janeiro de 2022: dispõe sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

6.1. Da adoção do Sistema de Registro de Preços - SRP

Quanto à adoção do SISTEMA DE REGISTRO DE PREÇOS, a Lei nº 14.133/2021, em seu inc. II do art. 40, estabelece que o planejamento de compras deverá considerar o “processamento por meio de sistema de registro de preços, quando pertinente ” - assim definido como o " conjunto de procedimentos para a realização, mediante contratação direta ou licitação nas modalidades pregão ou concorrência, de registro formal de preços relativos à prestação de serviços, às obras e à aquisição e à locação de bens para contratações futuras " (Decreto nº 11.462/2023, art. 2, I).

De acordo com o disposto no Decreto nº nº 11.462/2023, a utilização do Sistema de Registro de Preços enquadra-se nas seguintes hipóteses:

I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;

II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;

III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;

IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou

V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração

A adoção do SRP foi julgada como não pertinente para esta contratação, tendo em vista que se trata de contratação de natureza continuada com vistas a atender à necessidade pública de forma permanente e contínua.

6.2. Do Princípio da Padronização

A consulta realizada nos catálogos de soluções de TIC com condições padronizadas – endereço eletrônico Catálogos de Soluções de TIC — Governo Digital (www.gov.br) - não localizou item com compatibilidade de especificações estéticas, técnicas ou de desempenho em relação ao item constante na solução pretendida.

6.3. Da natureza comum do objeto

O objeto é de natureza comum para efeito de utilização da modalidade Pregão, na forma eletrônica. Neste sentido, a fim de confirmar que os objetos são comuns, observou-se o núcleo do conceito de bem e serviço: “disponibilidade no mercado próprio; predeterminação dos atributos essenciais do objeto de forma objetiva e uniforme e desnecessidade de constar características peculiares para satisfação da Administração”.

O presente objeto possui os seguintes atributos básicos:

- a) possuem especificações definidas objetivamente por meio de padrões usuais; e
- b) há possibilidade de julgamento objetivo das propostas pelo menor preço.

6.4. Enquadramento da contratação para fins de vigência

O objeto licitatório é enquadrado como de fornecimento contínuo, pois a entrega do bem e a prestação dos serviços de suporte técnico é uma necessidade da UFRGS para a manutenção das suas atividades administrativas e acadêmicas, decorrentes de necessidades permanentes ou prolongadas, devendo a contratação utilizar prazo de vigência plurianual, conforme os prazos e as hipóteses definidas em lei e mediante a assinatura de Contrato.

6.5. Do critério de julgamento

O objeto é caracterizado como comum e está definido em requisitos mínimos de desempenho, qualidade, segurança e suporte, permitindo comparação objetiva entre propostas. Portanto, o critério de julgamento pelo menor preço mostra-se o mais adequado, garantindo economicidade, isonomia e seleção da proposta mais vantajosa para a Administração.

7. Estimativa da demanda - quantidade de bens e serviços

Grupo	Item	CATMAT/ CATSER	Descrição	Unidade de Medida	Qtd.
1	1	609340	Equipamento FortiGate FG-1801F .	Unidade	01
	2	27111	Serviço de instalação, configuração e implementação do item 1.	Unidade	01
	3	27502	Contratação do licenciamento Enterprise Protection pelo período de 60 meses para firewall Fortigate FG-1801F, a ser acoplado ao item 1.	Unidade	01
	4	27502	Renovação do licenciamento Enterprise Protection pelo período de 60 meses para firewall Fortigate FG-1801F, a ser acoplado ao equipamento em produção. SN FG181FTK21901099 .	Unidade	01
	5	27502	Renovação do licenciamento FortiAnalyzer com 100 GB/dia de logs, com licenciamento por 60 meses, com capacidade de armazenamento ilimitada, a ser adquirido para equipamento em produção. SN FAZ-VMTM22000548 .	Unidade	01
	6	27740	Contrato de manutenção e suporte original da fabricante para os equipamentos mencionados nos itens 1, 3 e 4 desta contratação. A manutenção e o suporte deverão ser prestados na modalidade 24 horas por dia, 7 dias na semana, pelo período de 60 meses, com substituição por equipamento equivalente em, no máximo, um (1) dia útil.	Mês	60

A estimativa da demanda está amparada no atual cenário da Instituição, que com a aquisição de novo equipamento NGFW oportunizará a alta disponibilidade (HA), que é uma configuração que usa redundância (dois ou mais firewalls agrupados) para garantir que a proteção da rede continue ininterruptamente, mesmo se um dos equipamentos falhar.

7.1 Justificativa para o parcelamento ou não da solução

A adoção do critério de julgamento por grupo (lote único) para a presente contratação de equipamento firewall, licenças de software e serviços de suporte técnico justifica-se em razão da indissociabilidade técnica e funcional entre os itens que compõem o objeto. O pleno funcionamento da solução depende da integração integral entre o hardware, os módulos de licenciamento de segurança e o serviço de suporte especializado, sendo tecnicamente inviável ou antieconômico o seu fracionamento.

A contratação de fornecedores distintos para cada componente (equipamento, licenças e suporte) acarretaria riscos significativos à continuidade do serviço, tais como: incompatibilidades tecnológicas, responsabilização difusa em caso de falhas, dificuldades na atualização de firmwares, prejuízos à

segurança da informação e aumento do tempo de resposta a incidentes. Ademais, o suporte técnico exige conhecimento especializado e certificações vinculadas ao fabricante da solução, o que reforça a necessidade de contratação conjunta.

Sob o aspecto econômico e operacional, a contratação por grupo proporciona padronização da solução, redução de custos administrativos, agilidade na implantação, melhor governança contratual e mitigação de riscos operacionais, assegurando maior eficiência na gestão do serviço e maior nível de segurança à infraestrutura de rede institucional.

Assim, nos termos do art. 23, §1º, da Lei nº 14.133/2021, o julgamento por grupo se revela a forma mais vantajosa para a Administração, atendendo aos princípios da eficiência, segurança, economicidade e interesse público.

8. Levantamento de soluções

Com o objetivo de suprir as necessidades de negócio e tecnológicas descritas, foi realizado um levantamento mercadológico para identificar as alternativas viáveis capazes de prover proteção de perímetro, visibilidade centralizada de *logs* e Alta Disponibilidade para as operações vitais da universidade.

A análise considerou a existência prévia de um *appliance* FortiGate FG-1801F e de um *appliance* virtual FortiAnalyzer em produção no *datacenter* da instituição. A partir desta premissa, configuraram-se duas soluções de contratação:

8.1. Solução 1: Expansão em Alta Disponibilidade e Renovação do Ecossistema Atual (Adequação aos Requisitos)

Este cenário consiste na preservação dos investimentos já realizados pela Administração, promovendo a expansão e a atualização do parque tecnológico atual. Envolve a aquisição de apenas 1 (um) *appliance* FortiGate FG-1801F para compor o *cluster* HA com o equipamento existente, a renovação dos licenciamentos de segurança (*Enterprise Protection*) por 60 meses e a renovação da subscrição do FortiAnalyzer, acrescidos dos serviços especializados de configuração.

- Vantagens:
 - Continuidade e Estabilidade: A formação do *cluster* ativo-passivo ou ativo-ativo com equipamentos idênticos garante a transição transparente de tráfego (*failover*) em caso de falha física, assegurando o funcionamento ininterrupto da rede.
 - Integração Nativa (*Security Fabric*): A manutenção do ecossistema Fortinet garante que o *firewall* e o correlacionador de *logs* (FortiAnalyzer) comuniquem de forma transparente, otimizando a detecção de ameaças e o tempo de resposta a incidentes.
 - Eficiência Financeira (Menor TCO): Evita o custo de aquisição de um segundo equipamento redundante e maximiza o Retorno sobre o Investimento (ROI) dos ativos em produção. A curva de aprendizagem da equipe técnica é nula, pois a plataforma já é de domínio institucional.
- Desvantagens e Riscos:
 - Restrição de Marca: Exige a indicação da marca Fortinet (fundamentada no Art. 41, inciso I, da Lei nº 14.133/2021) para garantir a compatibilidade e a padronização, o que requer uma justificativa técnica robusta nos autos do processo (já contemplada neste ETP). O risco de sobrepreço é mitigado através de ampla pesquisa de mercado em múltiplos canais de revenda e no Painel de Preços.

8.2. Solução 2: Substituição Integral da Solução Atual (Migração de Fabricante)

Este cenário consiste na substituição completa do ecossistema de segurança atual. Para atingir a Alta Disponibilidade (HA) e a capacidade de retenção de *logs* exigida, a universidade precisaria adquirir: dois novos *appliances* físicos de NGFW de outro fabricante, um novo sistema de correlação de *logs* compatível e todos os serviços de implementação do zero.

- Vantagens: Ampla competitividade no certame licitatório para a escolha da nova plataforma, sem a necessidade de indicação de marca.
- Desvantagens e Riscos: Obriga o descarte precoce do *hardware* FortiGate FG-1801F e do FortiAnalyzer atualmente em funcionamento.
 - Elevado Risco Operacional: A migração completa de arquitetura de *firewall* exige a reescrita de milhares de políticas de segurança, regras de NAT e túneis VPN, o que aumenta exponencialmente o risco de indisponibilidade dos sistemas estratégicos durante a janela de transição.
 - Custos adicionais: Investimento necessário no treinamento da equipe técnica na nova console de administração e solução de gestão de *logs*.

Id	Descrição das soluções
1	Expansão em Alta Disponibilidade e Renovação do Ecossistema Atual (Adequação aos Requisitos)
2	Substituição Integral da Solução Atual e Expansão em Alta Disponibilidade (Migração de Fabricante)

9. Análise comparativa de soluções

A diversidade de fabricantes de *firewall* no ambiente de rede eleva injustificadamente os custos operacionais da instituição, exigindo a aquisição de múltiplos *softwares* de gerência proprietários e a contratação contínua de novos treinamentos. Em contrapartida, a padronização tecnológica permite o pleno aproveitamento do conhecimento analítico e operacional já consolidado pela equipe técnica, garantindo maior eficiência e celeridade na resposta a incidentes cibernéticos sem a necessidade de uma nova curva de aprendizado. Esse entendimento, que rechaça a multiplicidade em prol da segurança e da economicidade, encontra firme respaldo na jurisprudência do TCU (Acórdão nº 2789 /2019 – Plenário), que alerta expressamente que: *"A falta de padronização das tecnologias afeta o acúmulo de conhecimento e a disseminação de boas práticas, o que poderia reduzir as necessidades de capacitação de pessoal e tornar a troca de experiências e movimentação de pessoal mais eficiente. Além disso, diminui a possibilidade de o Estado tirar proveito do efeito escala como grande comprador de tecnologia, aumentando a pressão sobre os custos. Por fim, dificulta a interoperabilidade entre os ambientes, tornando-se um incentivo perverso à criação de silos de informação, o que tanto emperra a integração de dados para a prestação de serviços públicos eficientes, sem contar com o esforço adicional que impõe às áreas de TI para lidar com tais complexidades."*

Portanto, a análise de cenários privilegia a resiliência operacional e a mitigação de riscos associados a falhas de operação, com foco na garantia de continuidade dos serviços em um ambiente crítico.

9.1. Matriz de Comparação

Abaixo, apresenta-se o quadro comparativo resumindo os impactos de cada cenário:

--	--	--

Critério de Avaliação	Solução 1: Expansão em HA e Renovação	Solução 2: Substituição Integral (Migração de Fabricante)
Continuidade e Risco Operacional	Baixo Risco. A inserção de um equipamento idêntico para a formação do cluster HA ocorre de forma transparente, garantindo estabilidade e resiliência imediata.	Alto Risco. A reescrita completa das políticas de segurança, regras de NAT e integrações aumenta substancialmente a probabilidade de indisponibilidade de serviços durante a migração.
Integração Nativa de Segurança	Nativa. A comunicação entre o FortiGate e o FortiAnalyzer já está validada e homologada no ambiente de produção.	Complexa. Exigiria esforço adicional de engenharia para garantir que as novas soluções conversem adequadamente com o ecossistema remanescente da rede.
Curva de Aprendizado da Equipe	Nula. A equipe técnica e a equipe de resposta a incidentes (TRI) já dominam a arquitetura e as rotinas operacionais da solução.	Alta. Exigiria investimento financeiro e de tempo em capacitação técnica oficial para a operação da nova consola de administração.

9.2. Análise Técnica e Operacional

Do ponto de vista técnico, a adoção da **Solução 2** introduz um nível inaceitável de risco à operação da Universidade. A substituição do fabricante principal da borda da rede não se resume à simples troca de equipamento físico; envolve a transição de milhares de regras lógicas de segurança. Qualquer inconformidade durante esta transição pode resultar no isolamento da rede institucional, paralisando os sistemas estratégicos de ensino e administração.

Em contrapartida, a **Solução 1** assegura a estabilidade. Ao optar pela expansão com um segundo equipamento FortiGate FG-1801F, a instituição estabelece a desejada Alta Disponibilidade (HA), onde o sincronismo de estado e de sessões entre os *firewalls* garante que o tráfego não sofra interrupções em caso de falha de um dos nós. Adicionalmente, a manutenção do FortiAnalyzer assegura que o histórico de retenção de *logs* para fins de auditoria não seja fragmentado.

9.3. Levantamento de Portal de Compras

No Portal Compras.gov.br, foram identificadas contratações pactuadas nos últimos 12 meses envolvendo soluções de firewall de diversos fabricantes. A análise individual dos itens da Pesquisa de Preços nº 373-2025 demonstrou que, embora tratem de objetos da mesma natureza (soluções de NGFW), os modelos encontrados apresentam diferenças de capacidade, desempenho e arquitetura, variando entre equipamentos inferiores e superiores ao modelo atualmente em operação na UFRGS (FortiGate FG-1801F), conforme a relação abaixo.

Contratações Públicas - Pesquisa de Preços nº 373-2025

Órgão/Sigla	UASG	Pregão	CATMAT/ CATSER	Descrição	Marca/Modelo	Valor Unitário (R\$)

ANM	323102	90004/2025	27111	Serviços de Instalação de Equipamentos de TI (Computadores e Periféricos)		99.000,00
ANVISA	110792	90001/2025	27740	Serviços de Garantia de Equipamentos de TIC (60 meses)		4.400,00
ANM	323102	90004/2025	609340	Firewall – Appliance NGFW	Fortinet - FG 901G	990.000,00
MRE	240010	90001/2025	609340	Firewall – Appliance NGFW	Fortinet - FG 2601F	2.300.000,00
MS	250110	90164/2025	609340	Firewall – Appliance NGFW	Checkpoint – Quantum Force 9800	1.109.000,00
UFPR	153079	90002/2025	609340	Firewall – Appliance NGFW	Fortinet - FG 1800F	999.685,00

Nas contratações consultadas, não foram localizadas composições contendo os mesmos elementos de *hardware*, licenciamento e suporte requeridos nesta contratação. Dessa forma, os valores obtidos não permitem estabelecer comparação válida nem servem como referência para estimar o custo total da solução objeto deste ETP, conforme previsto no art. 6º, §3º, da IN SEGES/ME nº 65/2021.

Assim, embora a pesquisa tenha sido realizada e registrada, seus resultados não foram utilizados na composição da estimativa de custos por não representarem solução tecnicamente comparável ou equivalente ao objeto desta contratação. A estimativa de preços apresentada neste ETP baseia-se, portanto, exclusivamente em proposta formal de fornecedor especializado na solução Fortinet.

Requisitos		Solução 1	Solução 2
Negócio	Garantia de Continuidade Operacional e Alta Disponibilidade (HA): Eliminar pontos únicos de falha e garantir operações ininterruptas na rede.	Atende. A formação do <i>cluster</i> HA ativo-passivo ou ativo-ativo com o equipamento já existente ocorre de forma fluida, assegurando o <i>failover</i> imediato.	Não atende. A mudança completa de arquitetura acarreta um elevado risco de indisponibilidade dos serviços essenciais durante a janela de transição e reescrita de regras.
	Proteção Avançada contra Ameaças e Conformidade Regulatória (LGPD): Aplicação de controles	Atende	Atende

	proativos para proteção de dados pessoais e propriedade intelectual.		
Tecnológico	Telemetria, Retenção de Logs e Correlação de Eventos: Integração nativa de exportação de <i>logs</i> sem estrangulamentos.	Atende. A renovação da licença do FortiAnalyzer assegura a retenção ilimitada das trilhas de auditoria, preservando a visibilidade centralizada.	Atende parcialmente. Exigiria a aquisição e configuração de um novo sistema correlacionador, quebrando a continuidade do histórico de auditoria já armazenado.
	Arquitetura de Resiliência e Processamento: Necessidade técnica estrita de compatibilidade de <i>hardware</i> para formação de <i>cluster</i> HA.	Atende. Requer a aquisição de 1 (um) <i>appliance</i> FortiGate FG-1801F para expandir o parque tecnológico existente de forma padronizada.	Não atende. Obrigaria à aquisição de 2 (dois) <i>appliances</i> novos e ao descarte do FG-1801F atual.
Resultado da Análise		Atende	Não atende

10. Registro de soluções consideradas inviáveis

Durante a fase de levantamento de alternativas para atender à demanda da instituição, o estudo concentrou-se na avaliação de dois cenários principais. A **Solução 1 (Expansão em Alta Disponibilidade e Renovação do Ecossistema Atual)** atendeu plenamente aos requisitos tecnológicos, financeiros e operacionais, sendo classificada como viável e escolhida para a contratação. Por outro lado, a **Solução 2**, correspondente à troca completa de arquitetura, foi descartada em virtude do não atendimento a todos os requisitos da contratação.

11. Análise comparativa de custos (TCO)

Solução Viável 1 – Expansão em Alta Disponibilidade e Renovação do Ecossistema Atual (Adequação aos Requisitos)

Ano -->	1	2	3	4	5	Total Acumulado R\$
Item						
	506.050,33	0,0	0,0	0,0	0,0	506.050,33

Equipamento FortiGate FG-1801F (Hardware novo, de primeiro uso para composição de cluster HA).						
Serviço de Instalação, Configuração e Implementação (Serviço técnico especializado para o Item 1, incluindo fixação física, migração lógica e integração).	35.225,00	0,0	0,0	0,0	0,0	35.225,00
Aquisição Licenciamento Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, Licenciamento Forticare Premium) por 60 meses, para firewall Fortigate FG-1801F, com substituição por modelo equivalente em 1 (um) dia útil. FC-10-F18F1-809-02-x. FC-10-F18F1-210-02-x.	1.397.500,00	0,0	0,0	0,0	0,0	1.397.500,00
Renovação Licenciamento Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) por 60 meses, para firewall Fortigate FG-1801F, com substituição por modelo equivalente em 1 (um) dia útil.	1.383.710,15	0,0	0,0	0,0	0,0	1.383.710,15

<p>Equipamento Modelo: FortiGate FG-1801F</p> <p>SN FG181FTK21901099</p> <p>FC-10-F18F1-809-02-x.</p> <p>FC-10-F18F1-210-02-x.</p> <p>SN: FG181FTK21901099.</p>						
<p>Renovação Licenciamento FortiAnalyzer FAZ-VM-GB-100 (SN: FAZ-VMTM22000548), com 100 GB/dia de logs, com licenciamento por 60 meses, com capacidade de armazenamento ilimitada.</p> <p>Modelo: FortiAnalyzer FAZ-VM-GB-100</p> <p>FC5-10-LVOVM-248-02-x.</p>	237.010,27	0,0	0,0	0,0	0,0	237.010,27
<p>Contrato de manutenção e suporte para o equipamento FG-1801F em operação, bem como para os equipamentos dos itens 1,3, 4 e 5 desta contratação. A manutenção e o suporte deverão ser prestados na modalidade 24 horas por dia, 7 dias na semana, pelo período de 60 meses, com substituição por equipamento equivalente em, no máximo, um (1) dia útil. Os demais itens da contratação, relacionados aos licenciamentos, deverão permanecer cobertos por garantia e manutenção da fabricante Fortinet durante o mesmo período de 60 meses.</p>	59.982,00	59.982,00	59.982,00	59.982,00	59.982,00	299.910,00
Custo Total no Ano	3.619.477,75	59.982,00	59.982,00	59.982,00	59.982,00	-
Custo Total de Propriedade da Solução Viável 1 (5 anos)						<u>R\$ 3.859.405,75</u>

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na expansão, atualização e suporte contínuo do ecossistema de segurança de perímetro da UFRGS. A contratação será realizada por adjudicação global (lote único), visando garantir a integração nativa dos componentes, a responsabilidade centralizada do fornecedor e a formação de uma arquitetura de Alta Disponibilidade (HA) para a proteção das operações vitais da instituição.

O escopo exato da contratação é composto pelos 6 (seis) itens descritos a seguir:

12.1. Enquadramento do Modelo de Licenciamento de Software:

Em estrita observância à Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, registra-se que os componentes lógicos da solução (Itens 3, 4 e 5) enquadram-se no modelo de contratação de *software* por meio de subscrição e cessão temporária de direitos de uso, conforme tipificado no seu art. 4º, inciso I, e art. 6º, inciso II. A adoção do horizonte temporal de 60 (sessenta) meses atende à diretriz da referida Portaria quanto à diluição do Custo Total de Propriedade (TCO), garantindo a previsibilidade orçamentária e a manutenção ininterrupta das atualizações de segurança e assinaturas contra ameaças (*malware*, IPS, DLP) durante todo o ciclo de vida do ativo, sem a geração de custos ocultos com renovações anuais de curto prazo.

12.2. Infraestrutura Física (Hardware)

Item 1: Aquisição de 1 (um) equipamento (*appliance*) de *firewall* de próxima geração modelo **FortiGate FG-1801F**. O equipamento será destinado à composição de um *cluster* de Alta Disponibilidade (HA) com o ativo idêntico já operante no *datacenter* da UFRGS, eliminando pontos únicos de falha na borda da rede.

12.3. Serviços Especializados de Implementação

- **Item 2:** Serviço de instalação, configuração e implementação do equipamento descrito no **Item 1**. Contempla a instalação física (fixação em rack, cabeamento e energização), a configuração lógica para pareamento em HA, migração de políticas e integração com o ecossistema existente, culminando na entrega de documentação técnica.

12.4. Licenciamentos de Segurança Avançada (NGFW)

- **Item 3:** Aquisição de Licenciamento *Enterprise Protection* para o novo *firewall* FortiGate FG-1801F (Item 1), com vigência de 60 (sessenta) meses. O pacote inclui a habilitação contínua de: IPS, Prevenção de Malware baseada em Inteligência Artificial (*AI-based Inline Malware Prevention*), *Inline CASB Database*, DLP, *App Control*, *Advanced Malware Protection*, Filtro de URL/DNS/Vídeo, Anti-spam, *Attack Surface Security* e *Converter Svc*.
 - *Part Numbers* de Referência: FC-10-F18F1-809-02-60.
- **Item 4:** Renovação do Licenciamento *Enterprise Protection* para o *firewall* modelo FortiGate FG-1801F que já se encontra em produção na rede da UFRGS. A renovação terá vigência de 60 (sessenta) meses e garantirá a continuidade do mesmo escopo de proteção avançada listado no Item 3.
 - *Part Numbers* de Referência: FC-10-F18F1-809-02-60.

12.5. Telemetria e Gestão de Eventos de Segurança

- **Item 5:** Renovação do licenciamento da plataforma de correlação de *logs* FortiAnalyzer FAZ-VM-GB-100, instanciada no ambiente da universidade. A subscrição, com validade de 60 (sessenta)

meses, garantirá a capacidade de ingestão de 100 GB/dia de *logs* de segurança e armazenamento com capacidade ilimitada, garantindo a rastreabilidade necessária para auditorias e resposta a incidentes.

- *Part Number* de Referência: FC5-10-LVOVM-248-02-60.

12.6. Suporte Técnico Avançado e Acordo de Nível de Serviço (SLA)

- **Item 6:** Contrato de manutenção e suporte técnico avançado, prestado na modalidade 24 horas por dia, 7 dias por semana (24x7), pelo período contínuo de 60 (sessenta) meses. Este serviço cobrirá o equipamento FG-1801F recém-adquirido (Item 1), o FG-1801F já em operação, bem como o pleno funcionamento das plataformas e subscrições dos Itens 3, 4 e 5. Como garantia de resiliência e mitigação de riscos, o contrato exige a substituição de qualquer equipamento abrangido que apresente falha de hardware (*RMA*) por modelo equivalente no prazo máximo de 1 (um) dia útil (*FortiCare Premium* ou equivalente).
 - *Part Number* de Referência: FC-10-F18F1-210-02-60.

13. Estimativa de custo total da contratação

Valor (R\$): 3.859.405,75

A estimativa do custo total para a contratação da solução de segurança de perímetro foi apurada mediante pesquisa de mercado, em estrita observância ao Art. 23 da Lei nº 14.133/2021. Os valores de referência foram consolidados a partir da obtenção de cotações formais junto a fornecedores especializados (revendas autorizadas do fabricante) e de consultas a contratações similares na Administração Pública, garantindo a representatividade e a justeza dos preços estimados.

O modelo de contratação por adjudicação global (lote único) abrange o ciclo de vida da solução para um período de 60 (sessenta) meses, incorporando o Custo Total de Propriedade (TCO) e garantindo a previsibilidade orçamentária da Universidade para a proteção das suas operações vitais.

13.1. Planilha de Custos Estimados

Abaixo, apresenta-se a tabela com o detalhamento dos custos máximos aceitáveis para a contratação, cujas memórias de cálculo e documentos comprobatórios encontram-se acostados aos autos do processo:

Item	Descrição Resumida do Objeto	Quantidade	Valor Unitário Estimado (R\$)	Valor Total Estimado (R\$)
1	Equipamento FortiGate FG-1801F (Hardware novo, de primeiro uso para composição de cluster HA).	1 un.	506.050,33	506.050,33
2	Serviço de Instalação, Configuração e Implementação (Serviço técnico especializado para o Item 1, incluindo fixação física, migração lógica e integração).	1 sv.	35.225,00	35.225,00
	Aquisição Licenciamento Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB			

3	<p>Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, Licenciamento Forticare Premium) por 60 meses, para firewall Fortigate FG-1801F, com substituição por modelo equivalente em 1 (um) dia útil.</p> <p>FC-10-F18F1-809-02-x.</p> <p>FC-10-F18F1-210-02-x.</p>	1 conj.	1.397.500,00	1.397.500,00
4	<p>Renovação Licenciamento Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) por 60 meses, para firewall Fortigate FG-1801F, com substituição por modelo equivalente em 1 (um) dia útil.</p> <p>Equipamento Modelo: FortiGate FG-1801F</p> <p>SN FG181FTK21901099</p> <p>FC-10-F18F1-809-02-x.</p> <p>FC-10-F18F1-210-02-x.</p>	1 conj.	1.383.710,15	1.383.710,15
5	<p>Renovação Licenciamento FortiAnalyzer FAZ-VM-GB-100 (SN: FAZ-VMTM22000548), com 100 GB/dia de logs, com licenciamento por 60 meses, com capacidade de armazenamento ilimitada.</p> <p>Modelo: FortiAnalyzer FAZ-VM-GB-100</p> <p>FC5-10-LVOVM-248-02-x.</p>	1 un.	237.010,27	237.010,27
6	<p>Contrato de manutenção e suporte para o equipamento FG-1801F em operação, bem como para os equipamentos dos itens 1,3, 4 e 5 desta contratação. A manutenção e o suporte deverão ser prestados na modalidade 24 horas por dia, 7 dias na semana, pelo período de 60 meses, com substituição por equipamento equivalente em, no máximo, um (1) dia útil. Os demais itens da contratação, relacionados aos licenciamentos, deverão permanecer cobertos por garantia e manutenção da fabricante Fortinet durante o mesmo período de 60 meses.</p>	60 meses.	4.998,50	299.910,00
	<p>VALOR TOTAL ESTIMADO DA CONTRATAÇÃO (LOTE ÚNICO):</p>			3.859.405,75

13.2. Considerações sobre a Formação de Preços

- **Inclusão de Custos Indiretos:** Os valores estimados já contemplam todos os custos operacionais, encargos trabalhistas, previdenciários, tributos, despesas com logística, deslocamento técnico, seguros e o lucro da contratada, não cabendo qualquer pleito de acréscimo futuro a estes títulos.
- **Economicidade:** A contratação consolidada de *hardware*, licenciamento e suporte para o período de 60 meses, em detrimento de renovações anuais sucessivas, protege a Administração Pública contra flutuações cambiais severas (haja vista a natureza importada das tecnologias envolvidas) e reajustes inflacionários anuais por parte do fabricante, configurando a estratégia mais econômica e segura para a universidade.

14. Justificativa técnica da escolha da solução

A escolha pela **Solução de Expansão em Alta Disponibilidade e Renovação do Ecossistema Atual (Solução 1)** fundamenta-se na confluência entre a mitigação rigorosa de riscos cibernéticos, a imperatividade técnica de padronização e a observância irrestrita ao princípio da economicidade na Administração Pública.

Abaixo, elencam-se as justificativas que atestam ser esta a alternativa mais vantajosa para a UFRGS:

14.1. Imperatividade Técnica de Padronização e Compatibilidade

A indicação e exigência de continuidade com a tecnologia Fortinet (equipamento FortiGate FG-1801F e plataforma FortiAnalyzer) encontra amparo legal no Art. 41, inciso I, da Lei nº 14.133/2021, que versa sobre a padronização e a compatibilidade técnica com os sistemas já existentes. A Universidade já possui um equipamento FG-1801F em produção. Para alcançar a Alta Disponibilidade — com sincronismo de estado, sessões e tolerância a falhas transparente (*failover*) —, é um requisito técnico inflexível que o equipamento a ser adquirido possua a mesma arquitetura de *hardware*, sistema operacional e fabricante do nó principal. A inserção de um equipamento de marca distinta impossibilitaria a formação do *cluster*, mantendo a vulnerabilidade de ponto único de falha na borda da rede.

14.2. Preservação da Integração Nativa e Telemetria

A arquitetura de segurança atual da instituição consolida a telemetria e o armazenamento de *logs* no *appliance* virtual FortiAnalyzer (FAZ-VM-GB-100). A escolha por renovar esta subscrição e manter o parque de *firewalls* no mesmo ecossistema garante a comunicação nativa. A introdução de plataformas heterogêneas exigiria o desenvolvimento de integrações complexas via API ou a adoção de um novo correlacionador (SIEM) de terceiros, o que geraria estrangulamentos na ingestão dos 100 GB/dia exigidos e fragmentaria a visibilidade da equipe de resposta a incidentes.

14.3. Garantia de Continuidade das Operações Vitais

A transição para um novo fabricante de *firewall* (Solução 2, descartada) exigiria a tradução e a recriação manual de milhares de políticas de segurança, regras de roteamento e túneis VPN essenciais. Esse procedimento possui um risco elevadíssimo de falhas de configuração (*misconfigurations*), o que poderia resultar na indisponibilidade dos sistemas acadêmicos e administrativos. A expansão da solução atual garante uma transição segura, rápida e sem interrupções no tráfego, assegurando a continuidade ininterrupta dos serviços essenciais.

14.4. Conformidade Regulatória (LGPD) e Defesa Proativa

A renovação e aquisição unificada dos pacotes de licenciamento *Enterprise Protection* garantem a aderência imediata e contínua às exigências de proteção de dados pessoais (Lei nº 13.709/2018). Ao consolidar funcionalidades como Prevenção de Perda de Dados (DLP), Prevenção de Malware baseada em Inteligência Artificial, IPS e Controle de Aplicações (*App Control*) diretamente na borda, a UFRGS adota uma postura proativa de mitigação de riscos, alinhada ao PPSI e às melhores práticas da ISO/IEC 27001 e às diretrizes da IN SGD/ME nº 94/2022.

Diante do exposto, a contratação em lote único da expansão e atualização do ecossistema Fortinet constitui a única via técnica, operacional e legalmente segura para dotar a Universidade da resiliência exigida, otimizando os recursos públicos e blindando as operações institucionais contra ameaças cibernéticas.

15. Justificativa econômica da escolha da solução

Sob o ponto de vista econômico, considerou-se mais vantajosa a solução 1, por necessitar adquirir apenas um único equipamento. A solução 2 exigiria a substituição de toda a atual infraestrutura Fortinet de segurança por uma outra, de diferente fabricante, implicando na aquisição de mais de um equipamento e diversos licenciamentos e serviços, resultando em um impacto financeiro e técnico.

15.1 O PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

Considerando os valores apurados para a Solução 1 e apresentados na Análise Comparativa de Custos (TCO), haverá o parcelamento do item 6 da solução em decorrência da prestação mensal do serviço.

16. Benefícios a serem alcançados com a contratação

O atendimento da presente demanda representa não só a continuidade, mas também melhorias nos controles e nos níveis de segurança dos recursos de TI da Universidade. Essa contratação assegura também a conformidade com os requisitos de segurança exigidos pelo Governo Federal e pelo arcabouço normativo interno da Universidade.

Seguem alguns dos resultados a serem alcançados:

- 1) Continuidade da solução de segurança para os sistemas de informação e infraestrutura de rede da Universidade;
- 2) Continuidade do controle de acesso à rede e a serviços da Universidade;
- 3) Implementação e gerenciamento das políticas de acesso aos serviços e à rede da Universidade;
- 4) Aumento da resiliência contra interrupções das comunicações entre a rede da UFRGS e a Internet;
- 5) Expansão da abrangência de atuação da infraestrutura de segurança para outras áreas da UFRGS;
- 6) Monitoramento do tráfego de rede, visando identificar ameaças cibernéticas e dar apoio à resolução de tratamento de incidentes de segurança;

7) Manutenção dos controles para mitigação de ameaças cibernéticas e resolução de incidentes de segurança;

8) Armazenamento e análise de informações do tráfego com a Internet para o monitoramento e o tratamento de incidentes.

17. Providências a serem Adotadas

Não serão necessárias providências ou adaptação do ambiente.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A escolha da solução 1 insere-se nas ações estratégicas previstas no Plano de Desenvolvimento Institucional da Universidade (PDI), atendendo ao Plano de Desenvolvimento de Tecnologia da Informação (PDTI). Alinha-se também à Política de Segurança da UFRGS, aos planos institucionais da Unidade e ao Plano Anual de Aquisições.

Após análise, considerou-se a **solução 1**: Contratação de equipamento Firewall, com licenciamentos e suporte técnico, do fabricante Fortinet, como a solução mais vantajosa para a Universidade, sob o ponto de vista técnico e econômico, atendendo plenamente aos requisitos de segurança exigidos e à manutenção dos controles de segurança já existentes.

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](#).

ARTHUR BOOS JUNIOR

Integrante Requisitante

GUILHERME ROTTH ZIBETTI

Integrante Técnico

VIVIANE MARIA DOS SANTOS SOARES

Integrante Administrativo



Assinou eletronicamente em 07/04/2026 às 15:17:29.

RUI DE QUADROS RIBEIRO

Autoridade Máxima da Área de TIC