

# Estudo Técnico Preliminar

## 1. Informações Básicas

Número do processo: 23205.032712/2022-19

## 2. Descrição da necessidade

As informações referente a este item estão dispostas no tópico 2 do documento anexo

## 3. Área requisitante

Área Requisitante	Responsável
Diretoria de Infraestrutura de TI	Jefferson Caramori

## 4. Necessidades de Negócio

As informações referente a este item estão dispostas no tópico 4.1 do documento anexo

## 5. Necessidades Tecnológicas

As informações referente a este item estão dispostas no tópico 4.2 do documento anexo

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

As informações referente a este item estão dispostas no tópico 4.3 do documento anexo

## 7. Estimativa da demanda - quantidade de bens e serviços

As informações referente a este item estão dispostas no tópico 5 do documento anexo

## 8. Levantamento de soluções

As informações referente a este item estão dispostas no tópico 6 do documento anexo

## 9. Análise comparativa de soluções

As informações referente a este item estão dispostas no tópico 7 do documento anexo

## **10. Registro de soluções consideradas inviáveis**

As informações referente a este item estão dispostas no tópico 8 do documento anexo

## **11. Análise comparativa de custos (TCO)**

As informações referente a este item estão dispostas no tópico 8 do documento anexo

## **12. Descrição da solução de TIC a ser contratada**

As informações referente a este item estão dispostas no tópico 10 do documento anexo

## **13. Estimativa de custo total da contratação**

**Valor (R\$):** 1.026.978,40

As informações referente a este item estão dispostas no tópico 11 do documento anexo

## **14. Justificativa técnica da escolha da solução**

As informações referente a este item estão dispostas no tópico 12 do documento anexo

## **15. Justificativa econômica da escolha da solução**

As informações referente a este item estão dispostas no tópico 13 do documento anexo

## **16. Benefícios a serem alcançados com a contratação**

As informações referente a este item estão dispostas no tópico 14 do documento anexo

## **17. Providências a serem Adotadas**

As informações referente a este item estão dispostas no tópico 15 do documento anexo

## **18. Declaração de Viabilidade**

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

### **18.1. Justificativa da Viabilidade**

As informações referente a este item estão dispostas no tópico 1 do documento anexo

## 19. Responsáveis

NEIMAR MARCOS ASSMANN

Analista de Tecnologia da Informação

FLAVIO HUMBERTO TESTA

Analista de Tecnologia da Informação

MARCOS EUGÊNIO DIETRICH

Técnico de Tecnologia da Informação

MICHEL ARCARI

Técnico de Tecnologia da Informação

## Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ENCARTE C - Estudo Técnico Preliminar - (Firewall).pdf (1.93 MB)

**Anexo I - ENCARTE C - Estudo Técnico Preliminar -  
(Firewall).pdf**



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

# **ESTUDO TÉCNICO PRELIMINAR**

**Processo Administrativo nº 23205.004012/2022-26**

**Processo Administrativo de Compras nº 23205.032712/2022-19**

**Solução para licenciamento, garantias e suporte de  
firewall**

Chapecó, outubro de 2022



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

### Histórico de Revisões

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Autor</b>
26/09/2022	1.0	Finalização da primeira versão do documento	Flavio Testa
10/10/2022	2.0	Revisão e ajustes do documento	equipe de planejamento



## Sumário

<b>INFORMAÇÕES BÁSICAS E INTRODUÇÃO</b>	<b>5</b>
<b>DESCRIÇÃO DA NECESSIDADE PÚBLICA</b>	<b>5</b>
Necessidade Pública	5
Motivação/Justificativa	5
<b>ÁREA REQUISITANTE</b>	<b>5</b>
<b>DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS</b>	<b>5</b>
Identificação das necessidades de negócio	5
Identificação das necessidades tecnológicas	6
Demais requisitos necessários e suficientes à escolha da solução de TIC	7
Requisitos de Capacitação	7
Requisitos Legais	7
Requisitos de Manutenção	7
Requisitos temporais	8
Requisitos de Segurança e Privacidade	8
Requisitos Sociais, Ambientais e Culturais	8
Requisitos de arquitetura tecnológica	8
Requisitos de projeto e de implementação	9
Requisitos de implantação	9
Requisitos de garantia e manutenção	9
Requisitos de experiência profissional	10
Requisitos de formação de equipe	10
Requisitos de metodologia de trabalho	10
Requisitos de entrega e de fornecimento	10
Requisitos de qualidade e padronização	10
<b>ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS</b>	<b>10</b>
<b>LEVANTAMENTO DE SOLUÇÕES</b>	<b>11</b>
Análise de soluções	11
Identificação das soluções	11
<b>ANÁLISE COMPARATIVA DE SOLUÇÕES</b>	<b>12</b>
Análise comparativa de cenários	14
Análise SWOT das alternativas	14
<b>REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS</b>	<b>15</b>
<b>ANÁLISE COMPARATIVA DE CUSTOS (TCO)</b>	<b>15</b>
Cálculo dos custos totais de propriedade	15
Mapa comparativo dos cálculos totais de propriedade (TCO)	16
<b>DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA</b>	<b>16</b>
<b>ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO</b>	<b>16</b>
Justificativa técnica da escolha da solução	16
Justificativa econômica da escolha da solução	16
Benefícios a serem alcançados com a contratação	16
Providências a serem Adotadas	16
<b>DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO</b>	<b>16</b>





## ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

### 1. INFORMAÇÕES BÁSICAS E INTRODUÇÃO

- 1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda PORTARIA Nº 711/PROAD/UFFS/2022, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 01/2019.
- 1.2. O objeto do estudo é o **licenciamento, garantias e suporte de firewall** que atenda de forma ampla às demandas institucionais de toda a UFFS, registradas no Plano Anual de Contratação (PAC), por meio do Sistema de Planejamento e Gerenciamento de Contratações (sistema PGC).

### 2. DESCRIÇÃO DA NECESSIDADE PÚBLICA

#### 2.1. Necessidade Pública

Garantir a segurança da informação institucional através de solução de perímetro de rede firewall de borda, que inspecione e proteja proativamente o trânsito de informações entre a rede pública, também conhecida como internet, e a rede interna da UFFS, suas aplicações, sistemas e ativos de informação.

#### 2.2. Motivação/Justificativa

O Ciclo de licenciamentos do Firewall se encerra agora em 2022, ter esses equipamentos renovados e up to date é parte da solução que protege o ativo mais valioso da UFFS: a informação. Garantindo assim a integridade, disponibilidade e autenticidade da mesma.

### 3. ÁREA REQUISITANTE

Área Requisitante	Responsável
Diretoria de Infraestrutura de TI	Jefferson Caramori



#### 4. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITO

##### 4.1. Identificação das necessidades de negócio

Necessidades		Funcionalidades		Atores envolvidos	
Id	Descrição da Necessidade	Id	Descrição da funcionalidade	Id	Atores envolvidos
1	Atualização tecnológica e Renovação de licença, garantia e suporte do firewall PA 3020, Threat prevention e URL Filtering. Aquisição do Global Protect	1	Contrato de licença, garantia e suporte para firewall modelo que irá substituir PA 3020 à segurança de rede do datacenter da UFFS.	1	Equipe de planejamento
2	Renovação de licença, garantia e suporte de firewall PA 220 <b>ou atualização tecnológica</b> , Threat prevention e URL Filtering	2	Contrato de licença, garantia e suporte para firewall modelo PA 220 ou superior destinado à segurança de rede dos campi UFFS.	1	Equipe de planejamento
3	Licença e suporte do Software de Gerenciamento de Segurança de Redes - Panorama - para gerenciar até 25 dispositivos	3	Contrato de aquisição de licença, garantia e suporte do software de gerenciamento centralizado para os firewalls da UFFS	1	Equipe de planejamento
4	Configuração da solução	4	Contrato de aquisição do serviço de configuração do ambiente proposto com vistas a melhorar a autonomia e redundância da rede	1	Equipe de planejamento



#### 4.2. Identificação das necessidades tecnológicas

##### **Aquisição de equipamento que irá substituir PA 3020, Contrato de licença, garantia, para Threat prevention e URL Filtering ou superior**

Na eventual necessidade de substituição de peças, as mesmas deverão possuir características idênticas às defeituosas. Na impossibilidade de substituir por peças idênticas, mediante avaliação pela equipe de TI, as novas deverão ser superiores e compatíveis com o ambiente de infraestrutura da UFFS. Caso seja necessário atendimento local, os custos com transporte, hospedagem e outros custos operacionais ficarão a cargo da contratada, de acordo com o disposto na IN 01 de 04 de abril de 2019.

Este equipamento deve ser compatível com transceiver CISCO, e os cabos que irão ser conectorizados com equipamento Switch Cisco, deverão ser fornecidos.

Abaixo segue a configuração mínima necessária, de acordo com as necessidades atuais:

- Throughput de firewall: 4 Gbps,
- Throughput de prevenção contra ameaças: 2 Gbps
- Throughput de VPN IPSec: 1 Gbps
- No mínimo 12 portas RJ-45
- No mínimo 2 portas SFP/SFP+
- Novas sessões por segundo: 50.000
- Máximo de sessões: 250.000
- Interfaces de túneis de VPN: 1.000
- Usuários VPN simultâneos: 1.000
- Roteadores virtuais: 10
- Zonas de Segurança: 40
- Número máximo de políticas: 2.500
- Licença, Suporte e garantia de atualizações de acordo com SLA.
- O fornecimento das licenças, garantia e suporte devem estar de acordo com a IN 01 de 04 de abril de 2019.
- Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em next business day;

##### **Contrato de licença, garantia e suporte de firewall PA 220 ou atualização tecnológica, Threat prevention e URL Filtering:**

Na eventual necessidade de substituição de peças, as mesmas deverão possuir características idênticas às defeituosas. Na impossibilidade de substituir por peças idênticas, mediante avaliação pela equipe de TI, as novas deverão ser superiores



e compatíveis com o ambiente de infraestrutura da UFFS. Caso seja necessário atendimento local, os custos com transporte, hospedagem e outros custos operacionais ficarão a cargo da contratada, de acordo com o disposto na IN 01 de 04 de abril de 2019.

Abaixo segue a configuração mínima necessária, de acordo com as necessidades atuais:

- Throughput de firewall: 1 Gbps
- Throughput de prevenção contra ameaças: 500 Mbps
- Throughput de VPN IPSec: 50 Mbps
- Novas sessões por segundo: 42000
- Máximo de sessões: 64.000
- Interfaces de túneis de VPN: 250
- Usuários VPN simultâneos: 1.000
- Roteadores virtuais: 3
- Zonas de Segurança: 20
- Número máximo de políticas: 1.000
- Licença, Suporte e garantia de atualizações de acordo com SLA.
- O fornecimento das licenças, garantia e suporte devem estar de acordo com a IN 01 de 04 de abril de 2019.
- Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em next business day;

#### **Renovação Software de Gerenciamento Centralizado dos firewalls - Panorama**

Especificações mínimas:

- Deve prover gestão centralizada dos Módulos de Proteção de Rede, e ser necessariamente do mesmo fabricante;
- Deve permitir visualização de registros (logs) e dados de relatórios dos Módulos de Proteção de Rede do ambiente, de forma centralizada;
- Deve permitir criação de políticas de segurança compartilhadas;
- Deve suportar a gestão de, no mínimo, 25 (vinte e cinco) Módulos de Proteção de Rede;
- Deve ser do tipo “Appliance Virtual”, solução de software baseada em máquina virtual (VM);
- Deve ser compatível com VMWare ESX(i);
- A comunicação entre o Módulo de Gestão Centralizada e os Módulos de Proteção de Rede deve ser criptografada;
- O gerenciamento deve permitir/Possuir:



1. Criação e administração de políticas;
2. Administração de políticas de IPS, Anti-virus e Anti-Spyware;
3. Política de Filtro de Dados e Filtro de URLs;
4. Monitoração de logs;
5. Ferramentas de investigação de logs;
6. Deve possuir relatórios de utilização dos recursos
7. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;
8. Deve possuir mecanismo Drill-Down para navegação nos relatórios RealTime;
9. Nas opções de Drill-Down ser possível identificar o usuário que fez determinado acesso independente do IP e local que o usuário esteja no momento do acesso;
10. Deve ser possível exportar os logs em formato CSV;
11. Deve ser possível capturar as URLs acessadas para todas as sessões HTTP;
12. Deve possibilitar a criação de diferentes perfis de administração separando pelo menos: Leitura, Alterações, Relatórios e Monitoração;
13. Deve ser possível, de forma granular, assinar permissões para os administradores criarem outros usuários, alterem configurações, ler configurações, etc;
14. Suportar validação de regras antes da sua aplicação no módulo de proteção;
15. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas, possibilitando retornar a uma configuração previamente utilizada;
16. O gerenciamento centralizado deve permitir controle sobre todos os Firewalls em uma única console, com administração de privilégios ou funções;
17. O gerenciamento centralizado deve possibilitar a instalação como virtual appliance sobre VMware, fornecendo a flexibilidade para instalar-se em diferentes combinações de Hardware e sistemas operacionais;
18. Deve suportar autenticação de administradores usando base de dados local e Radius, Microsoft AD, Secure-ID, Kerberos ou LDAP;
19. Permitir geração de relatórios de atividades do usuário;
20. Permitir controle Global de Políticas;
21. Deve suportar organização em grupos de Firewalls: Os sistemas virtuais serão administrados como dispositivos individuais, os grupos podem ser geográficos, por Funcionalidade (por exemplo, como IPS), e distribuição;



22. Deve suportar objetos e políticas compartilhadas;
23. Deve possuir relatórios predefinidos e permitir relatórios projetados pelo usuário;
24. Deve permitir exportar todos os relatórios nos formatos CSV e PDF.

#### Autenticação

1. Para autenticação dos administradores da solução deve ser suportado:

1. LDAP
2. Radius
3. Soluções Baseadas em Token (i.e. Secure-ID)
4. Kerberos

#### Relatórios

1. Deve incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente;
2. Deve permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário;
3. Deve contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças;
4. Deve permitir a criação de relatórios personalizáveis;
5. Deve contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, ip origem e ip destino e usuário;
6. Deve ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
7. Deve gerar relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
8. O equipamento deve proporcionar, no mínimo, os seguintes conjuntos de relatórios:
  1. Utilização de largura de banda de entrada e saída por aplicação (TOP 10);
  2. Número de Sessões por aplicação (TOP 10);
  3. Comparativo semanal de aplicações utilizadas na rede que possam induzir Latência. (TOP 10);
  4. Taxa de transferência (em bytes) por aplicação (TOP 10);
  5. Origem e destino do tráfego por aplicação – Usuário (TOP 10);
  6. Sessões e E-mail público;
  7. Utilização de navegação;
  8. Eventos / Ataques por: Origem, Categoria, Ameaça, Protocolo (TOP



10);

9. Nível de risco da rede;

10. Principais protocolos e aplicações que circulam pelo Firewall (TOP 25);

11. Principais endereços de IP destino por protocolo (TOP 25);

12. Os principais endereços IP para cada um dos protocolos e aplicações principais (TOP 50);

O fornecimento das licenças, garantia e suporte devem estar de acordo com a IN 01 de 04 de abril de 2019;

Garantia de 36 (trinta e seis) meses.

A ferramenta de gerenciamento de segurança deve ser compatível com os firewalls já existentes na instituição sendo eles:

- Palo alto PA3020;
- Palo alto PA220
- Palo Alto PA500

#### **Configuração da solução:**

Demanda de configuração da solução:

O serviço de configuração do ambiente proposto deverá ser fornecido pela contratada de forma remota. Caso seja necessário atendimento local, os custos com transporte, hospedagem e outros custos operacionais ficarão a cargo da contratada, de acordo com o disposto na IN 01 de 04 de abril de 2019.

#### **4.3. Demais requisitos necessários e suficientes à escolha da solução de TIC**

##### **4.3.1. Requisitos de Capacitação**

Atualmente o quadro de servidores lotados no DRT (Departamento de Redes e Telecomunicações) e DITI possuem conhecimento necessário para a utilização dos itens descritos na sessão 1.2, ou seja, não é necessário a realização de capacitações para a utilização de tais itens.

##### **4.3.2. Requisitos de Manutenção**

Os requisitos de garantia e manutenção apresentados estão organizados e descritos de acordo com o tipo e finalidade identificados nas necessidades



elencadas na seção 1.1 deste documento.

Contrato de atualização tecnológica do PA 3020 e renovação da licença, garantia e suporte de firewall. Funcionalidades Threat prevention e URL Filtering:

Especificações:

A contratada ou fabricante deverá:

- Fornecer diagnósticos de problemas e suporte remoto;
- Fornecer atendimento telefônico direto por especialistas da área técnica;
- Fornecer suporte de hardware nas instalações do cliente com peças e mão de obra inclusas no contrato;
- Fornecer períodos de cobertura e tempos de resposta flexíveis, na modalidade 8x5;
- Realizar o atendimento pela própria PaloAlto ou por autorizada;
- Fornecer acesso a informações e serviços eletrônicos avançados de suporte que aumentam a produtividade do serviço, onde se possa obter informações sobre hardware e documentações, atualizações de firmware, abertura eletrônica e acompanhamento de chamados;
- Fornecer acesso a um sistema web onde é possível gerenciar os contratos de serviços de suporte com a PaloAlto, obter visualização dos equipamentos atualmente sob contrato com os devidos detalhes (modelo, nível de serviço e vigência);
- Atendimento na modalidade 8x5.

Contrato de renovação da licença, garantia e suporte de firewall modelo PA 220 ou atualização tecnológica. Funcionalidades Threat prevention e URL Filtering:

Especificações:

A contratada ou fabricante deverão:

- Fornecer diagnósticos de problemas e suporte remoto;
- Fornecer atendimento telefônico direto por especialistas da área técnica;
- Fornecer suporte de hardware nas instalações do cliente com peças e mão de obra inclusas no contrato;
- Fornecer períodos de cobertura e tempos de resposta flexíveis, na modalidade 8x5;
- Realizar o atendimento pela própria PaloAlto ou por autorizada;
- Fornecer acesso a informações e serviços eletrônicos avançados de suporte que aumentam a produtividade do serviço, onde se possa obter informações sobre hardware e documentações, atualizações de firmware, abertura eletrônica e acompanhamento de chamados;
- Fornecer acesso a um sistema web onde é possível gerenciar os contratos de serviços de suporte com a PaloAlto, obter visualização dos equipamentos atualmente sob contrato com os devidos detalhes (modelo, nível de serviço e vigência).

Contrato de aquisição da licença, garantia e suporte de Software de Gerenciamento de Segurança de Redes PANORAMA:





Especificações:

A contratada ou fabricante deverão:

- Fornecer diagnósticos de problemas e suporte remoto;
- Fornecer atendimento telefônico direto por especialistas da área técnica;
- Fornecer períodos de cobertura e tempos de resposta flexíveis, na modalidade 8x5;
- Realizar o atendimento pela própria PaloAlto ou por autorizada;
- Fornecer acesso a informações e serviços eletrônicos avançados de suporte que aumentam a produtividade do serviço, onde se possa obter informações sobre hardware e documentações, atualizações de firmware, abertura eletrônica e acompanhamento de chamados;
- Fornecer acesso a um sistema web onde é possível gerenciar os contratos de serviços de suporte com a Paloalto, obter visualização dos equipamentos atualmente sob contrato com os devidos detalhes (modelo, nível de serviço e vigência).

#### **4.3.3. Requisitos temporais**

Para renovação de licenças, onde não há troca de equipamento, a entrega deverá ser disponibilizada imediatamente após a assinatura do contrato, seguindo os padrões de entrega do fornecedor Palo Alto.

Para aquisição de novo equipamento e a respectiva configuração da solução o prazo de vigência deverá ser definido em reunião conjunta de implantação da solução.

#### **4.3.4. Requisitos de Segurança e Privacidade**

Segurança física: Atualmente a UFFS já dispõe de infraestrutura operacional nas unidades e respectiva segurança física.

Segurança da informação: Deve estar em conformidade com a política de segurança da informação e comunicação da UFFS (POSIC PORTARIA Nº 216/GR/UFFS/2018) vigente.

#### **4.3.5. Requisitos Sociais, Ambientais e Culturais**

Os equipamentos devem estar em acordo com a Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos.

No que couber, visando atender ao disposto na legislação aplicável – em destaque às Instruções Normativas nº 05/2017/SEGES e nº 01/2019/SGD – a CONTRATADA deverá priorizar, para o fornecimento do objeto, a utilização de bens que sejam no todo ou em parte compostos por materiais recicláveis, atóxicos e biodegradáveis.

Nenhum dos equipamentos fornecidos poderá conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil



polibromados (PBBs), éteres difenil-polibromados (PBDEs) em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), sendo que para efeitos de avaliação das amostras e aceitação do produto deverá ser fornecido certificação emitida por instituição credenciada pelo INMETRO, sendo aceito ainda, a comprovação deste requisito por intermédio da certificação EPEAT ou declaração emitida pelo fabricante, desde que esta apresente explicitamente tal informação;

#### **4.3.6. Requisitos de arquitetura tecnológica**

Compatíveis com os equipamentos já existentes no parque PA 3020, PA 220 e PA 500, mesmo aqueles que não integram a rede de produção da UFFS, devem estar visíveis e disponíveis no Panorama da instituição, que terá seu licenciamento renovado.

#### **4.3.7. Requisitos de projeto e de implementação**

Os PAs 220 localizados em Campis remotos, bem como o Panorama localizado no datacenter da UFFS, não necessitam de nenhum procedimento especial de implementação, já que trata-se de ativação exclusiva de licença. Para o PA 3020 será necessário a troca de equipamento frente ao fim de vida do produto que se encerra em 2024 e também pelas necessidades de interface física da UFFS, o PARC Chapecó, bem como novos arranjos que demandam o refresh tecnológico. Para o equipamento que irá suceder o PA 3020, os requisitos de projeto deverão ser definidos em reunião conjunta de implantação da solução.

#### **4.3.8. Requisitos de implantação**

1. Os serviços devem ser executados de forma 100% remota e planejados por técnicos certificados em gerenciamento de projetos. Fica a cargo deste órgão a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;
2. Será de responsabilidade da contratada todo o planejamento e implementação da topologia de rede e de recursos de segurança.
3. Os serviços devem ser executados de segunda a sexta-feira, das 8 às 20 horas, nas unidades da contratante;
4. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência/videoconferência;
5. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos; descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos



- serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da contratante e contratada; cronograma faseado do projeto, dividido em etapas, com responsáveis e data de início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da contratante e contratada; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
6. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;
  7. Serviço referente à solução de Firewall de Próxima Geração (NGFW):
    1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução;
    2. Configurar o firewall para proteção de perímetro e internet;
    3. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões conforme acordado previamente no planejamento dos serviços utilizando de autenticação integrada ao Microsoft Active Directory (AD) ou servidor radius;
    4. Configurar as funcionalidades relevantes a implementação da solução conforme acordado previamente no planejamento dos serviços como: Endereçamento, VLANs, LACP, DHCP e tipos NAT;
    5. Configurar o monitoramento da solução via SNMP em sistema de gerenciamento da CONTRATANTE para monitoramento de falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede;
    6. Configurações de roteamento conforme acordado previamente no planejamento dos serviços como configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF para IPv4 e/ou IPv6;
    7. Configurar e testar conexões vpn *client-to-server* e *site-to-site* cujas licenças já estão embarcadas no licenciamento adquirido.
    8. Migrar e otimizar QOS de acordo com a realidade da CONTRATANTE;
    9. Configurar de-criptografia SSL/TLS inbound e outbound (utilizando o certificado da CONTRATANTE)
    10. Migrar Configuração DMZ para permitir as configurações do firewall seguindo as boas práticas;
    11. Atualizar, habilitar e configurar através das boas práticas, todas as features das licenças adquiridas;
    12. Atualização de firmware dos appliances;
    13. Migrar e Configurar schedules de atualizações dos appliances e suas features;
    14. Migrar a Configuração de interfaces em modos: transparente, camada 2 (L2) ou camada 3 (L3), conforme acordado previamente no planejamento dos serviços;



15. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles por zona de segurança, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários, grupos de usuários e políticas por geolocalização;
16. Na configuração de VPN cliente-to-site deverá ser configurado no mínimo 10 (dez) perfis de checagem de conformidade de dispositivo, a fim de homologar e realizar um repasse de informações desta funcionalidade em específico;
17. Implementar políticas de bloqueios de arquivos conforme acordado no planejamento dos serviços (Wildfire);
18. Configurar limitações de banda por com base no IP de origem, usuários e grupos conforme acordado previamente no planejamento dos serviços;
19. Realizar a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias da CONTRATANTE conforme acordado previamente no planejamento dos serviços;
20. Configurar regras de filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL com conformidade de dispositivo, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Segurança de DNS, Filtro de URL, conforme acordado previamente no planejamento dos serviços;
21. Realizar backup das configurações realizadas;
22. Todas as configurações devem ser enviadas via Panorama;
23. As atividades de instalação no racks padrão 19" existente, energização e conectorização das interfaces de rede e interface de gerenciamento dos equipamentos ficará a cargo da CONTRATANTE;
24. Deve ser entregue relatório contendo todo o serviço realizado executado;
25. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da contratante.

#### 4.3.9. Requisitos de garantia e manutenção

##### Condições de Participação e Realização dos Serviços

- A solução deverá ser constituída dos equipamentos relacionados nos itens deste **grupo (lote)**, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;
- A escolha do agrupamento dos itens em **grupo** visa a plena qualificação da empresa fornecedora que prestará os serviços de fornecimento, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total



compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.

#### Garantia

- Os equipamentos fornecidos deverão estar cobertos por garantia do fabricante no Brasil pelo período especificado em cada item;
- A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos;
- Os softwares fornecidos deverão estar cobertos por garantia que oferece atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório dos softwares;
- A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição;
- Devem ser descritos, no momento da proposta, qual o tipo de garantia fornecida. Os equipamentos devem ter seus números seriais atrelados ao sistema de suporte do fabricante dos equipamentos com data específica de início e fim do suporte.

#### Atualizações

- A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e *firmwares* dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;
- As atualizações incluídas devem ser do tipo “*minor release*” e “*major release*”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware.



#### **4.3.10. Requisitos de experiência profissional**

- Exigências Comerciais e de Qualificação do Fornecedor (Habilitação)
  - Atestado de capacidade técnica, fornecidos por pessoas jurídicas de direito público ou privado, impresso em papel timbrado, com os dados do responsável pela informação atestada, comprovando que a licitante forneceu, instalou, configurou, realizou treinamento e prestou suporte técnico de solução Palo Alto Networks com as características solicitadas neste termo ;
  - Devido ao serviço crítico de implementação e suporte a empresa deverá comprovar que possui nível de parceria Palo Alto Networks nível Certified Professional Services Partner (CPSP);

#### **4.3.11. Requisitos de formação de equipe**

- A empresa deverá possuir, após a assinatura do contrato, pelo menos 2 (dois) profissionais com certificação técnica oficial do fabricante, compatível com o(s) objeto(s) deste processo, capaz de prestar o suporte em garantia e escalar o chamado ao fabricante conforme necessidade;

#### **4.3.12. Requisitos de metodologia de trabalho**

Deverá ser definido em reunião conjunta de implantação da solução. Para as demais entregas pode ser encontrado no Encarte I - Termo de Referência no item 4.13.

#### **4.3.13. Requisitos de entrega e de fornecimento**

Prazo de entrega de produtos: no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato; prorrogáveis por mais 90 (noventa) mediante justificativa. A entrega deve ser agendada com antecedência mínima de 24 horas; Para itens de software (licenças), estes devem ser fornecidos em até 30 dias. O processo de entrega dos equipamentos deverá ser realizado pela CONTRATADA sob a supervisão do preposto, que dará conhecimento do andamento do fornecimento aos diversos locais ao gestor do contrato. O local de entrega dos bens será no setor de patrimônio da UFFS em Chapecó/SC ou em local acordado entre a UFFS e o preposto; Av. Fernando Machado, 108 E, Centro, Chapecó, SC - Brasil, Caixa Postal 181 - CEP



89802-112.

As unidades do equipamento deverão ser entregues devidamente acondicionadas em embalagens individuais adequadas, que utilizem preferencialmente materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e a armazenagem;

#### **4.3.14. Requisitos de qualidade e padronização**

Deverá ser apresentado prospecto com as características técnicas de todos os componentes do equipamento, como placa principal, processador, memória, interfaces de comunicação (dados, áudio e vídeo), fonte de alimentação, unidade de armazenamento, incluindo especificação de marca, modelo, part number e outros elementos que de forma inequívoca identifiquem e comprovem as configurações cotadas, possíveis expansões e melhorias, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes, inclusive declarações técnicas. Serão aceitas cópias das especificações obtidas em sítios dos fabricantes na Internet, em que constem o respectivo endereço eletrônico. A escolha do material a ser utilizado fica a critério do proponente;

Caso os catálogos técnicos dos bens não apresentem alguma informação ou exigência técnica em relação aos descritivos do Edital e seus Anexos, deverão ser anexadas declarações do fabricante, completando estas informações, preferencialmente em português ou, se não disponível, em inglês.

Todos os equipamentos a serem entregues deverão ser idênticos, ou seja, todos os componentes externos e internos de mesmos modelos e marcas dos utilizados nos equipamentos enviados para avaliação e homologação. Caso o componente não mais se encontre disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante nova homologação;

Todos os cabos e conectores necessários ao funcionamento dos equipamentos deverão ser fornecidos, incluindo os cabos SFP+ que ligarão o equipamento Palo Alto e Switch Cisco. Cabos de conexão à rede elétrica deverão seguir o padrão NBR-14136;

Todos os equipamentos a serem fornecidos deverão ser novos, estar em linha de produção e fabricação, com a embalagem original de fábrica lacrada, sendo que, em hipótese alguma, a UFFS aceitará equipamentos recondicionados ou já utilizados anteriormente.

Os equipamentos devem ser fornecidos com todos os itens e acessórios necessários à sua perfeita ativação e funcionamento.



## 5. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

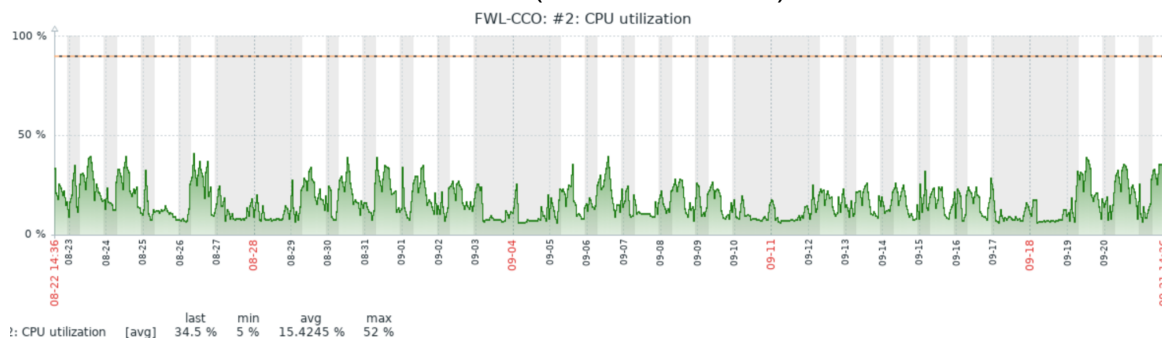
### 5.1. Cenário Atual

Campus	Modelo	Identificação	Serial	Necessidade
Chapecó - SC	Panorama	Panorama	000702033251	Renovação
Chapecó - SC	PA-3020	FWL-CCO	001801057433	Atualização Tecnológica <sup>1</sup>
Realeza - PR	PA- 220	FWL-RLZ	012801144041	Renovação
Laranjeiras do Sul - PR	PA- 220	FWL-LJS	012801143798	Renovação
Cerro Largo	PA- 220	FWL-CRR	012801143812	Renovação
Erechim - RS	PA- 220	FWL-ERE	012801143592	Renovação
Passo Fundo - RS	PA- 220	FWL-PAS	012801144033	Renovação

O presente estudo visa a manutenção da atual solução de firewall, pois a mesma tem se provado eficiente em conter as tentativas de ataque, bem como a gestão de ameaças, filtro e gerenciador entre a rede interna e externa.

Verifique-se que o principal firewall localizado no datacenter é o mais antigo da instituição estando presente na infraestrutura da UFFS desde 2016. Ao longo de 6 anos ainda é um equipamento que suporta bem as demandas, como conseguimos visualizar no gráfico de CPU que chega ao máximo de quase 50% de sua capacidade. O mesmo vale para o número de sessões ativas atualmente tendo picos de 30% de sua capacidade, o throughput mantendo-se no máximo entre 30 e 50% e o throughput de VPN este sim o que chega mais próximo das capacidades deste modelo de equipamento. A VPN site to site, tem alcançado picos de 100 Mbps ou mais por campi remoto, ao todo são 5 campi remotos (Laranjeiras do Sul, Realeza, Passo Fundo, Cerro Largo e Erechim) e ainda tem a mais os tráfegos dos usuários que trabalham de casa via VPN, mantendo um fluxo diário entre 50 e 100 Mbps, desta forma o firewall tem trabalhado no limite de sua capacidade de throughput de VPN, que é de 500 Mbps.

#### Firewall Datacenter - Consumo CPU (modelo PA 3020)



<sup>1</sup> <https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates>





## UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Outro ponto de grande sensibilidade é que o equipamento PA 3020, não possui portas SFP+ (10Gbps) e a UFFS a partir deste ano deve se tornar um Ponto de Presença (PoP) da rede acadêmica de Chapecó (PARC), onde está sendo construindo uma rede em anel que deve interligar as universidades, hospitais e órgãos públicos da cidade, conferindo a cidade de Chapecó, instituições participantes e comunidade acadêmica maior robustez e confiabilidade em nossa rede. Para a UFFS aproveitar o máximo desta rede no tráfego de entrada e saída será necessário utilizarmos de interface SFP+ disponibilizadas no equipamento, o que não acontece hoje, pois o firewall possui portas RJ-45 apenas. Mesmo as interfaces com capacidade até 1Gbps já estão em seu limite de uso, sendo conveniente um equipamento mais moderno que disponibilize mais interfaces diretamente no firewall.

Por fim, o terceiro levantamento que nos obriga a concluir que haverá a necessidade de troca de equipamento é que PA 3020 está com o fim de vida já anunciado pelo fabricante para o dia 31.10.2024, ou seja dentro do ciclo de vida desta contratação que é de 3 anos. Após esta data o equipamento perde totalmente a capacidade de receber atualizações diárias contra ameaças, as licenças perdem a utilidade, tornando o mesmo obsoleto e incapaz de cumprir com suas funções mais críticas.

End-of-Sale Product	End-of-Sale Date	End-of-Life Date	Resources	Last Supported OS
PA-220	January 31, 2023	January 31, 2028	<a href="#">PA-220 Datasheet</a>	PAN-OS 10.2^^
ION 7000	February 1, 2022	February 1, 2027	<a href="#">ION 7000 Hardware Reference Manual</a>	TBD
PA-7000-20GXM-NPC PA-7000-20GQXM-NPC	May 8, 2021	May 8, 2026	<a href="#">PA-7000 Series</a> <a href="#">PA-7000 Series Datasheet</a>	PAN-OS 10.1‡
PA-7050-SMC PA-7080-SMC PA-7000-LPC	February 28, 2021	February 28, 2026	<a href="#">PA-7000 Series</a> <a href="#">PA-7000 Series Datasheet</a>	PAN-OS 10.1‡
K2-Series (PA-5280-K2, PA-7050-K2, PA-7080-K2)	February 28, 2021	February 28, 2026	<a href="#">K2-Series Datasheet</a>	PAN-OS 10.1‡
M-500	February 29, 2020	February 28, 2025	<a href="#">Panorama Overview</a> <a href="#">Panorama Specs sheet</a>	PAN-OS 10.1‡
PA-3000 Series (PA-3020, PA-3050, PA-3060)	October 31, 2019	October 31, 2024	<a href="#">PA-3000 Series Overview</a> <a href="#">PA-3000 Series Specs sheet</a>	PAN-OS 9.1++

Portanto a recomendação para este caso será de troca de equipamento, para um modelo mais novo, tendo em vista que PA 3020 terá cumprido 6 anos em produção. A previsão é que o equipamento componha a infraestrutura pelos próximos 3 anos como equipamento de redirecionamento interno de tráfego entre unidades ou backup em caso de disaster & recovery, no entanto sem contato direto com a internet.

O equipamento Palo Alto que pode substituir o PA 3020 é a linha PA 400, PA 800, PA3200 e PA 3410. No entanto, o PA 400 não possui interface física SFP+, portanto não



# UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

poderá atender ao requisito. Já o PA 800 possui throughput limite de 2Gbps, tendo sido a solução desenhada para um requisito mínimo de 4Gbps.

Nesta linha o herdeiro natural do PA 3020 seria um equipamento da linha PA 3200 ou o PA 3410, que seria o modelo de entrada da linha 3400.

**Table 1: PA-3400 Series Performance and Capacities**

	PA-3440	PA-3430	PA-3420	PA-3410
Firewall throughput (HTTP/appmix)*	30.2/24 Gbps	25.5/20.5 Gbps	20.8/16.9 Gbps	14.5/11.6 Gbps
Threat Prevention throughput (HTTP/appmix)†	11.0/12.8 Gbps	9.2/10.5 Gbps	7.6/8.7 Gbps	5.2/5.9 Gbps
IPsec VPN throughput‡	14.5 Gbps	12.2 Gbps	9.9 Gbps	6.8 Gbps
Max sessions	3M	2.5M	2M	1.4M
New sessions per second§	268,000	240,000	205,000	145,000
Virtual systems (base/max)	1/11	1/11	1/11	1/11

PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)

X

**Tabela 1: Desempenho e capacidades do PA-3200 Series**

	PA-3260	PA-3250	PA-3220
Taxa de transferência de firewall (HTTP/appmix)*	7,8/8,7 Gbps	5,3/5,8 Gbps	4,3/4,8 Gbps
Taxa de transferência do Threat Prevention (HTTP/appmix)†	3,9/4,7 Gbps	2,6/3,1 Gbps	2,1/2,6 Gbps
Taxa de transferência da VPN IPsec‡	4,7 Gbps	2,9 Gbps	2,6 Gbps
Máximo de sessões	2,2 M	2 M	1 M
Novas sessões por segundo§	94.400	63.700	52.800
Sistemas virtuais (base/máx)	1/6	1/6	1/6

Observação: os resultados foram medidos no PAN-OS 10.1.

PA-3260: (12) 10/100/1000, (8) 1G/10G SFP/SFP+, (4) 40G QSFP+
PA-3250: (12) 10/100/1000, (8) 1G/10G SFP/SFP+
PA-3220: (12) 10/100/1000, (4) 1G SFP, (4) 1G/10G SFP/SFP+

Comparando a linha 3400 x 3200 nota-se que a 3400 é bastante superior, sendo o modelo PA 3410 atendendo todos os requisitos com excelência, já a série 3200, seria necessário contratar o PA 3250, pois o PA 3220 possui configurações muito em cima da mínima necessário, tendo cara de que possivelmente ficaria devendo com o passar dos anos. Desta forma é sempre interessante prever uma capacidade extra do momento presente, pois trata-se de equipamento que devemos contar por muitos anos na

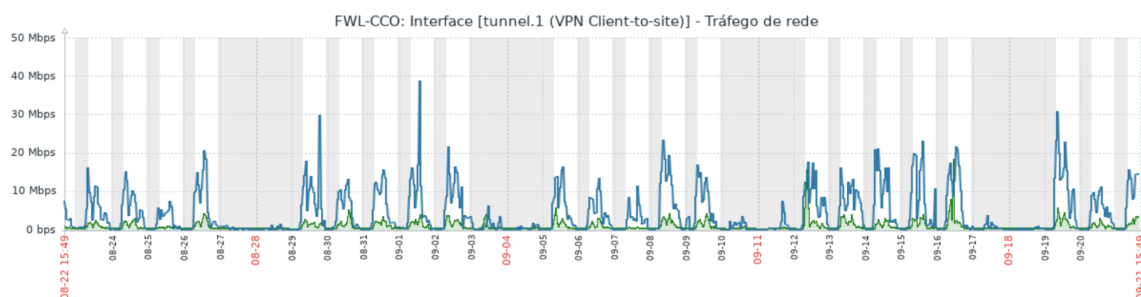


infraestrutura.

Outro dado importante é que o PA 3250 foi lançado em 2018, já o PA 3410 foi lançado em 2022, com o primeiro já completando 5 anos de mercado, é possível que já esteja na metade de seu ciclo de vida completo pelo fabricante, ou seja, o que reforça a tese de que teríamos um tempo de vida útil limitado deste equipamento.

Por fim, o ponto mais importante é que o novo equipamento, possui uma série de novas funcionalidades que no equipamento de 2018 precisa ser comprada, caso do Wildfire, ou que não existe, caso do DNS Security +. Prezando pela economicidade, pelo ciclo de vida e pelo ferramental tecnológico e de capacidade, caso se opte em ir pelo caminho da atualização tecnológica mantendo-se o fabricante, o modelo PA 3410 é o mais adequado para herdar a posição do equipamento hoje vigente PA 3020.

Outra aquisição que se provou necessária este ano é a licença de VPN, tendo em vista o número significativo de servidores que fazem uso do trabalho remoto, como é possível comprovar no gráfico de consumo de banda com VPN client to site abaixo:



Até 2019, antes da pandemia, este cenário era bastante limitado, ficando a alguns usuários da TI, o costume de se conectar para trabalhar de casa em situações emergenciais. Após a pandemia, o que se verifica é que este cenário híbrido de conexão local e remota através da VPN, é um cenário que todos os usuários já se habituaram, inclusive os alunos, que fazem uso da VPN para acessar periódicos e bibliotecas online que só permitem o acesso através de um IP da UFFS, ou seja, de casa o aluno se conecta na VPN para poder navegar com um IP como se estivesse presencialmente na UFFS, podendo assim acessar estes recursos para estudo e pesquisa. O mesmo vale para os servidores de outras áreas que não a tecnológica, já se acostumaram a de casa por conveniência e comodidade acessar os recursos que antes só era possível acessar fisicamente na UFFS.

Toda esta conveniência traz também riscos associados, como por exemplo, perdemos o controle dos endpoints que estão sendo utilizados para acessar a rede interna da UFFS. Dentro da UFFS, há um controle sobre os computadores que são disponibilizados na UFFS, desta forma há um controle mais rígido na rede, com o fortalecimento do advento do acesso remoto se faz necessário adquirir a licença de Global Protect que hoje é utilizada em sua versão gratuita, porém sem a capacidade de



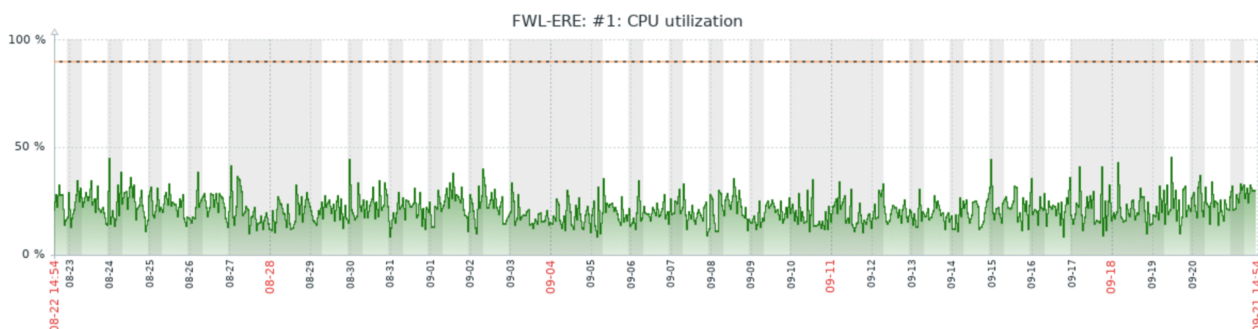
## UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

estabelecemos requisitos mínimos de segurança para que estes equipamentos acessem a informação sensível da universidade, sem que haja uma exposição dos dados e sistemas críticos da universidade.

Os PA 220 são os firewalls localizados no diversos campi da UFFS e já são equipamentos mais novos, que entraram na infraestrutura da universidade em 2019, tendo ainda pelo menos mais um ciclo de vida antes que seja avaliada a necessidade de troca destes equipamentos, note que o fim do ciclo de vida deste equipamento na figura acima está marcado para acontecer em 31.01.2028. A presente contratação prevê renovação até 2026, logo antes deste limite.

Olhando para os gráficos dos equipamentos, como no exemplo a seguir, consumo de CPU do firewall de Erechim, todas as medidas de consumo de importante medida estão abaixo de 50%. Não existe também nenhuma demanda física/de interface como ocorre com o PA 3020 que justifique a troca do equipamento neste momento. Portanto não se faz necessária a troca dos mesmos, apenas renovar as licenças e garantias destes.

### Firewall Erechim - Consumo de CPU (modelo PA 220)



O software de gerência centralizada destes equipamentos, conhecido como Panorama, também deve ter suas licenças de uso e garantias renovadas.

## 6. LEVANTAMENTO DE SOLUÇÕES

### 6.1. Análise de soluções

Considerando a estimativa de demanda e os requisitos da solução descritos anteriormente, verificou-se as características mínimas para o atendimento das demandas institucionais como:

- 1) Manter a padronização da tecnologia existente;
- 2) Adquirir nova tecnologia de outros fabricantes; ou
- 3) Terceirização através de um SOC (Security Operations Center – Centro de Operações de Segurança) ou estrutura equivalente onde a



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

função de firewall de borda é contratada como serviço.

Dessa forma, listam-se a seguir algumas soluções apresentadas como potenciais para um processo de contratação da solução;

## 6.2. Identificação das soluções

### Solução I: Atualização tecnológica e renovação da solução vigente

Aquisição de hardware para substituir o equipamento PA 3020 para um PA 3410 com aquisição da licença Global Protect para VPN. Renovação das licenças e garantias para 3 anos. Renovação do Panorama. Renovação das licenças PRORATA PA 3020 em 3 meses.

ID	Especificação Técnica	
1	Aquisição de Firewall PA-3410 para Data Center com licenças e garantias para 3 anos e Global Protect. Verificar licenças e serial numbers a ser renovado no Encarte A "Especificação Técnica da Solução"	Quantidade 01
2	PANORAMA RENOVAÇÃO SUPORTE GARANTIA 3 anos. Verificar licenças e serial number a ser renovado no Encarte A "Especificação Técnica da Solução"	Quantidade 01
3	Serviço de Instalação, Migração e Otimização das Configurações do PA-3020 para o PA-3410. Conforme descrito no Encarte C "Estudo Técnico Preliminar" do item 4.3.8 ao 4.3.12	Quantidade 01
4	Renovação de licenças/garantia dos Firewalls PA 220 dos 05 campi da UFFS em 3 anos. Verificar licenças e serial numbers a ser renovado no Encarte A "Especificação Técnica da Solução"	Quantidade 01
5	Renovação PA 3020 PRO RATA 3 meses. Verificar licenças e serial numbers a ser renovado no Encarte A "Especificação Técnica da Solução"	Quantidade 01

Além das renovações e trocas identificadas, por razões de segurança foi identificado a necessidade de fazer uma renovação das licenças do PA 3020 por três meses, a fim de cobrir duas situações: 1- colocá-lo em datas semelhantes de renovação com o Panorama e demais firewalls que está entre fim de fevereiro e março; e 2 - tempo hábil para chegada do hardware novo e conclusão do projeto de migração. Neste cenário,



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

manteríamos a rede da UFFS segura e atualizada durante todo o tempo, só ocorrendo a migração, após o encerramento destes 3 meses de PRO-RATA.

**Solução II: Aquisição de nova solução de segurança de rede**

Solução II: CISCO ou Fortigate

ID	Nome da Solução	Descrição da Solução
1	Aquisição de Firewall para Data Center	Aquisição da solução da Cisco ou Fortigate, com cinco appliances que atendam as configurações dispostas no item 1.2.1, respectivas licenças de defesa de ameaças, filtragem de URLs, para 3 anos
2	Aquisição de Firewall pra Campi Remoto	Aquisição da solução da Cisco ou Fortigate, com cinco appliances que atendam as configurações dispostas no item 1.2.2, respectivas licenças de defesa de ameaças, filtragem de URLs, para 3 anos
3	Aquisição de SW Gerenciador	Aquisição do software de gerenciador de firewalls da Cisco ou Fortigate que atendam as configurações dispostas no item 1.2.3
4	Serviço de Projeto, Instalação e Configuração	Serviço de Projeto, Instalação e Configuração.
5	Treinamento	Treinamento FTD - Cisco Firepower Threat Defense FTD NGFW & NGIPS

**Solução III:Terceirização da solução de segurança de rede**

Solução III: Algar

ID	Nome da Solução	Descrição da Solução
1	Gerência e Controle de Uso Interna Firewall, incluindo app control, Web Filtering, VPN, antispam. Por três anos. (Utiliza Fortigate)	Terceirização da solução de segurança da rede, totalmente provida pelo fornecedor. A solução de firewall inclui, app control, Web Filtering, VPN, antispam e antivírus. Por três anos.

ID	Descrição da solução (ou cenário)
1	Solução I: Atualização tecnológica e renovação da solução vigente
2	Solução II: Aquisição de nova solução de segurança de rede
3	Solução III: Terceirização da solução de segurança de Rede



## 7. ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do <a href="#">Software Público Brasileiro</a> ? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
A solução é uma alternativa existente no mercado?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A solução exigirá adequação do ambiente do órgão?	Solução 1		X	
	Solução 2	X		
	Solução 3	X		
A solução pode ser segmentada em pacotes passíveis de ser executada por fornecedores distintos?	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A solução é uma ampliação da solução implantada?	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A solução é a substituição da solução implantada?	Solução 1		X	
	Solução 2	X		
	Solução 3	X		
A solução possibilita a absorção do legado da solução implantada? (Caso existe solução implantada)	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A estimativa de preços da solução pode ser obtido de contratações de outros entes públicos?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Requisito	Solução	Sim	Não	Não se Aplica
A estimativa de preços da solução podem ser obtido no Painel de Preços?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A solução pertence ao catálogo de Soluções de TIC com Condições Padronizadas? Disponível em: <a href="https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic">https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic</a>	Solução 1		X	
	Solução 2		X	
	Solução 3		X	

Outro ponto relevante no comparativo de soluções é o último Gartner disponibilizado, onde a Palo Alto segue sendo a líder de mercado por anos consecutivos.

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (November 2021)



**ANÁLISE QUALITATIVA/ANÁLISE COMPARATIVA DE CENÁRIOS****7.1. Análise comparativa de cenários**

<b>Cenário</b>				
<b>Requisito</b>		<b>Solução I</b>	<b>Solução II</b>	<b>Solução III</b>
<b>Negócio</b>	Suporte nbd	atende	atende	atende
	Projeto de implantação de baixo impacto	atende	não atende	não atende
	Equipe local da UFFS qualificada na solução	atende	parcialmente	atende
	Líder de mercado	atende	não atende	não atende
<b>Tecnológico</b>	Melhoria da solução presente	atende	atende	atende
	Não necessita treinamento adicional em tecnologia	atende	não atende	atende
	Não impacta o usuário?	atende	não atende	atende
<b>Resultado da análise</b>		Atende em todos os quesitos	Não atende	Atende parcialmente

**7.2. Análise SWOT das alternativas****7.2.1. Solução I - Atualização tecnológica e renovação da solução vigente**

<b>ANÁLISE SWOT</b>	
<b>Análise da solução em relação às outras soluções</b>	<b>Análise dos impactos da adoção da solução</b>
<b>Vantagens</b>	<b>Oportunidades</b>
Já possui 6 anos no ambiente da UFFS com alto valor agregado de acoplamento e refinamento da solução com o ambiente da UFFS	Agregar novos serviços em uma versão estendida do que já possuímos, novas features como DNS Security e Wildfire, além da licença de Global Protect
Projeto de implantação de menor complexidade se comparado aos demais	Tornar o conhecimento na solução ainda mais completo



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Nenhuma indisponibilidade para os usuários	
Manutenção da qualidade já conhecida e aprovada pela equipe técnica	
Equipe altamente treinada na solução	
<b>Desvantagens</b>	<b>Ameaças</b>
Redução da concorrência	Concorrência superar o fabricante e se tornar o líder de mercado
	Alta dependência de um único fornecedor
	Possibilidade de custo mais alto em relação a outras soluções

7.2.2. Solução II - Aquisição de nova solução de segurança de rede

ANÁLISE SWOT	
Análise da solução em relação às outras soluções	Análise dos impactos da adoção da solução
<b>Vantagens</b>	<b>Oportunidades</b>
Novos paradigmas tecnológicos, logo novas oportunidades de aprendizado em arquiteturas diferentes	Vir a se tornar uma líder de mercado no futuro.
Equipamentos mais baratos	
<b>Desvantagens</b>	<b>Ameaças</b>
Maior tempo de projeto, de recursos materiais e humanos para chegar em um resultado igual ou potencialmente inferior.	Trocar o estado da arte em firewall por uma solução intermediária
Todos investimentos em equipamentos nos campi seriam perdidos e os mesmos ainda tem uma vida útil de mais de 3 anos.	Má qualidade de implementação
Recomeçar do zero significa perder 6 anos de inteligência de software	Efetividade da solução



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

construída na interação da equipe da UFFS com a ferramenta	
Necessidade de comprar treinamento formal na nova solução para toda a equipe	Não temos dados históricos sobre a confiabilidade do hardware para o acionamento de garantia, bem como se cumprem os prazos
Maior risco à segurança da rede, considerando a curva de aprendizado da ferramenta para otimização de seu uso	

7.2.3. Solução III: Terceirização da solução de segurança de rede

ANÁLISE SWOT	
Análise da solução em relação às outras soluções	Análise dos impactos da adoção da solução
<b>Vantagens</b>	<b>Oportunidades</b>
TI da UFFS pode se dedicar a outras atividades de planejamento	TI da UFFS pode criar novas soluções tecnológicas e de segurança com o tempo economizado em atividades de inspeção no firewall
Ter o parque sempre atualizado e com maior monitoramento humano	
Alto controle gerencial	
<b>Desvantagens</b>	<b>Ameaças</b>
Maior custo. Não há aproveitamento dos equipamentos em nosso inventário	Entregar para um terceiro todo o controle de tráfego da rede
Baixo controle técnico	Possível vazamento na rede do terceiro, poderia afetar a informação da UFFS
Confiança na efetividade das ações diminui, já que depende de um terceiro.	Em caso de rompimento de contrato, o parque da UFFS encontraria-se defasado.



## **8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS**

### **8.1. Solução II- Aquisição de nova solução de segurança de rede**

Mesmo que a solução II ofereça melhor custo por item, a mesma envolve uma maior aquisição de equipamentos, tendo em vista que nada do parque atual seria aproveitado. Ou seja, os custos de projeto ficariam bem mais elevados, necessitando a contratação de mais horas de projeto e o resultado seria na melhor das hipóteses equivalente ao já implantado hoje. Seria necessário contratar horas de treinamento para a equipe UFFS também. Não há dados históricos sobre a efetividade em nosso parque, bem como acionamentos de suporte e garantia. Em razão da eficiência, eficácia e efetividade da contratação, podemos descartar a solução.

### **8.2. Solução III- Terceirização solução de segurança de rede**

Envolve um alto grau de mudança de paradigma da gestão e dos técnicos, logo a instituição que vai por esta via precisa estar preparada tendo em vista sabendo onde vai e o que vai exigir do fornecedor. Ainda não desenvolvemos este tipo de cultura na SETI e entendemos que a gestão técnica de segurança da informação em nosso parque, sob a nossa guarda, é a confiável possível. Além do grau de confiabilidade que os terceiros não podem entregar se comparado aos servidores da casa, este tipo de solução envolve maiores custos, pois não se contrata apenas o uso dos equipamentos e software de terceiros, bem como seus recursos humanos. Desta forma, rejeitamos terceirizar a segurança de rede neste momento.

## **9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

### **9.1. Estimativa de custos das soluções Solução I**

A tabela a seguir apresenta a estimativa de custo da solução I para a aquisição de Atualização tecnológica e renovação da solução vigente.



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

item	Descrição	Unid	QTD	Preço Unitário I	Preço Unitário II	Preço Unitário III	Valor Unitário (médio)	Valor total
1	Firewall PA-3410 para Data Center	Un	1	R\$ 871.203,90	R\$ 700.413,00	R\$ 913.743,00	R\$ 828.453,30	R\$ 828.453,30
2	Panorama Renovação Suporte Garantia	Un	1	R\$ 40.678,90	R\$ 39.159,00	R\$ 42.511,00	R\$ 40.782,97	R\$ 40.782,97
3	Projeto de Instalação, Migração e Configuração do Firewall PA-3410	Un	1	R\$ 37.900,00	R\$ 33.195,00	R\$ 40.000,00	R\$ 37.031,67	R\$ 37.031,67
4	Renovação de licenças/garantia dos Firewalls PA 220 dos 05 campi da UFFS	Un	1	R\$ 100.141,50	R\$ 93.300,00	R\$ 104.306,50	R\$ 99.249,33	R\$ 99.249,33
5	Renovação Suporte Garantia Firewall PA 3020 PRO RATA	Un	1	R\$ 21.704,70	R\$ 19.913,00	R\$ 22.765,70	R\$ 21.461,13	R\$ 21.461,13
							<b>TOTAL</b>	<b>R\$ 1.026.978,40</b>



## 9.2. Cálculo dos custos totais de propriedade

<b>Solução Viável 1</b>
<b>Descrição: Atualização tecnológica e renovação da solução vigente</b>
<b>Custo Total de Propriedade – Memória de Cálculo</b>
As propriedades das licenças vem para o período de 3 anos, bem como equipamentos e garantias. Sendo assim, após encerrada a última atividade, que é o serviço de migração descrito no item 2, o pagamento total deverá ser efetuado, ainda no primeiro ano de contrato.

## 9.3. Mapa comparativo dos cálculos totais de propriedade (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
<b>Atualização tecnológica e renovação da solução vigente</b>	<b>R\$ 1.026.978,40</b>	<b>R\$ -</b>	<b>R\$-</b>	<b>R\$ 1.026.978,40</b>

## 10. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A solução escolhida será a de **atualização tecnológica e renovação da solução vigente**.

Aquisição de hardware para substituir o equipamento PA 3020 para um PA 3410 com aquisição da licença Global Protect para VPN. Renovação das licenças e garantias para 3 anos. Renovação do Panorama. Renovação das licenças PRORATA PA 3020 em 3 meses.

O equipamento PA 3020 seria o primeiro a receber as licenças em PRORATA para 3 meses. Na sequência haveria a renovação de licença do Panorama no fim de fevereiro de 2023, válido por 36 meses.

Então seriam ativadas as licenças de campi de março de 2023 para março de 2026, válidas por 6 meses. Até este momento não há intervenção técnica no ambiente apenas a atividade de gerar as licenças no site da Palo Alto e aplicá-las no Firewall. Ficando evidenciado que as licenças se estenderam para o período adquirido, bem como serviço de suporte e garantia PREMIUM SUPPORT, então é dado como concluído o projeto para estes itens.

A última etapa que deve ocorrer em março de 2023 é a chegada do novo firewall PA



UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

3410, recebimento da equipe de REDES da UFFS, estando tudo ok, realizar a configuração inicial de interfaces de gerenciamento e por fim fixá-lo no DATACENTER. Quando o equipamento estiver no ar, o CONTRATADO de forma remota deve executar todas as etapas que irão migrar as configurações do antigo PA 3020 (que neste momento ainda deve estar em PRODUÇÃO), deve ser feito todas as novas configurações de novas funcionalidades, conforme especificado neste documento e colocado no PANORAMA junto com os demais equipamentos. Ativação das licenças e por fim troca da produção, passando o PA 3410 a desempenhar esta função. Note que este é um overview de projeto, atividades específicas e possíveis necessidades aqui não contempladas serão alinhadas na reunião de KICK OFF do projeto entre CONTRATADA e CONTRATANTE.

Após a conclusão destas atividades e aceite por parte da UFFS, poderá ser dado ok para pagamento dos serviços de implantação e ativação do PA 3410. O que deve ocorrer até o fim de março em um cenário sem atrasos.

## 11. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

A estimativa de custos para a aquisição de equipamentos e acessórios para a solução de aulas interativas remotas é apresentada na tabela 11.1.

**Tabela 11.1 - Custo de contratação**

item	Descrição	Unid	QTD	Valor Unitário (médio)	Valor total
1	Firewall PA-3410 para Data Center	Un	1	R\$ 828.453,30	R\$ 828.453,30
2	Panorama Renovação Suporte Garantia	Un	1	R\$ 40.782,97	R\$ 40.782,97
3	Projeto de Instalação, Migração e Configuração do Firewall PA-3410	Un	1	R\$ 37.031,67	R\$ 37.031,67
4	Renovação de licenças/garantia dos Firewalls PA 220 dos 05 campi da UFFS	Un	1	R\$ 99.249,33	R\$ 99.249,33
5	Renovação Suporte Garantia Firewall PA 3020 PRO RATA	Un	1	R\$ 21.461,13	R\$ 21.461,13
				<b>TOTAL</b>	<b>R\$ 1.026.978,40</b>

## 12. Justificativa técnica da escolha da solução

- 12.1. Solução sem impacto para o usuário final, mantendo a disponibilidade de nossos serviços. Estado da arte no mercado de firewalls. Alto grau de conhecimento e estudos desenvolvidos ao longo de seis anos interagindo com a tecnologia.



**13. Justificativa econômica da escolha da solução**

- 13.1. Melhor custo-benefício, onde parte do parque se mantém, tendo a necessidade de contratação apenas de licenças e garantias. Custo com projeto diminuído. Custo com treinamento igual a zero.

**14. Benefícios a serem alcançados com a contratação**

- 14.1. Manutenção da segurança de borda de rede da UFFS. Melhorias das funcionalidades tecnológicas tornando a UFFS mais pronta para encarar novos desafios que tem sido impostos na administração pública, alvo frequente de ataques maliciosos e amplamente noticiado. Adaptação aos novos tempos e ao trabalho remoto.

**15. Providências a serem Adotadas**

- 15.1. A contratação deve ser planejada e acompanhada pela equipe de planejamento nas fases de planejamento e seleção de fornecedores conforme o disposto na IN SGD/ME nº 1/2019.
- 15.2. O recebimento de bens ou serviços que compõem a solução deve ser realizada por integrantes da equipe de planejamento responsável, se adotada a nota de empenho ao invés de contrato, ou pela equipe de gestão contratual a ser nomeada pela área institucional competente.

**16. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

**A Atualização tecnológica e renovação da solução vigente, através deste documento se provou a mais viável para contratação tendo como base os seguintes conceitos:**

- **Eficácia:** É a solução que menos impacta no ambiente, logo a mais pronta para ser fiel ao planejamento, com zero impacto aos usuários quanto a disponibilidade, integridade e autenticidade no uso da rede e dados da UFFS.
- **Eficiência:** É a única solução que aproveita os recursos físicos, materiais e de conhecimento existentes, mesmo que o custo por licença não seja o mais barato, quando se coloca na balança que estamos optando pela líder de mercado, o lugar onde as demais soluções pretendem chegar, quando lembramos que não precisa comprar equipamentos para os campi, pois os mesmos ainda estão com equipamentos dentro do ciclo de vida de atendimento do fabricante, quando não é necessário comprar muitas horas de projeto e/ou treinamento para a equipe interna é onde garantimos a economicidade da solução
- **Efetividade:** Seguindo um planejamento de longo prazo onde os recursos seguem sendo aproveitados e novos são incorporados granularmente, com alta agregação tecnológica e baixo custo de implantação.
- **Economicidade:** Pelas razões expressadas acima, é a solução que agrega o melhor custo-benefício.





## 17. ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pela PORTARIA Nº 711/PROAD/UFFS/2022, DE 10 DE FEVEREIRO DE 2022.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
<hr/> Neimar Marcos Assmann <b>Matrícula/SIAPE: 1944186</b>	<hr/> Flavio Humberto Testa <b>Matrícula/SIAPE: 2388204</b>
INTEGRANTE TÉCNICO	INTEGRANTE TÉCNICO
<hr/> Marcos Eugenio Dietrich <b>Matrícula/SIAPE: 2126948</b>	<hr/> Michel Arcari <b>Matrícula/SIAPE: 2165290</b>

## 10 – APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

<b>AUTORIDADE MÁXIMA DA ÁREA DE TIC</b> <b>(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)</b>
<hr/> Ronaldo Antonio Breda <b>Matrícula/SIAPE: 1827490</b>



Emitido em 13/10/2022

**F0091 - ESTUDOS TÉCNICOS PRELIMINARES Nº 23/2022 - SETI (10.53)**

(Nº do Protocolo: NÃO PROTOCOLADO)

*(Assinado digitalmente em 13/10/2022 18:35 )*

FLAVIO HUMBERTO TESTA

ANALISTA DE TEC DA INFORMACAO

DITI (10.53.05)

Matrícula: ###882#4

*(Assinado digitalmente em 14/10/2022 13:18 )*

MARCOS EUGENIO DIETRICH

TEC DE TECNOLOGIA DA INFORMACAO

DRT (10.53.05.02)

Matrícula: ###269#8

*(Assinado digitalmente em 14/10/2022 08:11 )*

MICHEL ARCARI

TEC DE TECNOLOGIA DA INFORMACAO

DRT (10.53.05.02)

Matrícula: ###652#0

*(Assinado digitalmente em 13/10/2022 22:45 )*

NEIMAR MARCOS ASSMANN

ANALISTA DE TEC DA INFORMACAO

DRT (10.53.05.02)

Matrícula: ###441#6

*(Assinado digitalmente em 14/10/2022 10:56 )*

RONALDO ANTONIO BREDAS

SECRETARIO - TITULAR

SETI (10.53)

Matrícula: ###274#0

Visualize o documento original em <https://sipac.uffs.edu.br/documentos/> informando seu número: **23**, ano: **2022**,  
tipo: **F0091 - ESTUDOS TÉCNICOS PRELIMINARES**, data de emissão: **13/10/2022** e o código de verificação:  
**66306a9a92**