UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

DOD Nº: 5/2018 - F9841 - PCTI: Estudo Técnico Preliminar

Processo nº 23205.101202/2018-12

INTRODUÇÃO

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, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. DEFINIÇÃO E ESPECIFICAÇÃO DE REQUISITOS

Renovar contratos de licenças, garantia, suporte e adquirir equipamentos de firewall para manter a infraestrutura de segurança de redes, atendendo as necessidades conforme Necessidade de Infraestrutura - NI do PDTIC 2016-2018. A solução deve prover as minímas funcionalidades:

- Permitir o bloqueio de ameaças à rede interna da UFFS;
- Permitir o bloqueio de ameaças ao DataCenter da UFFS;
- Filtro de ameaças;
- NGFW (next generation firewall);
- Identificação de usuário por meio do LDAP institucional;
- Interconexão das unidades (site-to-site) de forma segura através de VPN (Rede Privada Virtual) dinâmica;
- VPN client-to-site permitindo que pessoas acessem remotamente a rede interna da UFFS;
- Análise de tráfego em tempo real;
- Gerenciamento centralizado;
- Relatórios gerenciais customizáveis;
- Retenção de logs centralizado.

1.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Necessidades		**Funcionalidades**		**Atores envolvidos**	
Id	**Descrição da Necessidade**	**Id**	**Descrição da funcionalidade**	**Id**	**Atores envolvidos**
1	Renovação de licença, garantia e suporte do firewall PA 3020 **ou atualização tecnológica**, Threat prevention e URL Filtering	1	Contrato de licença, garantia e suporte para firewall modelo PA 3020 ou superior destinado à segurança de rede do datacenter da UFFS.	1	Equipe de planejamento
2	Renovação de licença, garantia e suporte de firewall PA 500 **ou atualização tecnológica**, Threat prevention e URL Filtering	2	Contrato de licença, garantia e suporte para firewall modelo PA 500 ou superior destinado à segurança de rede dos campis UFFS.	1	Equipe de planejamento
3	Licença e suporte do Software de Gerenciamento de Segurançca 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

1.2. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

1.2.1. **Contrato de licença, garantia e suporte de firewall modelo PA 3020 ou atualização tecnológica, Threat prevention e URL Filtering**

Na eventual necessidade de substituição de peças, as mesmas deverão possuir características idênticas as 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: 2 Gbps,
- Throughput de prevenção contra ameaças: 1 Gbps
- Throuput de VPN IPSec: 500 Mbps
- 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;

1.2.2. **Contrato de licença, garantia e suporte de firewall PA 500 ou atualização tecnológica, Threat prevention e URL Filtering:**

Na eventual necessidade de substituição de peças, as mesmas deverão possuir características idênticas as 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: 250 Mbps
- Throughput de prevenção contra ameaças: 100 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;

1.2.3.**Aquisição 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 politicas;
    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 por aplicações, URL, Ameaças, etc;
    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, alterarem 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 e padronização.
    1. Garantia de 36 (trinta e seis) meses com envio de peças/equipamentos de reposição em next business day;
    2. A ferramenta de gerenciamento de segurança deve ser compatível com os firewalls já existentes na instituição, sendo eles:
        1. Palo alto PA3020;
        2. Palo alto PA500.

1.2.4. **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.

1.3. **DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DE TIC**

1.3.1.**Requisitos de Capacitação**

Atualmente o quadro de servidores lotados no DRT (Departamento de Redes e Telecomunicações) 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.

1.3.2. **Requisitos Legais**

Há softwares envolvidos na descrição dos itens descritos na sessão 1.2 que possuem licença comercial ou educacional. Neste caso, aceita-se as que enquadrem-se no negócio da instituição.

1.3.3. **Requisitos de Garantia e 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.

1.3.3.1. **Contrato de renovação da licença, garantia e suporte de firewall modelo PA 3020 ou atualização tecnológica. 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 ("on-site") 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.

1.3.3.2. **Contrato de renovação da licença, garantia e suporte de firewall modelo PA 500 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 ("on-site") 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).

1.3.3.3. **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 suporte de hardware nas instalações do cliente ("on-site") 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).

1.3.4. **Requisitos Temporais**

1.3.4.1. **Contrato de renovação da licença, garantia e suporte de firewall modelo PA 3020 ou atualização tecnológica. Funcionalidades Threat prevention e URL Filtering**

O prazo de vigência deverá ser definido em reunião conjunta de implantação da solução.

1.3.4.2. **Contrato de renovação da licença, garantia e suporte de firewall modelo PA 500 ou atualização tecnológica. Funcionalidades Threat prevention e URL Filtering**

O prazo de vigência deverá ser definido em reunião conjunta de implantação da solução.

1.3.4.3. **Contrato de aquisição da licença, garantia e suporte de Gerenciamento Centralizado dos firewalls PANORAMA**

O prazo de vigência deverá ser definido em reunião conjunta de implantação da solução.

1.3.4.4. **Contrato de configuração da solução:**

O prazo de vigência deverá ser definido em reunião conjunta de implantação da solução.

1.3.5. **Requisitos de Segurança Física e da Informação**

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

1.3.5.2. **Segurança da informação:** Respeitar a política de segurança da informação e comunicação da UFFS (POSIC PORTARIA Nº 216/GR/UFFS/2018) vigente.

1.3.6. **Requisitos de Projeto, de Implementação e de Implantação**

Compatível com a solução atualmente implantada e de acordo com a solução escolhida.

1.3.7. **Requisitos de Transferência de Conhecimento**

Compatível com a solução atualmente implantada e de acordo com a solução escolhida.

1.3.8. **Requisitos de Formação e Experiência das Equipes**

Em caso de manutenção da solução não há necessidade. Em caso de troca para nova tecnologia é necessário capacitação formal na tecnologia.

1.3.9. **Requisitos Sociais, Ambientais e Culturais**

1.3.9.1. **Requisitos sociais**

A empresa deverá informar via declaração que não possui em seus quadros trabalhadores menores de dezoito anos executando atividades em trabalho noturno, perigoso ou insalubre, e de qualquer trabalho aos menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos, nos termos do disposto no inciso XXXIII do art. 7o da Constituição Federal e do art. 27, V da Lei no 8.666/93.

1.3.9.2. **Requisitos ambientais**

Em sua constante preocupação com a sustentabilidade ambiental e em atendimento às regulamentações oficiais, em especial a Instrução Normativa nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional, a UFFS institui que produtos a serem adquiridos, se for cabível:
I. Sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR 15.448-1 e 15.448-2.
II. Sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.
III. Sejam preferencialmente acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.
IV. Não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (do inglês: Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).
V. Possuir selo de eficiência energética.
VI. Apresentar maior vida útil.
VII. Apresentar menor custo de manutenção.
A comprovação do disposto acima, se necessário, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências definidas.

1.3.9.3. **Requisitos culturais**
A empresa contratada deverá realizar os serviços de suporte, se necessário, nos horários pactuados com a UFFS, respeitando a cultura, as normas e padrões de trabalho da autarquia e ética profissional.

1.4. **CENÁRIO ATUAL**

1.4.1. **Dois PA 3020, Funcionalidades** Threat prevention e URL Filtering.

Modelo
PAN-PA-3020
Serial
001801025607
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

Modelo
PAN-PA-3020
Serial
001801025623
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

1.4.2. **Cinco PA 500, Funcionalidades** Threat prevention e URL Filtering.

Modelo
PAN-PA-500-2GB
Serial
009401019652
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

Modelo
PAN-PA-500-2GB
Serial
009401020139
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

Modelo
PAN-PA-500-2GB
Serial
009401020195
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

Modelo
PAN-PA-500-2GB
Serial
009401020245
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

Modelo
PAN-PA-500-2GB
Serial
009401036410
Licenças
Threat Prevention
PAN-DB URL Filtering
Premium Support

1.4.3. **PANORAMA software de gerencia centralizada** em versão trial para administração dos equipamentos, configurações, elaborações de políticas e gestão de logs.

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

É preciso manter, no mínimo, a infraestrutura atual, já que a mesma atende na ordem de 65% dos recursos de hardware (extraído de https://noc.uffs.edu.br/). Para os campi remotos a vazão (throughput) fica na média de 60 Mbps, cerca de 23% da capacidade total dos equipamentos PA 500 e o número de sessões na ordem de 6000 mil simultâneas, na ordem de 10% da capacidade dos PA 500. Já para o PA 3020 a vazão da reitoria e campus Chapecó fica na ordem de 200 Mbps ou seja, 20% da capacidade do PA 3020 e as sessões na ordem de 45 mil simultâneas, também próximo de 20% de sua capacidade total. No entanto, os equipamentos PA 500 estão em fase de descontinuidade pelo fabricante o que inviabiliza a escalabilidade da solução de segurança em funcionamento na UFFS. Sendo assim, é viável a agregação de novo equipamento na solução que é o PA 220.

3. ANÁLISE DE SOLUÇÕES

3.1. Identificação das Soluções

3.1.1. Contratação de renovação da licença, garantia e suporte de firewall modelo PA 3020, PA 500 ou atualização tecnológica. Funcionalidades de Threat prevention e URL Filtering. Aquisição de Licença, garantia e suporte do Panorama

Solução I: Contrato de renovação da licença, garantia e suporte de firewall modelo PA 3020, PA 500 e Aquisição do Panorama

ID	Nome da Solução	Descrição da Solução
1	Renovação PA 3020, Threat Prevention, URL Filtering	Suporte e garantia premium de 3 anos para 2 PA-3020. Renovação da licença do Threat prevention por 3 anos para 1 PA 3020. Renovação da licença d solução, passa a ficar como hot spare, configurado e pronto para entrar no ambiente em caso de falha do ativo principal.
2	Renovação PA 500, Threat Prevention, URL Filtering	Renovação de 5 PA 500. Suporte e garantia premium de 3 anos para PA-500, renovação da licença do Threat prevention por 3 anos para PA500. Renovação
3	Contrato de licença, garantia e suporte PANORAMA	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 dispositivos, suporte de 3 anos

Solução II: Contrato de atualização tecnológica para PA 220, renovação de PA 3020 e Aquisição do Panorama

ID	Nome da Solução	Descrição da Solução
1	Suporte e garantia para dois equipamentos PA-3020	Suporte e garantia premium de 3 (três) anos para os dois equipamentos PA-3020
2	Renovação da licença de Threat prevention para um PA 3020	Renovação das licenças de Threat prevention por 3 (três) anos para um PA 3020
3	Renovação da licença de PANDB URL filtering para um PA 3020	Renovação da licença de PANDB URL filtering para um PA 3020
4	Aquisição de 5 PA 220, com garantia, suporte premium e licenças de PANDB URL Filtering e Threat Prevention	Aquisição de 5 (cinco) PA 220, incluindo: 4.1. Suporte e garantia premium de 3 (três) anos para PA-220; 4.2. Renovação da licença do Threat prevention por 3 (três) anos para PA220; e 4.3. Renovação da licença de PANDB URL filtering por 3 (três) anos para PA 220. 4.4 AC para fonte redundante
5	Serviço remoto de configuração da solução	Serviço remoto de configuração da solução
6	Contrato de licença, garantia e suporte PANORAMA	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 dispositivos

3.1.2. Aquisição de nova solução de segurança de rede

Solução III: 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 a
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 a
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	Servico de Projeto, Instalacao e Configuracao	Servico de Projeto, Instalação e Configuração.
5	Treinamento	Treinamento FTD - Cisco Firepower Threat Defense FTD NGFW & NGIPS

3.1.3. Terceirização da solução de segurança de rede

Solução IV: Algar

ID	Nome da Solução	Descrição da Solução
1	Gerencia e Controle de Uso Interna Firewall (FortiGate-500E), incluindo app control, Web Filtering, VPN, antispam. Por três anos.	Terceirização da solução de segurança da rede, totalmente provida pelo fornecedor. A solução de firewall inclui, app control, Web Filtering, VPN, antispam e an anos.

3.2. Análise Comparativa de Soluções

Solução I: Contrato de renovação da licença, garantia e suporte de firewall modelo PA 3020, PA 500 e Aquisição do Panorama

ID	Nome da Solução	Descrição da Solução	Fornecedor	

ID	Nome da Solução	Descrição da Solução	Fornecedor	
1	Renovação PA 3020, Threat Prevention, URL Filtering	Suporte premium de 3 anos para PA-3020, renovação da licença do Threat prevention por 3 anos para PA3020. renovação da licença de PANDB URL filtering para PA 3020. Para dois PA-3020	TechDec	R
2	Renovação PA 500, Threat Prevention, URL Filtering	Suporte premium de 3 anos para PA-500, renovação da funcionalidade do Threat prevention por 3 anos para PA500. renovação da funcionalidade de PANDB URL filtering para PA 500. Para cinco PA-500	TechDec	R$
3	Contrato de licença, garantia e suporte PANORAMA	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 dispositivos	TechDec	
				Tota

Solução II: Contrato de atualização tecnológica para PA 220, renovação de PA 3020 e Aquisição do Panorama

ID	Nome da Solução	Descrição da Solução	Fornecedor	
1	Suporte e garantia para dois equipamentos PA-3020	Suporte e garantia premium de 3 (três) anos para os dois equipamentos PA-3020	Approach, Teltec, TechDEC	
2	Renovação da licença de Threat prevention para um PA 3020	Renovação das licenças de Threat prevention por 3 (três) anos para um PA 3020	Approach, Teltec, TechDEC	
3	Renovação da licença de PANDB URL filtering para um PA 3020	Renovação da licença de PANDB URL filtering para um PA 3020	Approach, Teltec, TechDEC	
4	Aquisição de 5 PA 220, com garantia, suporte premium e licenças de PANDB URL Filtering e Threat Prevention	Aquisição de 5 (cinco) PA 220, incluindo: 4.1. Suporte e garantia premium de 3 (três) anos para PA-220; 4.2. Renovação da licença do Threat prevention por 3 (três) anos para PA220; e 4.3. Renovação da licença de PANDB URL filtering por 3 (três) anos para PA 220.	Approach, Teltec, TechDEC	
5	Serviço remoto de configuração da solução	Serviço remoto de configuração da solução	Approach, Teltec, TechDEC	
6	Contrato de licença, garantia e suporte PANORAMA	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 dispositivos	Approach, Teltec, TechDEC	

Os números apresentados na Solução 2, representam uma média dos orçamentos enviados pelos três fornecedores elencados na tabela acima.

3.2.1. **Aquisição de nova solução de segurança de rede**

Solução III: CISCO ou Fortigate

ID	Nome da Solução	Descrição da Solução	Fornecedor	
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	Teltec/Cisco ou ALTAS NETWORKS/Fortigate	
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	Teltec/Cisco ou ALTAS NETWORKS/Fortigate	
3	Aquisição de SW Gerenciador	Aquisição do SW gerenciador de firewalls da Cisco ou Fortigate que atendam as configurações dispostas no item 1.2.3	Teltec/Cisco ou ALTAS NETWORKS/Fortigate	R
4	Servico de Projeto, Instalacao e Configuracao	Servico de Projeto, Instalacao e Configuracao	Teltec/Cisco	
5	Treinamento	Treinamento FTD - Cisco Firepower Threat Defense FTD NGFW & NGIPS	Teltec/Cisco	
				Total:

Os números apresentados na Solução 3, representam uma média dos orçamentos enviados pelos dois fornecedores elencados na tabela acima.

3.2.2. **Terceirização da solução de segurança de rede**

Solução IV: Algar

ID	Nome da Solução	Descrição da Solução	Fornecedor	
1	Gerencia e Controle de Uso Interna Firewall (FortiGate-500E), incluindo app control, Web Filtering, VPN, antispam. Por três anos.	Terceirização da solução de segurança da rede, totalmente provida pelo fornecedor. A solução de firewall inclui, app control, Web Filtering, VPN, antispam e antivirus. O equipamento utilizado será o Fortigate 500-E. Por três anos.	Algar/Fortigate	R$ 20
2				Total: R

3.2.3. **Quadro Comparativo**

Requisito: A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	ID	Identificação da Solução	Sim	Não	Não se Aplica
	Contratação de renovação da licença, garantia e suporte de firewall modelo PA 3020, PA 500 ou atualização tecnológica. Aquisição de Licença, garantia e suporte do Panorama	Solução 1	x		
		Solução 2	x		
	Aquisição de nova solução de segurança de rede	Solução 3	x		
	Terceirização da solução de segurança de rede	Solução 4		x	

Requisito	Identificação da Solução	Sim	Não	Não se Aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	Solução 1	x		
	Solução 2	x		
	Solução 3	x		
	Solução 4		x	

Requisito	Identificação da Solução	Sim	Não	Não se Aplica
A solução é um software livre ou software público?	Solução 1		x	
	Solução 2		x	
	Solução 3		x	
	Solução 4		x	

Requisito	Identificação da Solução	Sim	Não	Não se Aplica
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING e e-MAG?	Solução 1			x
	Solução 2			x
	Solução 3			x
	Solução 4			x

Requisito	Identificação da Solução	Sim	Não	Não se Aplica
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	x		
	Solução 2	x		
	Solução 3	x		
	Solução 4	x		

Requisito	Identificação da Solução	Sim	Não	Não se Aplica
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução 1			x
	Solução 2			x
	Solução 3			x
	Solução 4			x

3.3. **Análise SWOT das alternativas**

3.3.1. Solução 1

ANÁLISE SWOT	
Análise da solução em relação as outras soluções	**Análise dos impactos da adoção da solução**
Vantagens	**Oportunidades**
Fabricante de boa reputação	Aprofundamento do corpo técnico na tecnologia, otimizando a gestão
Ambiente já implantado e em produção na UFFS	
Equipe técnica com experiência na tecnologia	
Solução atendeu bem o proposto nos últimos três anos	

Desvantagens	**Ameaças**
Falta de equipamento sobressalente	Falha de um equipamento e a necessidade de acionar a garantia, pode gerar indisponibilidade já que não existe sobressalente.
Equipamentos PA 500 estão defasados e possuem o fim da vida marcado para outubro de 2022	PA 500 sendo utilizados com baixa margem de sobra de Hardware, o que pode ser uma ameaça caso cresça além do esperado o cenário de utilização nos próximos 3 anos
Não é a solução mais econômica	

3.3.2. Solução 2

ANÁLISE SWOT	
Análise da solução em relação as outras soluções	**Análise dos impactos da adoção da solução**
Vantagens	**Oportunidades**
Fabricante de boa reputação	Possibilidade de melhorar a redundância de rede
Modernização	Redução do tempo de indisponibilidade em caso de desastre.
Equipe técnica com experiência na tecnologia	Aprofundamento do corpo técnico na tecnologia, otimizando a gestão
Superior a solução que atendeu bem nos últimos 3 anos	
Antigos equipamentos são aproveitados na solução	
Melhor preço	
Desvantagens	**Ameaças**
Em caso de falha dos equipamentos nos campi, o trânsito fica centralizado em Chapecó. Cenário mitigado com os novos links de 1Gbps e 200Mbps	Equipamentos antigos (PA 500) apresentarem falha de Hardware, não possibilitando a implementação da solução conforme previsto
Envolve a aquisição de novos equipamentos e a respectiva configuração o que aumentaria o tempo de implantação	

3.3.3. Solução 3

ANÁLISE SWOT	
Análise da solução em relação as outras soluções	**Análise dos impactos da adoção da solução**
Vantagens	**Oportunidades**
Solução que a principio atenderia a demanda com folga tecnológica	Expertise em novas soluções de firewall
Fabricantes de boa reputação	
Desvantagens	**Ameaças**
Tempo de implantação	Perda de funcionalidades no conjunto de políticas atuais
Preço	Implantação / projeto deficiente
Necessidade de capacitação do corpo técnico	Falta de conhecimento por parte do corpo técnico
Não integração com a tecnologia atual (perda do hardware legado)	
Retrabalho na readequação de políticas, estruturas e topologia	

3.3.4. Solução 4

ANÁLISE SWOT	
Análise da solução em relação as outras soluções	**Análise dos impactos da adoção da solução**
Vantagens	**Oportunidades**
Desonera a equipe técnica da gestão da solução	Conhecer novos métodos para gestão da segurança de rede
Desvantagens	**Ameaças**
Preço	Entregar a gestão de segurança de rede para terceiros
Perda do controle do ambiente	Acesso à informações sigilosas pela terceirizada
Não implementado na APF - Administração Publica Federal	

4.REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Conforme a análise desenvolvida no item 3, concluímos que as soluções 3 e 4 se mostram inviáveis para a UFFS.
As mesmas são inviáveis pelos seguintes motivos.
1 - Custo. A solução 4, de modo geral, é entre 30% e 50% mais cara que as soluções 1 e 2. A solução 3, de modo geral, é entre 50% e 100% mais cara que as soluções 1 e 2.
2 - Não aproveitamento do parque atual da UFFS, sucateamento prematuro.
3 - Necessidade de um projeto do zero para implantação da nova solução de firewall, o que é totalmente incoerente diante do fato que já possuímos uma solução que se provou atender muito bem as demandas da universidade.
4 - Maior quantidade ou mais longas paradas do ambiente de produção para implantação das novas tecnologias.
5 - Para a solução 4 ainda acrescenta-se o fato de não estar amplamente implementado na APF.

5. ANÁLISE COMPARATIVA DE CUSTOS

A análise de Custo Total de Propriedade (TCO – *Total Cost Ownership*) é um instrumento utilizado para analisar e subsidiar a escolha da solução sob o aspecto de custo estimado durante o ciclo de vida de cada solução. O CTO foi calculado com base no orçamento que se provou mais econômico, tanto na escolha tecnológica, solução 2, quanto ao fornecedor que enviou o orçamento de menor preço.

5.1. – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

5.1.1. Solução Viável 1: Contrato de renovação da licença, garantia e suporte de firewall modelo PA 3020, PA 500 e Aquisição do Panorama

CRONOGRAMA FÍSICO / FINANCEIRO

Item	DESCRIÇÃO DO SERVIÇO	VALOR TOTAL		MÊS 01		MÊS 02		MÊS 03		TOT
		R$	%	%	R$	%	R$	%	R$	R$
1	Suporte premium de 3 anos para PA-3020, renovação da licença do Threat prevention por 3 anos para PA3020. renovação da licença de PANDB URL filtering para PA 3020. Para dois PA-3020	280.648,28	54,01%	100,00%	280.648,28	0,00%	-	0,00%	-	280.648,28
2	Suporte premium de 3 anos para PA-500, renovação da funcionalidade do Threat prevention por 3 anos para PA500. renovação da funcionalidade de PANDB URL filtering para PA 500. Para cinco PA-500	167.358,59	32,21%	100,00%	167.358,59	0,00%	-	0,00%	-	167.358,59
3	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 dispositivos	71.620,92	13,78%	100,00%	71.620,92	0,00%	-	0,00%	-	71.620,92
	TOTAL	519.627,79	100,00%	100,00%	519.627,79	0,00%	-	0,00%	-	519.6

5.1.2. Solução Viável 2: Contrato de atualização tecnológica para PA 220, renovação de PA 3020 e Aquisição do Panorama

CRONOGRAMA FÍSICO / FINANCEIRO

Item	DESCRIÇÃO DO SERVIÇO	VALOR TOTAL		MÊS 01		MÊS 02		MÊS 03		TOT
		R$	%	%	R$	%	R$	%	R$	R$
1	Suporte e garantia premium de 3 (três) anos para os 2 (dois) equipamentos PA-3020.	111.610,65	26,62%	100,00%	111.610,65	0,00%	-	0,00%	-	111.610,65
2	Renovação das licenças de Threat prevention por 3 (três) anos para 1 (um) PA 3020.	39.170,79	9,34%	100,00%	39.170,79	0,00%	-	0,00%	-	39.170,79
3	Renovação da licença de PANDB URL filtering para 1 (um) PA 3020.	39.170,79	9,34%	100,00%	39.170,79	0,00%	-	0,00%	-	39.170,79
4	Aquisição de 5 (cinco) PA 220, incluindo: 4.1. Suporte e garantia premium de 3 (três) anos para PA-220; 4.2. Renovação da licença do Threat prevention por 3 (três) anos para PA220; e 4.3. Renovação da licença de PANDB URL filtering por 3 (três) anos para PA 220.	111.270,69	26,54%	0,00%	-	0,00%	-	100,00%	111.270,69	111.270,69
5	Serviço remoto de configuração da solução de firewall.	22.725,33	5,42%	0,00%	-		-	100,00%	22.725,33	22.725,33
6	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 (vinte cinco) dispositivos, incluindo suporte de 3 (três) anos.	95.303,27	22,73%	100,00%	95.303,27	0,00%	-	0,00%	-	95.303,27
	TOTAL	419.251,52	100,00%	68,04%	285.255,50	0,00%	-	45,44%	133.996,02	419.2

5.2. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

Item	DESCRIÇÃO DO SERVIÇO	VALOR TOTAL		MÊS 01		MÊS 02		MÊS 03		TOT
		R$	%	%	R$	%	R$	%	R$	R$
1	Solução Viável 1: Contrato de Renovação da licença, garantia, e suporte de firewalls modelo PA 3020, PA 500 e Aquisição do Panorama	519.627,79	100,00%	100,00%	519.627,79	0,00%	-	0,00%	-	519.627,79
2	Solução Viável 2: Contrato de atualização tecnológica para PA 220, revovação de PA 3020 e Aquisição do Panorama	419.251,52	100,00%	68,04%	285.255,50	0,00%	-	31,96%	133.996,02	419.251,52

6. **DESCRIÇÃO DA SOLUÇÃO JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA**

6.1. **SOLUÇÃO ESCOLHIDA**

A solução escolhida foi a SOLUÇÃO II - Contrato de aquisição para PA 220, renovação de PA 3020 e Aquisição do Panorama

Durante o estudo técnico preliminar, verificamos que atualização tecnológica do parque de PA 500 para os PA 220 se provou mais econômica do que a pura renovação dos PA 500, para todos os fornecedores consultados.

Além disso, os PA 500 estão em condições de fim de vida. Programado para 31.10.2022.

O PA 220 é a atualização tecnológica oficial do PA 500. O mesmo possui características superiores ao seu antecessor, como por exemplo:

1. Firewall Throughput de 500 Mbps
2. Threat Prevention Throughput 150 Mbps
3. IPsec VPN Throughput 100 Mbps
4. Fonte redundante

Como forma de aproveitar os antigos equipamentos, vamos adotar uma solução onde os PA 500 atuem como backup dos PA 220 em primary. A ideia é que os equipamentos fiquem configurados de forma que, em condições de indisponibilidade de um PA 220, o PA 500 assume automaticamente ou o mais próximo possível com comutação manual mínima ou nenhuma, e este PA 500 que assume, passa a direcionar o tráfego para o PA 3020 de Chapecó, através de VPN site-to-site, obrigando, temporariamente, o tráfego de entrada e saída da internet a passar pela filtragem do PA 3020.

Importante salientar que os PAs 220 também farão VPN site-to-site com Chapecó, mas apenas para utilização dos sistemas do Datacenter.

A unidade do Bom Pastor migrará para o campus Chapecó dentro do próximo ciclo desta renovação. Desta forma, a solução já é adequada com apenas uma licença ativa de URL Filtering e Threat Prevention. O segundo PA 3020 ficará de *spare* no Datacenter, com o contrato de suporte e garantia vigorando. O mesmo deve ser configurado de forma que fique pronto para entrar em serviço em caso de inoperância do PA 3020 de produção, com configurações de dispositivo, redes, políticas e objetos atualizadas. O plano de recuperação envolveria a troca de equipamentos e transferências das licenças para o equipamento de *spare* colocado no ar. É calculado neste cenário de catástrofe um *downtime* aproximado de 01h, como plano de contingência e recuperação operacional, enquanto a garantia é acionada. O cenário de HA seria o ideal e pretendido já que em situações de desastres o *downtime* de 01h não ocorreria. Diante das restrições orçamentárias, será escolhida a solução que se provar a melhor no aspecto econômico.

O novo cenário se desenha da seguinte forma:

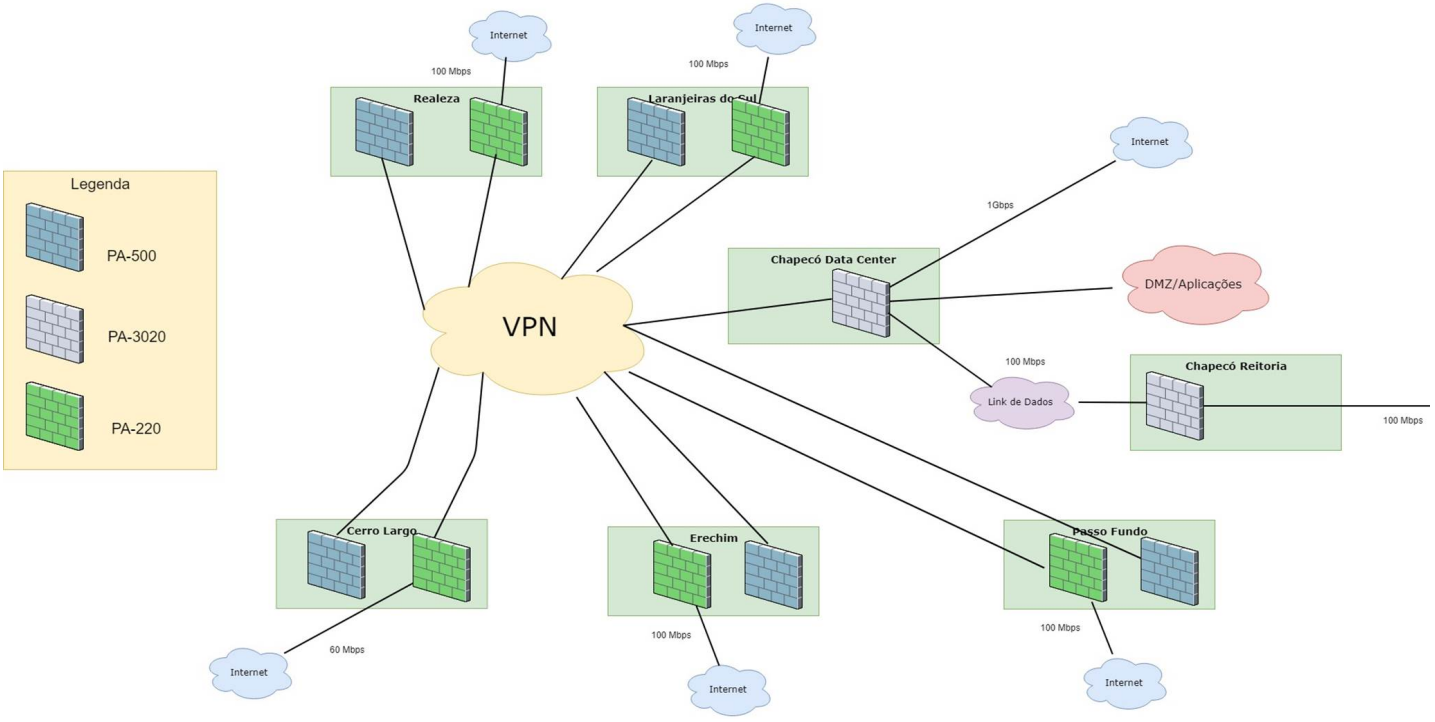
- Suporte premium de 3 anos para dois PA-3020

- Renovação da licença de Threat prevention por 3 anos para um PA 3020. renovação da licença de PANDB URL filtering para um PA 3020. Segundo PA 3020, na solução, passa a ficar como *hot spare*, configurado e pronto para entrar no ambiente em caso de falha do ativo principal.

- Aquisição de 5 PA 220 com o mesmo nível de licenças, suporte e garantia.

- Aquisição do Panorama para a gestão centralizada do ambiente

- Serviço de configuração remota deste cenário proposto (a equipe da UFFS daria o suporte local durante a implantação)



6.1.1. Bens e serviços que compõem a solução

Grupo	Item	Bem / Serviço	Unidade	Qtde
1	1	Suporte e garantia premium de 3 (três) anos para os dois equipamentos PA-3020	UND	2
	2	Renovação das licenças de Threat prevention por 3 (três) anos para um PA 3020	UND	1
	3	Renovação da licença de PANDB URL filtering por 3 (três) anos para um PA 3020	UND	1
	4	Aquisição de 5 (cinco) PA 220, incluindo: 4.1. Suporte e garantia premium de 3 (três) anos para PA-220; 4.2. Renovação da licença do Threat prevention por 3 (três) anos para PA220; e 4.3. Renovação da licença de PANDB URL filtering por 3 (três) anos para PA 220. 4.4 AC para fonte redundante	UND	5
	5	Serviço remoto de configuração da solução	UND	1
	6	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 (vinte cinco) dispositivos, suporte de 3 (três) anos	UND	1

O agrupamento dos itens em grupo/lote justifica-se pela possibilidade de responsabilização de um único fornecedor no momento da integração e funcionamento da solução, uma vez que, na hipótese de uma contratação separada, poderia se tornar difícil a identificação do responsável pela ocorrência de uma eventual falha na solução de segurança adquirida, pois cada fornecedor poderia alegar que a falha decorre de equipamento, software, ou componente fornecido pelo outro. A fim de obstar possíveis argumentos de transferência de responsabilidade, a Administração teria que se suprir com equipe técnica especializada capaz de fazer testes e identificar qual equipamento deu causa a cada ocorrência de falha, o que seria oneroso e demandaria nova contratação para a prestação de serviços terceirizados. Tal situação pode ser evitada com o agrupamento dos itens em lote, garantindo a contratação de um único fornecedor para prestar a solução e anulando possibilidades de transferência de responsabilidade entre fornecedores.

Ressalta-se ainda que esses riscos indesejáveis teriam que ser suportados, no mínimo, durante todo período do contrato, 3 (três) anos. A reunião em grupo transforma a garantia de funcionamento dos equipamentos em garantia de funcionamento da "solução", minimizando tais riscos.

6.2. **BENEFÍCIOS ESPERADOS**

6.2.1. Promover a segurança dos dados dos sistemas do *Data Center*, da rede interna da UFFS.

6.2.2. Promover o controle e monitoramento das rede UFFS, conforme disposto na POSIC.

6.2.3. Promover a rastreabilidade da rede UFFS, conforme disposto na POSIC.

6.2.4. Manter o uso da rede WAN da instituição (*Wide Area Network*), através de redes privadas de dados entre todos os campi da UFFS e a utilização do sistema autônomo da UFFS.

6.2.5. Suportar o crescimento institucional e a crescente demanda de usuários da rede.

7.**ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

GRUPO1						
Item	Catser/Catmat	Bem/Serviço	Unidade	Qtde	R$ Unitário	R$ Total
1	27090	Suporte e garantia premium de 3 (três) anos para os 2 (dois) equipamentos PA-3020.	Serviço	2	55.805,32	111.610,65
2	27502	Renovação das licenças de Threat prevention por 3 (três) anos para 1 (um) PA 3020.	Serviço	1	39.170,79	39.170,79
3	27502	Renovação da licença de PANDB URL filtering por 3 (três) anos para 1 (um) PA 3020.	Serviço	1	39.170,79	39.170,79
4	150100	Aquisição de 5 (cinco) PA 220, incluindo: 4.1. Suporte e garantia premium de 3 (três) anos para PA-220; 4.2. Renovação da licença do Threat prevention por 3 (três) anos para PA220; e 4.3. Renovação da licença de PANDB URL filtering por 3 (três) anos para PA 220.	Equipamento	5	22.254,13	111270,69
5	27090	Serviço remoto de configuração da solução de firewall.	Serviço	1	22.725,33	22725,33
6	27472	Software de Gerenciamento Centralizado dos firewalls - Panorama - até 25 (vinte cinco) dispositivos, incluindo suporte de 3 (três) anos.	Serviço	1	95.303,27	95.303,27
TOTAL						419.251,52

Os números aqui elencados representam uma média dos três fornecedores que enviaram orçamento. As evidências encontram-se em anexo a este documento.

8. **NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL**

8.1. O objetivo desta contratação é dar continuidade nos projetos de implantação da infraestrutura de TI nos campi da UFFS. Os ambientes que receberão estes equipamentos estão concluídos com toda a infraestrutura necessária de cabeamento, suporte elétrico e lógico necessário, incluindo no-break, rede elétrica estabilizada, alimentação e espaço para alocação destes equipamentos.

8.2. A infraestrutura de rede óptica interna nos campi da UFFS (Backbone) e também do DataCenter já esta concluída para os edifícios com construção finalizada.

9. **RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO**

9.1. **Recursos Materiais**

9.1.1. **Infraestrutura de cabeamento estruturado de rede.**

Quantidade: No âmbito de interconexão interna do espaço do *Datacenter/Salas de TI* e também de interconexão com o *backbone* do campus.

Disponibilidade: Permanente.

Ações Para Obtenção do Recurso e Seus Respectivos Responsáveis:

Tal recurso já está disponível no Datacenter/Salas de TI, tanto no que se refere a interconexão interna quanto a conexão dos prédios existentes ao backbone. Para as novas edificações o backbone apresenta disponibilidade de novas conexões.

9.1.2. **Salas adequadas para a instalação dos equipamentos.**

Quantidade: Uma sala de centralização do *backbone* em cada um dos campi da UFFS

Disponibilidade: Permanente.

Ações Para Obtenção do Recurso e Seus Respectivos Responsáveis:

A sala adequada diz respeito a espaço próprio para instalação de equipamentos, centralização do *backbone*, com recursos de climatização, rede elétrica estabilizada com garantia de não interrupção de fornecimento.

Atualmente as salas existentes contam com infraestrutura básica. O monitoramento do ambiente não está disponível, porém é interessante a análise de viabilidade para contratação de equipamentos para não interrupção de energia elétrica e monitoramento de condições de temperatura e umidade. Tal providência deverá ser prevista no plano de ações do próximo ano.

9.2. **Recursos Humanos**

9.2.1. **Técnico em Tecnologia da Informação**

Formação: Técnico em Tecnologia da Informação – Ênfase em redes.

Atribuições: Operação dos equipamentos e suporte técnico.

9.2.2. **Analista de Tecnologia da Informação**

Formação: Bacharel em Ciência da Computação ou área afim.

Atribuições: Configuração, manutenção e gestão das redes de dados.

10. **ESTRATÉGIA DE CONTINUIDADE CONTRATUAL**

10.1. **Atraso na entrega do material**

Setor do requisitante e Setor de Patrimônio notificam por escrito o fornecedor, e avaliam extensão do prazo. Não cumprindo-se, é encaminhado para o Setor Administrativo tomar as medidas de revogação da ordem de empenho e demais medidas cabíveis com o fornecedor, e se possível, realiza a chamada do segundo fornecedor na disputa licitatória.

10.2. **Atraso na instalação e configuração (motivado pelo fornecedor)**

Setor requisitante e SETI notificam por escrito o fornecedor e avaliam a extensão do prazo.

10.3. **Não conformidade do material entregue com as especificações da solução**

Setor do requisitante e Setor de Patrimônio notificam por escrito o fornecedor, apresentando as não conformidades e estabelecendo prazo para a adequação por parte do fornecedor. Não se cumprindo, é encaminhado para o Setor Administrativo tomar as medidas de revogação da ordem de empenho e demais medidas cabíveis com o fornecedor, e se possível, realiza a chamada do segundo fornecedor na disputa licitatória.

10.4. **Não atendimento dos prazos e formas no atendimento de garantia e suporte à solução.**

Setor do requisitante notifica por escrito o fornecedor, estabelecendo prazo para o atendimento. Não se cumprindo, é encaminhado para o Setor Administrativo tomar as medidas cabíveis na forma da lei.

11. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

Assim, diante do exposto acima, entendemos ser **VIÁVEL** a contratação da solução demandada.

12.**APROVAÇÃO E ASSINATURA**

A Equipe de Planejamento da Contratação foi instituída pela **PORTARIA Nº 75/PROAD/UFFS/2019**, de 28 de maio de 2019.

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:

Documento nato digital assinado eletronicamente por **CLAUNIR PAVAN**, **SECRETÁRIO ESPECIAL DE TECNOLOGIA E INFORMAÇÃO**, em 20/08/2019, às 11:48, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

Documento nato digital assinado eletronicamente por **FLAVIO HUMBERTO TESTA**, **Integrante Técnico**, em 20/08/2019, às 11:49, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

Documento nato digital assinado eletronicamente por **NEIMAR MARCOS ASSMANN**, **Integrante Requisitante**, em 20/08/2019, às 11:49, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

Documento nato digital assinado eletronicamente por **MARCOS EUGENIO DIETRICH**, **TECNICO DE TECNOLOGIA DA INFORMACAO**, em 20/08/2019, às 11:51, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

Documento nato digital assinado eletronicamente por **VOLNEI DARINO POL**, **Integrante Requisitante**, em 20/08/2019, às 12:58, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

Documento nato digital assinado eletronicamente por **RENATO TONELLO**, **Integrante Administrativo**, em 23/08/2019, às 11:34, conforme horário oficial de Brasília, com fundamento no art. 2º, da Portaria nº 154/GR/UFFS/2018, de 23 de fevereiro de 2018.

A autenticidade deste documento pode ser conferida no site http://sei.uffs.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0040354** e o código CRC **9C19C41A**.

Referência: Processo nº 23205.101202/2018-12 SEI nº 0040354