INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

Documentos dos participantes na licitação:

1. IFRN/Apodi;
2. IFRN/Caicó;
3. IFRN/Canguaretama;
4. IFRN/Currais Novos;
5. IFRN/Ipanguaçu;
6. IFRN/João Câmara;
7. IFRN/Macau;
8. IFRN/Mossoró;
9. IFRN/Natal Central;
10. IFRN/Nova Cruz;
11. IFRN/Parnamirim;
12. IFRN/Pau dos Ferros;
13. IFRN/Parelhas;
14. IFRN/Lajes;
15. IFRN/Santa Cruz;
16. IFRN/São Gonçalo do Amarante;
17. IFRN/São Paulo do Potengi.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/APODI

DOCUMENTAÇÃO DE PARTICIPAÇÃO

TERMO DE PARTICIPAÇÃO

IRP Nº 03/2022 – Aquisição de Material Permanente

UASG Gerenciador: 158368 – IFRN/*Campus* Zona Norte

UASG Participante: 158371 – IFRN/*Campus* Apodi

1. OBJETO

Atuação, como órgão participante, na licitação por Sistema de Registro de Preços a ser realizada pelo órgão gerenciador supracitado, cujo objeto contempla aquisição de material permanente (Firewall) que será utilizado no *Campus* Apodi do IFRN.

2. JUSTIFICATIVA

Esta solicitação de participação visa atender a necessidade de aquisição de firewall que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de *appliance*. Trata-se de um equipamento de segurança de rede, fundamental para garantir a confiabilidade das atividades acadêmicas e administrativas desenvolvidas em nossa unidade.

A aquisição se justificará também porque o equipamento atual que dispomos está sem licença e, por conseguinte, impossibilitado de usar todas as suas funcionalidades. O novo equipamento, no entanto, nos atenderá melhor porque sua capacidade de proteção e de atuação são superiores. A Coordenação de Tecnologia da Informação do *Campus* Apodi (CTI/AP) também informou que o equipamento que temos, o qual foi comprado há vários anos, carece de ser substituído por um modelo mais atual, tendo em vista o risco de ficar obsoleto com o passar do tempo e a modernização dos insumos de Tecnologia da Informação.

O decreto nº 7.892/2013 regulamenta o procedimento de Intenção de Registro de Preços a fim de permitir a aquisição de materiais/contratação de serviços para atendimento a mais de um órgão ou entidade, trabalhando de forma integrada aspectos técnicos da contratação, estimativas de consumo e minimização de tempo e custos, além de obter melhores preços junto ao mercado e maximizar o poder de compra da Administração Pública.

Além de melhorar a qualidade técnica dos procedimentos licitatórios, um planejamento integrado de contratação reduz a duplicidade de esforços entre as organizações interessadas e aperfeiçoa o trabalho dos gestores com ênfase nas atividades de aquisições, licitações e contratos, ensejando economia processual.

A tabela abaixo traz nossa demanda estimando, considerando os quantitativos mínimos e

máximos que pretendemos adquirir dentro da vigência da Ata de Registro de Preços:

ITEM	DESCRIÇÃO	QUANT. MÍN.	QUANT. MÁX.	VALOR UNT.	VALOR TOTAL
1	Compra de firewall que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance.	1	1	R$ 126.769,08	R$ 126.769,08

3. DEMONSTRATIVO DE NECESSIDADES/ESTIMATIVA DE CONSUMO

Conforme manifestado no SIASGnet, a quantidade solicitada bem como as justificativas para a participação está de acordo com a demanda pensada para nossa unidade, a ser adquirida dentro da vigência da ata e a depender da disponibilidade orçamentária.

A comprovação da nossa demanda teve como base uma consulta direta feita a CTI/AP. O setor apresentou sua necessidade, considerando o propósito de melhor atender alunos e servidores.

A Coordenação de Material e Patrimônio do *Campus* Apodi (COMPAT/AP) também foi consultada e informou que o Firewall que dispomos foi adquirido há vários anos, podendo estar próximo do fim de sua vida útil, e sujeito a vir a quebrar a qualquer momento.

O valor total estimado do item que pretendemos adquirir com o presente certame é da ordem de R$ 126.769,08 (cento e vinte seis mil, setecentos e sessenta e nove reais e oito centavos). Vale destacar que esse valor deverá ficar menor após o término do pregão. Vale destacar, ainda, que por se tratar de registro de preços nossa unidade pode comprar o item ou não, a depender da disponibilidade orçamentária.

4. LOCAL DE ENTREGA

ÓRGÃO: Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / *Campus* Apodi

ENDEREÇO COMPLETO: RN 233, Km 02, Sítio Lagoa do Clementino, S/N, Zona Rural | Apodi-RN | CEP: 59700-000|.

SETOR DE ENTREGA: ALMOXARIFADO.

TELEFONE PARA CONTATO: (84) 4005-4101 (ramal 6414, 6437)

E-MAIL: compat.ap@ifrn.edu.br

5. MANIFESTAÇÃO DE CONCORDÂNCIA

O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / *Campus* Apodi concorda com o objeto, aceita os prazos de entrega e as demais condições contidas no Termo de Referência do órgão gerenciador, bem como confirma os itens e quantidades informadas no sistema SIASGnet.

BRUNO JEFERSON L. A. S. OLIVEIRA
DIRETOR DE ADMINISTRAÇÃO – MAT: 1886690
CAMPUS APODI

LEONARDO DANTAS DOS SANTOS
DIRETOR-GERAL EM EXERCÍCIO – MAT 2209495
CAMPUS APODI

Apodi, 27 de junho de 2022

Estudo Técnico Preliminar - 32/2022

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Apodi, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitant	Responsável
Coordenação de Tecnologia da Informação	Francisco Jefferson Ferreira de Lima

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;
4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;
2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;
2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Apodi do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse

Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Apodi já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQBrasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual(exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens eserviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Apodi se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Apodi. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Apodi do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Renovar a solução atual**
2	**Firewall UTM**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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			
	Solução 2	X		
	Solução 3			
	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			
	Solução 2			
	Solução			X

	Solução 3			
	Solução 4			
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			

3 - COMPARAÇÃO DAS ALTERNATIVAS

Critérios	Justificativa para o critério	Avaliação da Alternativa 1	Avaliação da Alternativa 2	Avaliação da Alternativa 3
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Apodi, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-altonetworks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Apodi do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Apodi do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Apodi, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Apodi do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Apodi do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Apodi do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$

154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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	Ano 4	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Apodi do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$):126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de nternet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

FRANCISCO JEFFERSON FERREIRA DE LIMA
Membro requisitante / Coordenador de Tecnologia da Informação
Campus Apodi

GIRLEIDSON DE ALBUQUERQUE RODRIGUES
Integrante técnico / Coordenador de Tecnologia da Informação Substituto Eventual
Campus Apodi

BRUNO JEFERSON L. A. S. OLIVEIRA
Diretor de Administração do Campus Apodi

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/CAICÓ

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE PARTICIPAÇÃO - PREGÃO SRP

Ao IFRN campus Ceará-Mirim
UASG 158368 – IRP nº 03/2022

1 OBJETO
Aquisição de Solução de Firewall de Próxima Geração.

2 JUSTIFICATIVA DA NECESSIDADE

A presente manifestação de interesse em participação na IRP acima citada visa atender demandas do setor de Tecnologia da Informação do IFRN campus Caicó, no que se refere à aquisição de solução de firewall de próxima geração.

A necessidade se justifica em virtude da necessidade de adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014), manter a integridade dos dados e das informações sensíveis dos sistemas do campus além de melhorar o nível de qualidade ser serviço das aplicações internas do campus.

3 DA ENTREGA E DO RECEBIMENTO DO OBJETO
A entrega do material se dará conforme os seguintes dados:

IFRN Campus Caicó.

ENDEREÇO COMPLETO: RN 288, S/N, bairro Nova Caicó, Caicó/RN. CEP.: 59.300-000

CONTATO: (84) 4005-4102 / (84) 99600-0608 E-MAIL: licitacoes.ca@ifrn.edu.br ou diad.ca@ifrn.edu.br

4 DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

O quantitativo foi definido com base em levantamento de necessidade real, tendo como referência a análise do Setor de Tecnologia da Informação do campus.
Dessa forma, as quantidades solicitadas foram cadastradas no SIASGNET conforme abaixo:

N° do Item	Item	Unidade de Fornecimento	Valor Unitário Estimado (R$)	Quantidade	Valor total
01	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	Unidade	126.769,08	01	126.769,08

5 MANIFESTAÇÃO DE CONCORDÂNCIA COM AS CONDIÇÕES DO TERMO DE REFERÊNCIA
O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte – Campus Caicó, manifesta que aceita as condições contidas no Termo de Referência elaborado pelo IFRN Campus Ceará Mirim, tendo

como órgão gerenciador do certame o IFRN campus Natal Zona Norte

Tiago de Lima Wanderley
Matrícula SIAPE N° 1883737
Área requisitante

Elania Hortins Dantas
Matrícula SIAPE N° 2138986
Área Administrativa

Aprovo o presente documento e autorizo a adesão a referida IRP.

Francisco das Chagas Souza Junior
Matrícula SIAPE N° 2055569
Diretor Geral em exercício - Ordenador de Despesas
Campus Caicó.

Documento assinado eletronicamente por:

- **Tiago de Lima Wanderley, TEC DE TECNOLOGIA DA INFORMACAO**, em 27/06/2022 11:35:23.
- **Francisco das Chagas Souza Junior, DIRETOR GERAL - SUB-CHEFIA - DG/CA**, em 24/06/2022 15:02:00.
- **Elania Hortins Dantas, DIRETOR DE DIRETORIA - CD0004 - DIAD/CA**, em 24/06/2022 14:23:10.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418624
Código de Autenticação: 6ce677466f

Estudo Técnico Preliminar - 39/2022

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Adequação da infraestrutura de Tecnologia da Informação para interconexão a Rede Giga Caicó. Possibilitando o aumento considerável da banda de comunicação do Campus Caicó, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Tecnologia da Informação	Tiago de Lima Wanderley

4. Necessidades de Negócio

A presente manifestação de interesse em participação na IRP acima citada visa atender demandas do setor de Tecnologia da Informação do IFRN campus Caicó, no que se refere à aquisição de solução de firewall de próxima geração.

A necessidade se justifica em virtude da necessidade de adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014), manter a integridade dos dados e das informações sensíveis dos sistemas do campus além de melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

A presente aquisição vida gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

A aquisição ainda irá aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição, além de permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Caicó em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Rede Giga Caicó, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	2

Serão demandados duas unidades em virtude também do atendimento ao campus Avançado Jucurutu.

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Caicó se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Caicó. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS;

Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Caicó. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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			
	Solução 3			
	Solução 4			
	Solução 1			

A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Caicó.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Caicó, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Caic, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Caicó, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Caicó, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Caicó do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para instituição.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Caicó através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00

150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Caicó do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 253.538,00

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	02	R$126.769,08	R$253.538,16
Total				R$253.538,16

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado

neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Considerando o apresentado nesse Estudo Técnico Preliminar, quanto às necessidades das soluções disponíveis, das providências quanto aos possíveis impactos ambientais apontados e da estimativa de valor para aquisição, é viável a participação no processo licitatório de registro de preço, com adjudicação por item.

19. Responsáveis

Como membro da parte demandante da contratação, informo necessidade e ser viável a presente contratação.

ELANIA HORTINS DANTAS

Assistente em Administração- Diretoria de Administração

Como setor demandante da contratação, informo necessidade e ser viável a presente contratação.

TIAGO DE LIMA WANDERLEY

TEC DE TECNOLOGIA DA INFORMACAO

Como Ordenador de Despesa, aprovo o presente Estudo Técnico Preliminar, que dará base a contratação pleiteada.

FRANCISCO DAS CHAGAS SOUZA JUNIOR

Professor -Diretor Geral em exercício

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

ETP DIGITAL Nº 39/2022.

OBJETO: Aquisição de Solução de Firewall de Próxima Geração.

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)
Elania Hortins Dantas
Matrícula SIAPE nº 2138986
Membro Administrativo

(assinado digitalmente)
Tiago de Lima Wanderley
Matrícula SIAPE nº 1883737
Membro Técnico

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o presente Estudo Técnico Preliminar, considerando que o objeto da contratação está claro e justificado; os requisitos relevantes da contratação foram adequadamente relacionados e analisados; a análise de mercado foi devidamente realizada e demonstrou haver boa capacidade em atender ao objetivo da contratação; o modelo de prestação de serviços sugerido é apropriado e plenamente compatível com a Instituição, especialmente do ponto de vista legal; os riscos e impactos relevantes foram satisfatoriamente levantados e considerados no planejamento. Portanto, demonstra a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de Aquisição de Solução de Firewall de Próxima Geração.

Caicó, 24 de junho de 2022.

(assinado digitalmente)
Francisco das Chagas Souza Junior.
Diretor Geral campus Caicó - *em exercício*.

Documento assinado eletronicamente por:

- **Tiago de Lima Wanderley, TEC DE TECNOLOGIA DA INFORMACAO**, em 27/06/2022 11:36:02.
- **Elania Hortins Dantas, DIRETOR DE DIRETORIA - CD0004 - DIAD/CA**, em 24/06/2022 14:52:15.
- **Francisco das Chagas Souza Junior, DIRETOR GERAL - SUB-CHEFIA - DG/CA**, em 24/06/2022 15:01:25.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418656
Código de Autenticação: dc269a75a7

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/CANGUARETAMA

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS CANGUARETAMA
Diretoria de Administração

TR 11/2022 - DIAD/DG/CANG/RE/IFRN

27 de junho de 2022

TERMO DE PARTICIPAÇÃO

MANIFESTAÇÃO DE INTERESSE EM PARTICIPAR DA IRP N° 03/2022
UASG 158368 - INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

1. TERMO DE ABERTURA

Esta Unidade Gestora, **Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Campus Canguaretama, UASG 154839**, em atendimento ao que preconiza o Art. 6° do Decreto n° 7.892/2013, manifesta total concordância com o serviço a ser licitado **"Aquisição de material permanente para os campi do IFRN com a finalidade de suprir as demandas do campus"**, bem como todas as condições a serem estabelecidas no Termo de Referência do IFRN (UASG 158368) e edital desta licitação.

2. JUSTIFICATIVA DA NECESSIDADE

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corroborativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas tiara vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Canguaretama.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

3. LOCAIS DA PRESTAÇÃO DO SERVICOS E ENTREGA DOS MATERIAIS

IFRN - Campus Canguaretama – BR 101, KM 159, S/N, Areia Branca, Canguaretama/RN. CEP: 59.190-000

4. DEMONSTRATIVO DAS NECESSIDADES

A demanda evidenciada pela equipe de tecnologia da informação do Campus tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garanta do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Termo de Manifestação elaborado por:

Assinado eletronicamente
Fabiana Melo de Araújo
Diretora Administrativa
IFRN – Campus Canguaretama

5. DESPACHO DOS ORDENADORES DE DESPESAS

Diante do Demonstrativo de Necessidade apresentado:
1. Aprovo o presente documento;
2. Autorizo o início dos procedimentos para adesão/manifestação na IRP citada.

Canguaretama/RN, 27/06/2022

Marcio Marreiro das Chagas
Diretor-Geral em exercício

Campus Canguaretama

Documento assinado eletronicamente por:

- **Marcio Marreiro das Chagas, DIRETOR GERAL - SUB-CHEFIA - DG/CANG**, em 27/06/2022 14:22:56.
- **Fabiana Melo de Araujo, DIRETOR - CD0004 - DIAD/CANG**, em 27/06/2022 14:00:37.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419042
Código de Autenticação: e301341177

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS CANGUARETAMA
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/CANG/RE/IFRN

27 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Eliel Assuncao	**Matrícula/SIAPE:**	1674218
E-mail:	eliel.assuncao@ifrn.edu.br	**Telefone**	(84) 4005-4114

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Eliel Assuncao	**Matrícula/SIAPE:**	1674218
Cargo:	Técnico Laboratório Área Sistema da Computação	**Lotação:**	CTI/CANG
E-mail:	eliel.assuncao@ifrn.edu.br	**Telefone**	(84) 4005-4114

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Eliel Assuncao

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Aquisição de solução de firewall que se adeque às necessidades do Campus Canguaretama

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;

O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Canguaretama do IFRN. O equipamento de firewall em operação é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Canguaretama.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023,

fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; e, ainda, que o atual equipamento está trabalhando no limite do processamento, limitando consideravelmente o desempenho do equipamento e consequentemente o tempo de resposta aos usuários da rede do *Campus.*

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Canguaretama;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Eliel Assuncao - Matrícula 1674218.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Eliel Assuncao	**Matrícula/SIAPE:**	1674218
Cargo:	Técnico Laboratório Área Sistema da Computação	**Lotação:**	CTI/CANG
E-mail:	eliel.assuncao@ifrn.edu.br	**Telefone**	(84)4005-4114

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Eliel Assuncao - SIAPE 1674218

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Salmon Carlos Vitorino	**Matrícula/SIAPE:**	1761954
Cargo:	Tecnólogo-Formação	**Lotação:**	COFINC/CANG
E-mail:	salmon.vitorino@ifrn.edu.br	**Telefone**	(84)4005-4114

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Salmon Carlos Vitorino - Matrícula 1761954.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Flávio Rodrigo Freire Ferreira - Matrícula 1938035

Documento assinado eletronicamente por:

- **Eliel Assuncao**, **COORDENADOR - SUB-CHEFIA - CTI/CANG**, em 27/06/2022 09:49:22.
- **Salmon Carlos Vitorino**, **TECNOLOGO-FORMACAO**, em 27/06/2022 10:07:03.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418693
Código de Autenticação: 4de10d21c6

Estudo Técnico Preliminar - 12/2022

1. Informações Básicas

Número do processo: 23516.000319.2022-44

2. Descrição da necessidade

Aquisição de solução de firewall que se adeque às necessidades do Campus Canguaretama.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Eliel Assunção

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Canguaretama do IFRN. O equipamento de firewall em operação é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Canguaretama.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; e, ainda, que o atual equipamento está trabalhando no limite do processamento, limitando consideravelmente o desempenho do equipamento e consequentemente o tempo de resposta aos usuários da rede do *Campus.*

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

- A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;
- As alternativas do mercado;
- A existência de software público brasileiro;
- As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;
- As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);
- A possibilidade de aquisição na forma de bens ou contratação como serviço;
- Os diferentes modelos de prestação do serviço;

- Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

- A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Canguaretama se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance;

Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS;

Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- ANÁLISE COMPARATIVA DE SOLUÇÕES				
Requisito	**Solução**	**Sim**	**Não**	**Não se aplica**
	Solução			

A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1			
	Solução 2	X		
	Solução 3			
	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			
	Solução 2			X
	Solução			

	3			
	Solução 4			
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução			

	2			
	Solução 3			
	Solução 4			
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			

3 - COMPARAÇÃO DAS ALTERNATIVAS

Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Canguaretama, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) será descontinuada pela Palo Alto em agosto de 2023. 2) A demanda de requisições dos usários está sobrecarregando a capacidade de processamento da atual caixa (PA-500), comprometendo o seu desempenho, pois se observa no monitoramente que o mesmo trabalha em grande parte do tempo no limite da sua capacidade 3) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença).

Solução 2: Firewall UTM

Para atender as necessidades do Campus Canguaretema do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Canguaretama, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus acima de 100Mbs (limite da caixa PA-500).

E por fim, com o intuito de proteger os investimentos do Campus Canguaretama do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Canguaretama.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1

Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Canguaretama do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL /SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05

/2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	D A T A HOMOLOGAÇÃO	R$

154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Canguaretama do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

ELIEL ASSUNÇÃO
Técnico de Laboratório

SALMON CARLOS VITORINO
Tecnólogo em Gestão Pública

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

PROCESSO Nº 23516.000319.2022-44

Estudo preliminar 12/2022 - DIAD/DG/CANG/RE/IFRN

OBJETO: Solução de firewall de próxima geração

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)
Eliel Assunção
Matrícula SIAPE nº 1674218
Membro Técnico

(assinado digitalmente)
Salmon Carlos Vitorino
Matrícula SIAPE nº 1761954
Membro Administrativo

(assinado digitalmente)
Márcio Marreiro das Chagas
Matrícula SIAPE nº 162456

Diretor de Geral - Substituto Eventual

Documento assinado eletronicamente por:

- **Eliel Assuncao**, **COORDENADOR - SUB-CHEFIA - CTI/CANG**, em 27/06/2022 13:22:46.
- **Marcio Marreiro das Chagas**, **DIRETOR GERAL - SUB-CHEFIA - DG/CANG**, em 27/06/2022 13:28:46.
- **Salmon Carlos Vitorino**, **TECNOLOGO-FORMACAO**, em 27/06/2022 13:18:46.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419046
Código de Autenticação: b7beb7e5eb

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/CURRAIS NOVOS

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE PARTICIPAÇÃO - PREGÃO SRP

IRP nº IRP 03/2022 – **Aquisição de solução de firewall de próxima geração do Campus Zona Norte**

UASG Gerenciador: 158368 – **IFRN - Campus Zona Norte**

UASG Participante: 158366 – **Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / *Campus* Currais Novos.**

1 OBJETO

1.1 Atuação, como órgão participante, na licitação por Sistema de Registro de Preços a ser realizada pelo **Campus Zona Norte**, cujo objeto contempla a aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede do IFRN/*Campus* Currais Novos.

2 JUSTIFICATIVA DA NECESSIDADE

2.1 Esta solicitação de participação visa atender às necessidades de gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs do IFRN/Campus Currais Novos.

2.2 O decreto nº 7.892/2013 regulamenta o procedimento de Intenção de Registro de Preços a fim de permitir a aquisição de materiais/contratação de serviços para atendimento a mais de um órgão ou entidade, trabalhando de forma integrada aspectos técnicos da contratação, estimativas de consumo e minimização de tempo e custos, além de obter melhores preços junto ao mercado e maximizar o poder de compra da Administração Pública;

2.3 Além de melhorar a qualidade técnica dos procedimentos licitatórios, um planejamento integrado de contratação reduz a duplicidade de esforços entre as organizações interessadas e aperfeiçoa o trabalho dos gestores com ênfase nas atividades de aquisições, licitações e contratos, ensejando economia processual.

3 DA ENTREGA E DO RECEBIMENTO DO OBJETO

ÓRGÃO: Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / Campus Currais Novos.

ENDEREÇO COMPLETO: Rua Manoel Lopes Filho, nº 773. Valfredo Galvão | Currais Novos-RN | CEP: 59380-000

SETOR DE ENTREGA: COORDENAÇÃO DE ALMOXARIFADO

TELEFONE PARA CONTATO: (84) 4005-4103

4 DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

4.1 Conforme manifestado no SIASGnet, a solicitação está de acordo com as seguintes tabelas:

4.1.1 Descrições, quantidades e valores:

ITENS	DESCRIÇÃO	UND	QTD TOTAL	VALOR MÁXIMO ACEITÁVEL	VALOR TOTAL
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	UND	1	R$ 126.769,08	R$ 126.769,08
TOTAL					R$ 126.769,08

4.1.2 O valor total dos itens é de **R$ 126.769,08 (cento e vinte e seis mil, setecentos e sessenta e nove reais e oito centavos);**

4.1.3 O quantitativo de material foram calculados com base nas demandas do setor CTI/CN do Campus Currais Novos e adequação da infraestrutura de TI para interconexão a Rede Infovia Potiguar. Possibilitando o aumento considerável da banda de comunicação do Campus Currais Novos, que sairá de 100Mbps para 1Gbps.;

4.1.4 O equipamento não têm empenho formalizado ou pregão vigente para contratação, sendo necessário o registro de preços para atendimento da demanda.

5 MANIFESTAÇÃO DE CONCORDÂNCIA COM AS CONDIÇÕES DO TERMO DE REFERÊNCIA

5.1 O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / Campus Currais Novos concorda com o objeto, aceita as condições contidas no Termo de Referência do órgão gerenciador, bem como confirma o item e quantidade informada no sistema SIASGnet.

Currais Novos/RN, 27 de Junho de 2022.

_____

Fábio Felix de França
Coordenador de Tecnologia da Informação
Matrícula 1851847

6. MANIFESTAÇÃO DE CONCORDÂNCIA

6.1 Aprovo o presente documento e autorizo a formalização da participação em IRP.

_____

Andreilson Oliveira da Silva (1816404)
Diretor Geral

Documento assinado eletronicamente por:

- **Fabio Felix de Franca**, **COORDENADOR - FG0002 - CTI/CN**, em 27/06/2022 10:48:35.
- **Andreilson Oliveira da Silva**, **DIRETOR GERAL - CD0002 - DG/CN** , em 27/06/2022 10:49:43.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418996
Código de Autenticação: f8e1f27674

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS CURRAIS NOVOS
Coordenação de Tecnologia da Informação

DOD 2/2022 - CTI/DG/CN/RE/IFRN

27 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Fábio Felix de França	**Matrícula/SIAPE:**	1851847
E-mail:	fabio.felix@ifrn.edu.br	**Telefone**	(84) 4005-4103

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Fábio Felix de França	**Matrícula/SIAPE:**	1851847
Cargo:	Assistente em Administração	**Lotação:**	CTI/CN
E-mail:	fabio.felix@ifrn.edu.br	**Telefone**	(84) 4005-4103

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para interconexão a Rede Infovia Potiguar. Possibilitando o aumento considerável da banda de comunicação do Campus Currais Novos, que sairá de 100Mbps para 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
Objetivos Estratégicos	**Nome do documento <vigência>**

GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade;	**M30**	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes.

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Currais Novos do IFRN. O equipamento de firewall em operação é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do Campus Currais Novos.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, integrando-se a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Currais Novos;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos

continuados; PI: **L20RLP60MCN**; - Conta Corrente SIAFI: **171168810000000000449052.**

ENCAMINHAMENTO
Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências. **Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda**

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO			
Nome:	Fábio Felix de França	**Matrícula/SIAPE:**	1851847
Cargo:	Assistente em Administração	**Lotação:**	CTI/CN
E-mail:	fabio.felix@ifrn.edu.br	**Telefone**	(84)4005-4103

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação**

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Edson Artefio de Medeiros	**Matrícula/SIAPE:**	1831955

Cargo:	Assistente em Administração	**Lotação:**	DIAD/CN
E-mail:	edson.artefio@ifrn.edu.br	**Telefone**	(84)4005-4103

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento

Documento assinado eletronicamente por:

- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 27/06/2022 10:23:35.
- **Fabio Felix de Franca**, **ASSISTENTE EM ADMINISTRACAO**, em 27/06/2022 08:59:39.
- **Edson Artefio de Medeiros**, **DIRETOR DE DIRETORIA - CD0004 - DIAD/CN**, em 27/06/2022 09:01:51.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418538
Código de Autenticação: 0f6f2e6845

Estudo Técnico Preliminar - 17/2022

1. Informações Básicas

Número do processo: 23035.001808.2022-26

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede Infovia Potiguar. Possibilitando o aumento considerável da banda de comunicação do Campus Currais Novos, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Fábio Felix de França

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Currais Novos do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de

interligação desse Campus à Rede Infovia Potiguar, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Currais Novos já dispõe de uma solução de firewall da Palo Alto. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Currais Novos se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Currais Novos. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Currais Novos do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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 Solução 2 Solução 3 Solução 4	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3			X

	Solução 4			
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Currais Novos, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Currais Novos do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Currais Novos do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Currais Novos, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Currais Novos do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Currais Novos do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Currais Novos do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00

150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Currais Novos do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado

neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas

ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade

19. Responsáveis

Aprovação válida com assinatura eletrônica do Integrante Requisitante e Técnico neste documento

FABIO FELIX DE FRANCA
MEMBRO REQUISITANTE / INTEGRANTE TÉCNICO

Fabio Felix de Franca:04432256486 Assinado de forma digital por Fabio Felix de Franca:04432256486 Dados: 2022.06.24 18:16:59 -03'00'

Aprovação válida com assinatura eletrônica da Autoridade Máxima da Área de TIC conforme Portaria nº 657/2022 - RE/IFRN.

ANDRE GUSTAVO DUARTE DE ALMEIDA
DIRETOR DE GESTÃO DE TI

Documento Digitalizado Público

ETP Digital - 17/2022 Aquisição de Solução de Firewall para o Campus Currais Novos

Assunto: ETP Digital - 17/2022 Aquisição de Solução de Firewall para o Campus Currais Novos
Assinado por: Fabio Felix
Tipo do Documento: Estudo preliminar - contratos
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original e Cópia Autenticada Administrativamente

Documento assinado eletronicamente por:

- **Fabio Felix de Franca**, **COORDENADOR - FG2 - CTI/CN**, em 24/06/2022 18:31:17.

Este documento foi armazenado no SUAP em 24/06/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1105461
Código de Autenticação: 181c6ddfbe

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/IPANGUAÇU

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE PARTICIPAÇÃO - PREGÃO SRP

Ao **IFRN - CAMPUS NATAL ZONA NORTE**
UASG **158368**– IRP nº 03/2022

1. TERMO DE ABERTURA

Esta Unidade Gestora, em atendimento ao que preconiza o Art. 6° do Decreto n° 7.892/2013, manifesta total concordância com o objeto a ser licitado, bem como todas as condições estabelecidas no Termo de Referência do **IFRN - Campus Natal Zona Norte** (UASG 158368), referente a **IRP n° 03/2022**, cujo objeto é o Registro de preços para **Compra de firewall que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance.**, sujeitas ao Termo de Referência e edital da UASG gerenciadora. Com a finalidade de atender as demandas da CTI/IFRN/Campus Ipanguaçu UASG 158367.

2. JUSTIFICATIVA DA NECESSIDADE

O decreto n ° 7.892, de 23 de janeiro de 2013 regulamento o procedimento de intenção de registro de preços (IRP) com o escopo de incentivar a participação de órgãos ou entidades públicas em um único processo licitatório, a fim de minimizar o tempo e os custos demandados na realização do certame. Ademais, essa participação amplia o poder de compra da Administração Pública com a maximização do quantitativo licitado.

Com isto, e considerando a presente necessidade de aquisição dos bens em comento, justifica-se a participação do IFRN c*ampus* Ipanguaçu no procedimento licitatório a ser realizado pelo IFRN - *Campus Natal Zona Norte* (UASG 158368), tendo como origem a IRP 03/2022. Tudo em conformidade com DOD 02/2022 - CTI/DG/IP/RE/IFRN, que visa adequação da infraestrutura de TI para interconexão a Info Via Potiguar (RNP). Possibilitando o aumento considerável da banda de comunicação do Campus Ipanguaçu, que sairá de 100Mbps para 1Gbps.

3. DA ENTREGA E DO RECEBIMENTO DO OBJETO

O responsável pela requisição e recebimento dos materiais será a COMPAT/IP - Coordenação de Materiais e Patrimônio do IFRN Campus Ipanguaçu, situado na Rodovia RN 118, s/n, Povoado de Base Física, – Zona Rural – Ipanguaçu/RN – CEP 59508-000 - Fone (84) 4005-4104, de Segunda a Sexta-Feira, no horário das 08h às 11h e das 13h às 15h.

4. DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

A estimativa de consumo está de acordo com as quantidades manifestadas na IRP 03/2022, para atender à demanda dA CTI - IFRN Campus Ipanguaçu, consoante o exposto no item Proposto do Resumo da Manifestação de Interesse da IRP em questão.

ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

5. MANIFESTAÇÃO DE CONCORDÂNCIA COM AS CONDIÇÕES DO TERMO DE REFERÊNCIA

O IFRN - Campus Ipanguaçu, manifesta que aceita as condições contidas no Termo de Referência elaborado pelo IFRN - Campus Natal Zona Norte, órgão gerenciador do certame.

Ipanguaçu/RN, 27 de junho de 2022.

João Maria Guedes da Cruz Júnior
Requisitante

6. DESPACHO DO ORDENADOR DE DESPESAS

Diante do Demonstrativo de Necessidade apresentado:

1. Aprovo o presente documento;

2. Autorizo o início dos procedimentos para participação na IRP citada;

3. Determino seguimento do presente processo conforme tramites habituais.

4. Encaminho o processo a Direção de Administração para que tome as providências cabíveis de acordo com as normas em vigor.

Ipanguaçu/RN, 27 de junho de 2022.

Jose Geraldo Bezerra Galvão Júnior
Diretor geral
Ordenador de despesa
Diretor Geral do IFRN/Campus Ipanguaçu

Estudo Técnico Preliminar - 14/2022

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Info Via Potiguar (RNP). Possibilitando o aumento considerável da banda de comunicação do Campus Ipanguaçu, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	João Maria Guedes da Cruz Júnior

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;	
2	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
3	Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;
4	Melhorar o nível de qualidade ser serviço das aplicações internas do campus.
Identificação das necessidades tecnológicas	
1	Adquirir uma solução de firewall de próxima geração;
2	Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Ipanguaçu do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Infovia Potiguar, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Ipanguaçu já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2015. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 6 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como o IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Ipanguaçu se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Ipanguaçu do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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 Solução 2 Solução 3 Solução	X		

	4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Ipanguaçu, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões:

1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Infovia Potiguar, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de Internet.

2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Ipanguaçu do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Ipanguaçu, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, a NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Ipanguaçu do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Ipanguaçu do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05/2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25

Preço médio estimado por unidade	R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)	R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Ipanguaçu do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

LEIDIANA ARCANJO DA SILVA
ASSISTENTE EM ADMINISTRAÇÃO

JOÃO MARIA GUEDES DA CRUZ JÚNIOR
COORDENADOR DE TI

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

PROCESSO: 23037.000846.2022-41

ETP DIGITAL Nº 14/2022

OBJETO: Aquisição de Solução de Firewall de Próxima Geraçãopar a atender a demanda da CTI - Campus Ipanguaçu

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)
JOÃO MARIA GUEDES DA CRUZ JÚNIOR
Coordenador da CTI/IP
Membro Requisitante

(assinado digitalmente)
LEIDIANA ARCANJO DA SILVA
Assistente em Administração
Membro

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o presente Estudo Técnico Preliminar, considerando que o objeto da contratação está claro e justificado; os requisitos relevantes da contratação foram adequadamente relacionados e analisados; a análise de mercado foi devidamente realizada e demonstrou haver capacidade em atender ao objetivo da contratação; os riscos e impactos relevantes foram satisfatoriamente levantados e considerados no planejamento. Portanto, demonstra a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Ipanguaçu/RN, 24 de junho de 2022

(assinado digitalmente)
JOSÉ GERALDO BEZERRA GALVÃO JÚNIOR
Diretor-Geral
(Portaria nº 1782-RE/IFRN, de 21/12/2020, publicada no DOU de 22/12/2020)

Documento assinado eletronicamente por:

- **Leidiana Arcanjo da Silva**, **ASSISTENTE EM ADMINISTRACAO**, em 27/06/2022 07:52:35.
- **Joao Maria Guedes da Cruz Junior**, **COORDENADOR - FG0002 - CTI/IP**, em 26/06/2022 21:06:46.
- **Jose Geraldo Bezerra Galvao Junior**, **DIRETOR GERAL - CD2 - DG/IP**, em 24/06/2022 17:02:16.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418689
Código de Autenticação: 1b747a7e1e

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/JOÃO CÂMARA

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS JOÃO CÂMARA
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/JC/RE/IFRN

23 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Thallyson Anselmo Soares Damasceno	**Matrícula/SIAPE:**	3082767
E-mail:	thallyson.damasceno@ifrn.edu.br	**Telefone**	(84) 4005-4105

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Thallyson Anselmo Soares Damasceno	**Matrícula/SIAPE:**	3082767
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/JC
E-mail:	thallyson.damasceno@ifrn.edu.br	**Telefone**	(84) 4005-4105

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Thallyson Anselmo Soares Damasceno

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TIC para interconexão à Rede GigaNatal por meio do link de rede da Infovia Potiguar, permitindo o aumento da banda de comunicação do Campus JC de 250Mbps para 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
Objetivos Estratégicos	**Nome do documento <vigência>**

GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade;	**M30**	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia, os hackers também avançam e desenvolvem e aplicam novas técnicas de ataques maliciosos, seja em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação e Comunicação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* João Câmara do IFRN. O equipamento de firewall em operação, adquirido em 2015 através da Nota de Empenho 2015NE800299, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito dos *campi* do IFRN.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta pela garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e

dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (antivírus, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall do *campus* por outro de mesma tecnologia e gerenciável pelo Panorama, solução já em uso no instituto, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TIC do Campus; também, o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, integrando-se a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 250Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* João Câmara;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do *Campus*.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do Integrante Requisitante da Demanda:
Thallyson Anselmo Soares Damasceno - Matrícula 3082767.

6 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO			
Nome:	Rezembrim de Paula Soares	**Matrícula/SIAPE:**	2092315
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/JC
E-mail:	rezembrim.soares@ifrn.edu.br	**Telefone**	(84)4005-4105

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento:
Rezembrim de Paula Soares - Matrícula 2092315.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

7 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

8 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Adriane de Morais Ferreira	**Matrícula/SIAPE:**	2101595
Cargo:	Administrador	**Lotação:**	DIAD/JC
E-mail:	adriane.morais@ifrn.edu.br	**Telefone**	(84)4005-4105

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento:
Adriane de Morais Ferreira - Matrícula 2101595.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento:
Matheus Augusto Avelino Tavares - Matrícula 1723860

Documento assinado eletronicamente por:

- **Thallyson Anselmo Soares Damasceno, TEC DE TECNOLOGIA DA INFORMACAO**, em 23/06/2022 15:01:16.
- **Rezembrim de Paula Soares, TEC DE TECNOLOGIA DA INFORMACAO**, em 23/06/2022 15:01:50.
- **Adriane de Morais Ferreira, ADMINISTRADOR**, em 24/06/2022 08:24:59.
- **Matheus Augusto Avelino Tavares, DIRETOR GERAL - CD2 - DG/JC**, em 24/06/2022 14:59:05.
- **Andre Gustavo Duarte de Almeida, Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 24/06/2022 11:54:53.

Este documento foi emitido pelo SUAP em 23/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418182
Código de Autenticação: 769d86fc31

Estudo Técnico Preliminar - 43/2022

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Adequação da infraestrutura de TIC para interconexão à Rede GigaNatal por meio do link de rede da Infovia Potiguar, permitindo o aumento da banda de comunicação do Campus JC de 250Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Thallyson Anselmo Soares Damasceno

4. Necessidades de Negócio

4.1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego, bem como proteção da rede;
4.2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei 13.709/2018) e Marco Civil da Internet (Lei 12.965/2014);
4.3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;
4.4. Melhorar o nível de qualidade de serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

5.1. Adquirir solução de firewall de próxima geração;
5.2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso no instituto e instalado na Reitoria do IFRN, otimizando a administração dos *appliances* e armazenamento de logs.

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

6.1. Aproveitar o conhecimento existente e capacitações prévias da equipe sobre a solução;
6.2. Garantir à equipe de segurança da informação a visibilidade das aplicações em uso na rede e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido à necessidade do campus João Câmara do IFRN em adquirir solução de firewall de próxima geração cujas características técnicas atendam a capacidade de *throughput* (vazão) de 1 Gbps ou superior, em função de interligação desse Campus à Rede GigaNatal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus João Câmara já dispõe de uma solução de firewall de próxima geração da Palo Alto Networks, a qual foi adquirido em 2015. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto Networks, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede desde 2015, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta no site do fabricante foi verificado que tal equipamento foi descontinuado, (conforme link: https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates) e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como o IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos que traz mais agilidade nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	Solução de proteção de rede - Firewall	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;
– As alternativas do mercado;
– A existência de software público brasileiro;
– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;
– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);
– A possibilidade de aquisição na forma de bens ou contratação como serviço;
– Os diferentes modelos de prestação do serviço;
– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;
– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus João Câmara se encontra operante, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional para correção de bugs e novas funcionalidades, bem como proteção contra ameaças, colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.
Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus João Câmara. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, garantindo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.
Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.
Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in*-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares.

Por contar com uma quantidade de funcionários reduzida para suportar as demandas da segurança da informação, o setor de TI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus João Câmara do IFRN e que inviabilizaria a administração da rede. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade. Além disso, esta solução não se adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	DESCRIÇÃO
1	Renovar a solução atual
2	Firewall UTM
3	Firewall de próxima geração

4	Composição de soluções de segurança

9. Análise comparativa de soluções

ANÁLISE DAS SOLUÇÕES				
Requisito	**Solução 1**	**Solução 2**	**Solução 3**	**Solução 3**
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	NSA	S	S	S
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	NSA	NSA	NSA	NSA
A solução é composta por software livre ou software público? (quando se tratar de software)	NSA	NSA	NSA	NSA
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	NSA	NSA	NSA	NSA
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	NSA	NSA	NSA	NSA
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	NSA	NSA	NSA	NSA

Legenda:
S - Sim
N - Não
NSA - Não se aplica

COMPARAÇÃO DAS ALTERNATIVAS					
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**	**Avaliação da Alternativa 4**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	O uso de firewall UTM não atende a demanda do instituto, considerando que são equipamentos projetados para uso com baixa demanda de rede.	Atende.	O uso de solução composta não atende a demanda do instituto pois acarretaria aumento dos custos pelas razões expostas anteriormente.

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus João Câmara, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) o equipamento atual (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps com todas as funções de segurança habilitadas, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?

_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus João Câmara do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus João Câmara do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus João Câmara, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus João Câmara do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus João Câmara do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus João Câmara do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus João Câmara do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE - FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

2. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	**Benefício**
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as

	condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

Aprovação válida com assinatura eletrônica do Integrante Requisitante neste documento.

THALLYSON ANSELMO SOARES DAMASCENO

Integrante Requisitante

Aprovação válida com assinatura eletrônica do Integrante Técnico neste documento.

REZEMBRIM DE PAULA SOARES

Integrante Técnico

Aprovação válida com assinatura eletrônica da Autoridade Máxima da Área de TIC.

ANDRÉ GUSTAVO DUARTE DE ALMEIDA

Diretor de Gestão de Tecnologia da Informação

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/MACAU

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS MACAU
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/MC/RE/IFRN

24 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Francisco Mauricio do Nascimento	**Matrícula/SIAPE:**	3152550
E-mail:	mauricio.nascimento@ifrn.edu.br	**Telefone**	(84) 4005-4106

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Francisco Mauricio do Nascimento	**Matrícula/SIAPE:**	3152550
Cargo:	Técnico de tecnologia da Informação	**Lotação:**	CTI/MC
E-mail:	mauricio.nascimento@ifrn.edu.br	**Telefone**	(84) 4005-4106

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Francisco Mauricio do Nascimento

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Ceará Mirim, que sairá de 100Mbps para 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;

ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Ceará Mirim do IFRN. O equipamento de firewall em operação, adquirido em 2016 através da Nota de Empenho 2016NE801365, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Ceará Mirim.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de

computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, integrando-se a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Ceará Mirim;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Aquisição de material permanente; PI: **L20RLP60MCN**; - Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Coordenador de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Francisco Mauricio do Nascimento - Matrícula 3152550.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Francisco Mauricio do Nascimento	**Matrícula/SIAPE:**	3152550
Cargo:	Técnico Tecnologia da Informação	**Lotação:**	CTI/MC
E-mail:	mauricio.nascimento@ifrn.edu.br	**Telefone**	(84)4005-4106

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Francisco Mauricio do Nascimento - Matrícula 3152550.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** Francisco Mauricio do Nascimento - Matrícula 3152550.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Antonio Felipe Fernandes Araujo	**Matrícula/SIAPE:**	3042898
Cargo:	ASSISTENTE EM ADMINISTRACAO	**Lotação:**	COFINC/MC
E-mail:	felipe.fernandes@ifrn.edu.br	**Telefone**	(84)4005-4106

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Antonio Felipe Fernandes Araujo - Matrícula 3042898.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Alan Paulo Oliveira da Silva - Matrícula 2806507

Documento assinado eletronicamente por:

- **Francisco Mauricio do Nascimento**, **COORDENADOR - FG2 - CTI/MC**, em 24/06/2022 10:20:16.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418438
Código de Autenticação: ac6ea7e4f1

Estudo Técnico Preliminar - 42/2022

1. Informações Básicas

Número do processo: 23135.001096.2022-17

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Macau, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Francisco Mauricio do Nascimento

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Macau do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação

desse Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Macau já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Macau se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Macau. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Ceará Mirim do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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			
	Solução 3			
	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução			

	Solução 3			
	Solução 4			
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Macau, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Macau do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Macau do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Macau, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Macau do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Macau do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Ceará Mirim do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$

154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Ceará Mirim do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Esta equipe de planejamento declara viável esta contratação.

19. Responsáveis

FRANCISCO MAURICIO DO NASCIMENTO

Técnico de Tecnologia da Informação

Documento Digitalizado Público

ETP-42-2022 - Aquisição de solução de firewall para campus MC

Assunto: ETP-42-2022 - Aquisição de solução de firewall para campus MC
Assinado por: Mauricio Nascimento
Tipo do Documento: Estudo preliminar - contratos
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Francisco Mauricio do Nascimento**, **COORDENADOR - FG0002 - CTI/MC** , em 23/06/2022 16:11:55.

Este documento foi armazenado no SUAP em 23/06/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1104412
Código de Autenticação: a52c43441f

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – NÚCLEO AGRESTE

ESTUDO TÉCNICO PRELIMINAR - ASSINATURA DIGITAL

ETP DIGITAL Nº 42/2022

(Processo Administrativo n.° 23135.001096.2022-17)

OBJETO: Solução de firewall de próxima geração.

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

FRANCISCO MAURICIO DO NASCIMENTO
Matrícula SIAPE nº 3152550
Membro Requisitante

Documento assinado eletronicamente por:

- **Francisco Mauricio do Nascimento**, **COORDENADOR - FG0002 - CTI/MC**, em 23/06/2022 16:27:52.

Este documento foi emitido pelo SUAP em 23/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418300
Código de Autenticação: 08eb2a8795

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/MOSSORÓ

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE PARTICIPAÇÃO - PREGÃO SRP

MANIFESTAÇÃO DE INTERESSE DE PARTICIPAÇÃO EM REGISTRO DE PREÇO NA IRP

N° 03/2022 DA UASG 158368 – INSTITUTO FEDERAL DE EDUCAÇÃO, CIENCIA E TECNOLOGIA DO RIO GRANDE DO NORTE - CAMPUS NATAL ZONA NORTE

1. **Finalidade**

Participação do(a) **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – CAMPUS MOSSORO – UASG 158365,** na condição de órgão participante do Pregão Eletrônico do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte/Campus Natal Zona Norte (UASG 158368), o qual tem como objeto a **aquisição, através de Registro de Preços, de firewall que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance, para fins de atendimento às necessidades institucionais**, em conformidade com o que preconiza o art. 6° do Decreto n° 7.892/2013.

2. **Justificativa da necessidade**

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Mossoró do IFRN. O equipamento de firewall em operação, adquirido em 2019, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do *Campus* Mossoró.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-820 será descontinuado pelo fabricante em 2024, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, integrando-se a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

Com isto, e considerando a presente necessidade de aquisição de firewall tem como objetivo a adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Mossoró, que sairá de 100Mbps para 1Gbps, justifica-se a participação do IFRN - Campus Mossoró na IRP 03/2022 – UASG 158368 - realizado pelo Instituto Federal de Educação, Ciência e Tecnologia da Rio Grande do Norte – Campus Natal Zona Norte

3. **Local de execução dos serviços**

A empresa vencedora fornecerá o item adquirido sob demanda, contra Nota de Empenho, atendendo a necessidade da Administração. Deverá ser entregue/ ou executado no IFRN Campus Mossoró localizado à **Rua Raimundo Firmino de Oliveira, nº 400-A, Conjunto Ulrick Graf, Bairro Presidente Costa e Silva, Mossoró/RN. Telefone: (84) 3422-2660. E-mail: diad.mo@ifrn.edu.br**, no horário de funcionamento da Instituição.

4. **Demonstrativo das necessidades**

As quantidades solicitadas foram cadastradas no Portal de Compras do Governo federal conforme abaixo e a comprovação da necessidade encontra-se justificada no Processo Administrativo de Gestão desta Unidade.

ITEM	DESCRIÇÃO	UNIDADE	QUANTID	VALOR UN.	VALOR TOTAL
01	Equipamento Segurança Rede Tipo: Ampliance , Aplicação: Firewall	Unidade	1	126.769,08	126.769,08

Diante do demonstrativo de necessidade apresentado:

1. Declaro a manifestação de Intenção de Registro de Preços para participar da IRP 03/2022 do Instituto Federal de Educação, Ciência e Tecnologia do RN/Campus Natal Zona Norte, tendo tomado conhecimento e

concordado com o Termo de Referência para realização de Pregão Eletrônico para a **escolha de proposta mais vantajosa para aquisição, através de Registro de Preços, de firewall que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance, para fins de atendimento às necessidades institucionais** conforme condições, quantidades, e estimativas declaradas na Intenção de Registro de Preços.

(ss l m)

l s S lv

TI - S bs Ev l

D m

IFRN – M ss

(ss l m)

F s B s h s G

D m s / DI D

IFRN - mp s M ss

6 AUTORIZAÇÃO DO ORDENADOR

Aprovo o presente documento e autorizo o início dos procedimentos para participar da IRP citada.

Hél H q h P h

Diretor Geral / Ordenador de despesas
IFRN – Campus Mossoró

D m ss l m p

- **F s B s h s G DIRET R DE DIRET RI - D - DI D/M** m / /
- **l s S lv RDEN D R - S B- HEFI - TI/M** m / /
- **H l H q h P h DIRET R GER - D - DG/M** m / /

Es m m p l S P m / / P mp v s l R l ss
h ps //s p b / - m / s s b

b

Estudo Técnico Preliminar - 24/2022

1. Informações Básicas

Número do processo: 23093.001296.2022-11

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Mossoró, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	JOSÉ EVANILDO DE LIMA

4. Necessidades de Negócio

Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;
2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;
2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Mossoró do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Mossoró já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	ITEM	DESCRIÇÃO	QUANTIDADE
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

- A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;
- As alternativas do mercado;
- A existência de software público brasileiro;
- As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQBrasil, quando aplicáveis;
- As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

- A possibilidade de aquisição na forma de bens ou contratação como serviço;
- Os diferentes modelos de prestação do serviço;
- Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens eserviços integrantes;
- A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Mossoró se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Mossoró. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance;

Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Mossoró do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	Descrição da solução (ou cenário)
1	Firewall UTM
2	Renovar a solução atual
3	Firewall de Próxima Geração
4	Composição de soluções de segurança

9. Análise comparativa de soluções

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			
	Solução 3			
	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 1			

A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objeto da solução abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	Justificativas para o critério	Avaliação da Alternativa 1	Avaliação da Alternativa 2	Avaliação da Alternativa 3
Economicidade, aderência às especificações técnicas, prazo de entrega, etc	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Mossoró, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-altonetworks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Mossoró do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Mossoró do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Mossoró, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Mossoró do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Mossoró do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Calculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Mossoró do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	113.000,00
150182	75/2021	4	09/02/2022	149.707,25
153103	62/2020	3	13/10/2021	117.600,00
Total				380.307,25
Preço médio estimado por unidade				126.769,08
Preço médio total estimado a ser contratado (1 unidade)				126.769,08

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	Ano 4	
Solução Viável 1	R$ 126.769,08	-	-	R$ 126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Mossoró do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	**BEM/ SERVIÇO**	**QUANTIDADE**	**VALOR UNITÁRIO ESTIMADO**	**VALOR TOTAL ESTIMADO**
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$ 126.769,08	R$ 126.769,08
TOTAL				R$ 126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando

for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014;
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças
5. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet;
7. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8. Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

JOSÉ EVANILDO DE LIMA
Coordenador de TI

CARLOS ANTONIO DA SILVA
Coordenador de TI - Substituto

JOSE WILSON FIRMINO JUNIOR
Assistente em Administração - NURELIC/MO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/NATAL CIDADE ALTA

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS NATAL - CIDADE ALTA
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/CAL/RE/IFRN

24 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Flavio Augusto Pereira Vale	**Matrícula/SIAPE:**	1635753
E-mail:	flavio.vale@ifrn.edu.br	**Telefone**	(84) 4005-0999

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Flavio Augusto Pereira Vale	**Matrícula/SIAPE:**	1635753
Cargo:	Técnico Laboratório Área Sistema de Informação	**Lotação:**	CTI/CAL
E-mail:	flavio.vale@ifrn.edu.br	**Telefone**	(84) 4005-0999

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Flavio Augusto Pereira Vale

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Cidade Alta, nas unidades Rocas e Rio Branco, que sairá de 100Mbps para 1Gbps cada uma.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;

ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Cidade Alta do IFRN, em suas duas unidades, na Rio Branco e Rocas. Os dois equipamentos de firewall em operação, adquiridos em 2015 e 2016 através das Notas de Empenho 2014NE800655 e 2015NE800299, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Cidade Alta.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de

computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, as duas unidades do campus Cidade Alta passarão a utilizar, cada uma, o link de 1Gbps da Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Cidade Alta;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Flavio Augusto Pereira Vale - Matrícula 1635753.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Fernando Henrique da Silva Breustedt	**Matrícula/SIAPE:**	2879298
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/CAL
E-mail:	fernando.henrique@ifrn.edu.br	**Telefone**	(84)4005-0099

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Fernando Henrique da Silva Breustedt - Matrícula 2879298.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Dalila Nathalia Bezerra Maia Mattozo	**Matrícula/SIAPE:**	1759590
Cargo:	Administradora	**Lotação:**	DIAD/CAL
E-mail:	dalila.maia@ifrn.edu.br	**Telefone**	(84)4005-0955

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Dalila Nathalia Bezerra Maia Mattozo - Matrícula 1759590.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Ayres Charles de Oliveira Nogueira - Matrícula 1722828.

Documento assinado eletronicamente por:

- **Flavio Augusto Pereira Vale**, **COORDENADOR - FG2 - CTI/CAL**, em 24/06/2022 16:59:13.
- **Dalila Nathalia Bezerra Maia Mattozo**, **ADMINISTRADOR**, em 24/06/2022 11:38:25.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 24/06/2022 18:00:42.
- **Fernando Henrique da Silva Breustedt**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 24/06/2022 11:36:40.
- **Ayres Charles de Oliveira Nogueira**, **DIRETOR GERAL - CD2 - DG/CAL**, em 24/06/2022 12:22:25.

Este documento foi emitido pelo SUAP em 21/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417157
Código de Autenticação: a943ec54a2

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS NATAL - CIDADE ALTA
Avenida Rio Branco, 743, Cidade Alta, NATAL / RN, CEP 59025-002
Fone: (84) 4005-0951

ESTUDO PRELIMINAR

Processo Administrativo nº 23466.000899.2022-11

Solução de firewall de próxima geração

Natal, 27 junho de 2022.

Histórico de Revisões

Data	Versão	Descrição	Autor
27/06/2022	1.0	Finalização da primeira versão do documento	Fernando Breustedt / Flávio Vale

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

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 01/2019.

1 - DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS	
Identificação das necessidades de negócio	
1	Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
2	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
3	Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;
4	Melhorar o nível de qualidade ser serviço das aplicações internas do campus.
Identificação das necessidades tecnológicas	
1	Adquirir uma solução de firewall de próxima geração;
2	Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.
Demais requisitos	
1	Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;
2	Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

2 - ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

Devido as necessidades do campus Cidade Alta do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Cidade Alta já dispõe de uma solução de firewall de próxima geração da Palo Alto, que foi adquirida entre 2014 e 2016 para atender suas duas unidades, na Rio Branco e nas Rocas. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente em cada Campus é o modelo PA-500 e, nas duas unidades do cidade alta,

está em uso na rede há mais de 3 anos de forma satisfatória, apesar da ausência de licenciamento e garantia, o que impossibilita o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	2

3 - ANÁLISE DE SOLUÇÕES

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

Os firewalls do Campus Cidade Alta se encontram operante e em conformidade com suas especificações, porém desatualizados em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus em suas duas unidades. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7/365 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Cidade Alta do IFRN, principalmente no cenário atual, em que o campus possui duas unidades e infraestruturas ativas. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

3.1 - IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

3.2. - 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 Solução 2 Solução 3 Solução 4	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3.3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

4 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Cidade Alta, apesar de aparentemente representar a melhor solução em função da economia, encontra fracasso por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus está integrado, a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps em cada unidade (Rio Branco e Rocas); posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Cidade Alta do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Cidade Alta do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software das duas caixas atualmente instaladas já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Cidade Alta, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Cidade Alta do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, a CTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Cidade Alta do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

5 - ANÁLISE COMPARATIVA DE CUSTOS (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1

Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Cidade Alta do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de dois equipamentos e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos

mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05/2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (2 unidades)				R$253.538,16

5.2 - 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	Ano 4	
Solução Viável 1	R$ 253.538,16	-	-	R$253.538,16	**R$ 507.076,32**

6 - DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o C ampus Alta do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

7 - ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$253.538,16
Total				R$253.538,16

8 - DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

Justificativa da solução escolhida

Benefícios a serem alcançados

ID	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

Necessidades de adequação do ambiente

ID	Adequação necessária	Responsável

1	Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.	Fernando Henrique da Silva Breustedt
2		
N		

Necessidades de adequações tecnológicas		
ID	**Adequação necessária**	**Responsável**
1	Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.	Fernando Henrique da Silva Breustedt
2		
N		

Declaração da viabilidade da contratação

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

9 - APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela **PORTARIA Nº 224/2022 - DG/CAL/RE/IFRN** , de 27 de junho 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 Técnico e Requisitante e pela autoridade máxima da área de TIC:

Aprovação válida com assinatura eletrônica do Integrante Técnico neste documento: Fernando Henrique da Silva Breustedt Matrícula 2879298

Aprovação válida com assinatura eletrônica do Integrante Requisitante neste documento: Flavio Augusto Pereira Vale Matrícula 1635753

Aprovação válida com assinatura eletrônica da Autoridade Máxima da Área de TIC (ou autoridade superior, se aplicável - § 3º do art. 11): André Gustavo Duarte de Almeida Matrícula 1577655

Documento assinado eletronicamente por:

- **Flavio Augusto Pereira Vale**, **COORDENADOR - FG0002 - CTI/CAL**, em 27/06/2022 14:00:39.
- **Fernando Henrique da Silva Breustedt**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 27/06/2022 14:00:48.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 27/06/2022 14:06:32.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418598
Código de Autenticação: f5d225196e

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/NOVA CRUZ

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS NOVA CRUZ
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/NC/RE/IFRN

27 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Vanilo Alexandre de Medeiros Dantas	**Matrícula/SIAPE:**	2234018
E-mail:	vanilo.alexandre@ifrn.edu.br	**Telefone**	(84) 4005-4107

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Vanilo Alexandre de Medeiros Dantas	**Matrícula/SIAPE:**	2234018
Cargo:	Técnico Tecnologia da Informação	**Lotação:**	CTI/NC
E-mail:	vanilo.alexandre@ifrn.edu.br	**Telefone**	(84) 4005-4107

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Vanilo Alexandre de Medeiros Dantas

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para suporte integral da banda disponível e futuras ampliações. Possibilitando o aumento considerável da banda de comunicação do Campus Nova Cruz, que atualmente dispõe de 2 links de 100Mbps, totalizando 200Mbps, mas o firewall atual limita o uso a 100Mbps, com a substituição poderíamos utilizar até 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade;	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Nova Cruz do IFRN. O equipamento de firewall em operação, adquirido em 2016, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Nova Cruz.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes

nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus possui dois links de 100Mbps, totalizando 200Mbps de banda, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Nova Cruz;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

TD - Execução do PDTI

Código 1 - Etapa: Monitorar PDTI

Origem de Recursos SUAP: **TD.20RL.171168.4** - Realizar Aquisição de Novo Firewall; PI: **L20RLP60TDN**; - Conta Corrente SIAFI: **171168810000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Vanilo Alexandre de Medeiros Dantas - Matrícula 2234018.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Vanilo Alexandre de Medeiros Dantas	**Matrícula/SIAPE:**	2234018
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/NC
E-mail:	vanilo.alexandre@ifrn.edu.br	**Telefone**	(84)4005-4107

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019,

bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Vanilo Alexandre de Medeiros Dantas - Matrícula 2234018.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Ana Alice Lima dos Santos	**Matrícula/SIAPE:**	1945269
Cargo:	Auxiliar em Administração	**Lotação:**	DIAD/NC
E-mail:	alice.lima@ifrn.edu.br	**Telefone**	(84)4005-4107

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Ana Alice Lima dos Santos - Matrícula 1945269.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Ana Alice Lima dos Santos - Matrícula 1945269

Documento assinado eletronicamente por:

- **Ana Alice Lima dos Santos**, **AUX EM ADMINISTRACAO**, em 27/06/2022 11:24:05.
- **Vanilo Alexandre de Medeiros Dantas**, **COORDENADOR - FG0002 - CTI/NC**, em 27/06/2022 11:22:51.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418948
Código de Autenticação: 44a4602657

Estudo Técnico Preliminar - 14/2022

1. Informações Básicas

Número do processo: 23516.000319.2022-44

2. Descrição da necessidade

Adequação da infraestrutura de TI para suporte integral da banda disponível e futuras ampliações. Possibilitando o aumento considerável da banda de comunicação do Campus Nova Cruz, que atualmente dispõe de 2 links de 100Mbps, totalizando 200Mbps, mas o firewall atual limita o uso a 100Mbps, com a substituição poderíamos utilizar até 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Vanilo Alexandre de Medeiros Dantas

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada, controle do tráfego e proteção da rede;
2. Adequação às legislações vigentes, tais como LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet (Lei nº 12.965/2014);
3. Manter a integridade dos dados e informações sensíveis dos sistemas do campus;
4. Melhorar o nível de qualidade de serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;
2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;
2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Nova Cruz do IFRN em adquirir uma solução de firewall de próxima geração, cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Rede GigaNatal, as quantidade abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Nova Cruz já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneisVPN, e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como o IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que a solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento instalado e em uso na Reitoria do IFRN.

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

- A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;
- As alternativas do mercado;
- A existência de software público brasileiro;
- As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;
- As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);
- A possibilidade de aquisição na forma de bens ou contratação como serviço;
- Os diferentes modelos de prestação do serviço;
- Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;
- A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Nova Cruz se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Nova Cruz. Portanto, manter a solução com suporte e garantia ativos é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do

firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, fireawalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection),* provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de Banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex.: NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Ceará Mirim do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709 /2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

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		
	Solução 4	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			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
	Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			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
	Solução 4			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
	Solução 4			X

COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetivade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a demanda atual e possíveis ampliações.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Nova Cruz, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) O equipamento atual (PA-500) não atende 100% da banda disponível atualmente (200Mbps), nem as possíveis ampliações; posto que o throughput do equipamento atual limita-se

aos 100Mbps, o que impossibilita o uso integral dos recursos da banda de internet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog /opinions/palo-altonetworks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Nova Cruz do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus, envolvendo em custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuários LDAP / Active Directory ou captive portal.

Quanto a atualização do software do equipamento atualmente instalado já se verificou a impossibilidade de atendimento da banda de internet do campus Nova Cruz e de possíveis ampliações.

E por fim, com o intuito de proteger os investimentos do Campus Nova Cruz do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, dendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, a Coordenção de TI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Nova Cruz do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Nova Cruz do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* de segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection)*, provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de Banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05/2014 da Secretaria De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$ 113.000,00
150182	75/2021	4	09/02/2022	R$ 149.707,25
153103	62/2020	3	13/10/2021	R$ 117.600,00
Total				R$ 380.307,25
Preço médio estimado por unidade				R$ 126.769,08
Preço médio total estimado a ser contratado (1 unidade)				R$ 126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$ 126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Nova Cruz do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$ 126.769,08	R$ 126.769,08
Total				R$ 126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
2. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme o perfil de usuários, controlando de forma granular a utilização dos recursos;
6. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8. Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9. Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN. A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

VANILO ALEXANDRE DE MEDEIROS DANTAS

Coordenador de Tecnologia da Informação

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS NOVA CRUZ
Av. José Rodrigues de Aquino Filho, RN 120, 640, Alto de Santa Luzia, NOVA CRUZ / RN, CEP 59215-000
Fone: (84) 4005-4107

ESTUDO PRELIMINAR

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE - *CAMPUS* NOVA CRUZ

PARTICIPAÇÃO EM PROCESSO LICITATÓRIO A SER GERENCIADO PELO IFRN NOVA CRUZ/RN

ESTUDO TÉCNICO PRELIMINAR 15/2022

OBJETO: Aquisição de material permanente e consumo para os campi do IFRN.

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR:

NOME	MATRÍCULA
VANILO ALEXANDRE DE MEDEIROS DANTAS	2234018

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o Estudo Técnico Preliminar, considerando os elementos que caracterizam o objeto, a relevância e a necessidade da contratação, a aplicabilidade dos recursos públicos empregados, bem como os resultados esperados, conforme fundamentado nos autos.

(assinado digitalmente)

Allan Nilson de Sousa Dantas

Diretor-Geral do *Campus* Nova Cruz
Delegação de Competência
PORTARIA Nº 1800/2020 - RE/IFRN

Documento assinado eletronicamente por:

- **Allan Nilson de Sousa Dantas**, **DIRETOR GERAL - CD0002 - DG/NC**, em 27/06/2022 12:45:29.
- **Vanilo Alexandre de Medeiros Dantas**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 27/06/2022 12:16:10.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419082
Código de Autenticação: 6d945133e9

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/PARNAMIRIM

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS PARNAMIRIM
Coordenação de Tecnologia da Informação

DOD 2/2022 - CTI/DG/PAR/RE/IFRN

24 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Jefferson Johnne Marques Silva	**Matrícula/SIAPE:**	2876071
E-mail:	jefferson.silva@ifrn.edu.br	**Telefone**	(84) 4005-4108

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Jefferson Johnne Marques da Silva	**Matrícula/SIAPE:**	2876071
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/PAR
E-mail:	jefferson.johnne@ifrn.edu.br	**Telefone**	(84) 4005-4108

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento:

Jefferson Johnne Marques da Silva - Matrícula 2876071.

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Manutenção da infraestrutura de TI para interconexão do Campus Parnamirim à Rede GigaNatal.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;

ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
958	EQUIPAMENTO SEGURANÇA REDE

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do ***Campus* Parnamirim** do IFRN. O equipamento de firewall em operação é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do ***Campus* Parnamirim**.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do ***Campus*** **Parnamirim**;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **171168810000000044905 2**.

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda:

Jefferson Johnne Marques da Silva - Matrícula 2876071.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Fillipe Morais Rodrigues	**Matrícula/SIAPE:**	1605918
Cargo:	Técnico Laboratório Área Sistema da Computação	**Lotação:**	CTI/PAR
E-mail:	fillipe.rodrigues@ifrn.edu.br	**Telefone**	(84)4005-4108

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento:

Fillipe Morais Rodrigues - Matrícula 1605918.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** **André Gustavo Duarte de Almeida - Matrícula 1577655.**

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Tatiana Cardoso Delgado Kobayashi	**Matrícula/SIAPE:**	1677949
Cargo:	Técnico de Laboratório	**Lotação:**	COCOMP/PAR
E-mail:	tatiana.delgado@ifrn.edu.br	**Telefone**	(84)4005-4108

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento:

Tatiana Cardoso Delgado Kobayashi - Matrícula SIAPE nº 1677949.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento:

Paulo Vitor Silva - Matrícula SIAPE nº 2691107.

Documento assinado eletronicamente por:

- **Tatiana Cardoso Delgado Kobayashi, Coordenador de Compras - FAG-IFRN - COCOMP/PAR**, em 24/06/2022 13:42:02.
- **Andre Gustavo Duarte de Almeida, Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 24/06/2022 13:37:58.
- **Jefferson Johnne Marques da Silva, COORDENADOR - FG2 - CTI/PAR**, em 24/06/2022 11:52:21.
- **Fillipe Morais Rodrigues, TECNICO DE LABORATORIO AREA**, em 24/06/2022 11:58:30.
- **Paulo Vitor Silva, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 24/06/2022 13:56:21.

Este documento foi emitido pelo SUAP em 23/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418332
Código de Autenticação: 82dc5f4b18

Estudo Técnico Preliminar - 36/2022

1. Informações Básicas

Número do processo: 23424.001304.2022-22

2. Descrição da necessidade

Manutenção da infraestrutura de TI para interconexão do Campus Parnamirim à Rede GigaNatal.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Jefferson Johnne Marques da Silva

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do **campus Parnamirim** do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o **Campus Parnamirim** já dispõe de uma solução de firewall de próxima geração da Palo Alto em operação. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-820 e está em uso na rede a mais de 3 anos de forma satisfatória. Entretanto o anterior já apresentou problemas que resultou na necessidade intempestiva de substituição.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de manutenção da solução de firewall, se faz necessário para este projeto a inclusão na IRP dessa solução de firewall de próxima geração para possível aquisição.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do **Campus Parnamirim** se encontra operante e em conformidade com suas especificações, porém em breve o mesmo se encontrará desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do **Campus Parnamirim**. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao **Campus Parnamirim** do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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			
	Solução 3			
	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução			

	Solução 3			
	Solução 4			
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no **Campus Parnamirim**, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do **Campus Parnamirim** do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do **Campus Parnamirim** do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do **Campus Parnamirim**, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do **Campus Parnamirim** do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o **Campus Parnamirim** do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do **Campus Panamirim** do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$

154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o **Campus Parnamirim** do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

Dessa forma a participação na **Intenção de Registro de Preços nº 03/2022 da UASG 158368 - INST.FED.DO R.G.DO NORTE/CAMPUS NATAL Z NORTE** atende à demanda de contratação de solução de TIC objeto deste estudo preliminar.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução

compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

A participação na **Intenção de Registro de Preços nº 03/2022 da UASG 158368 - INST.FED.DO R.G.DO NORTE /CAMPUS NATAL Z NORTE** traz diversos benefícios em termos de economia uma vez que os trâmites processuais encontram-se já superados e a manifestação encontra-se amparada pelas legislações vigentes.

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-820 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN. A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

Considerando ainda o apresentado nesse Estudo Técnico Preliminar, quanto a necessidades, das soluções disponíveis e da estimativa de valor para aquisição desse material permanente, declaramos ser viável a participação na **Intenção de Registro de Preços nº 03/2022 da UASG 158368 - INST.FED.DO R.G.DO NORTE/CAMPUS NATAL Z NORTE.**

19. Responsáveis

JEFFERSON JOHNNE MARQUES DA SILVA

Coordenador de Tecnologia da Informação

FILLIPE MORAIS RODRIGUES

Técnico de Laboratório / Área Sistemas de Computação

TATIANA CARDOSO DELGADO KOBAYASHI

Técnico de Laboratório

Documento Digitalizado Público

ETP36_2022 - Aquisição de Firewall

Assunto: ETP36_2022 - Aquisição de Firewall
Assinado por: Jefferson Silva
Tipo do Documento: Estudo preliminar - contratos
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Jefferson Johnne Marques da Silva**, **COORDENADOR - FG2 - CTI/PAR**, em 24/06/2022 15:14:49.

Este documento foi armazenado no SUAP em 24/06/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1105211
Código de Autenticação: 4892c83014

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TA-ETP 1/2022 - CTI/DG/PAR/RE/IFRN

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

PROCESSO Nº 23424.001304.2022-22

ETP DIGITAL Nº 36/2022

OBJETO: Manifestação de Interesse em Participação de Registro de Preços - UASG 158368 - IRP nº 3/2022

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)
Jefferson Johnne Marques da Silva
Matrícula SIAPE nº 2876071
Membro Requisitante

(assinado digitalmente)
Tatiana Cardoso Delgado Kobayashi
Matrícula SIAPE nº 1677949
Membro Administrativo

(assinado digitalmente)
Fillipe Morais Rodrigues
Matrícula SIAPE nº 1605918
Membro Técnico

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o presente Estudo Técnico Preliminar, considerando que o objeto da **Manifestação de Interesse em Participação de Registro de Preços - UASG 158368 - IRP nº 3/2022** está claro e justificado;

24 de junho de 2022

(assinado digitalmente)
André Gustavo Duarte
Matrícula SIAPE nº 1577655
Diretor de Gestão TI
Autoridade máxima da Área de TIC

Documento assinado eletronicamente por:

- **Jefferson Johnne Marques da Silva, COORDENADOR - FG2 - CTI/PAR**, em 24/06/2022 13:04:20.
- **Andre Gustavo Duarte de Almeida, Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 24/06/2022 14:50:13.
- **Tatiana Cardoso Delgado Kobayashi, Coordenador de Compras - FAG-IFRN - COCOMP/PAR**, em 24/06/2022 13:57:19.
- **Fillipe Morais Rodrigues, TECNICO DE LABORATORIO AREA**, em 24/06/2022 14:26:05.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418565
Código de Autenticação: 6cd623e13a

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/PAU DOS FERROS

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE PARTICIPAÇÃO - PREGÃO SRP

Ao Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / Campus Natal Zona Norte

UASG 158368 – IRP nº 03/2022

Processo: 23137.001070.2022-59

1 OBJETO

Aquisição de Solução de Firewall de Próxima Geração para a adequação da infraestrutura de TI para interconexão a Rede Infovia Potiguar. Visto que atualmente o throghtput máximo de saída do campus é 250 mbps. Tal adequação possibilitará o aumento da banda de comunicação do Campus Pau dos Ferros, visto que é previsto que o projeto Infovia libere no mínimo 1Gbps para acesso ao campus, sem contar o outro link contratados de 100mbps para o IFRN Campus Pau dos Ferros, conforme condições, quantidades e exigências estabelecidas no Termo de Referência da IRP 03/2022 UASG 158368.

2 JUSTIFICATIVA DA NECESSIDADE

Esta solicitação de participação visa atender as demandas para 2023 daCoordenação de Tecnologia da Informação do IFRN Campus Pau dos Ferros para plena realização de suas atividades de suporte acadêmico e administrativo.

O decreto nº 7.892/2013 regulamenta o procedimento de Intenção de Registro de Preços a fim de permitir a aquisição de materiais/contratação de serviços para atendimento a mais de um órgão ou entidade, trabalhando de forma integrada aspectos técnicos da contratação, estimativas de consumo e minimização de tempo e custos, além de obter melhores preços junto ao mercado e maximizar o poder de compra da Administração Pública.

Além de melhorar a qualidade técnica dos procedimentos licitatórios, um planejamento integrado de contratação reduz a duplicidade de esforços entre as organizações interessadas e aperfeiçoa o trabalho dos gestores com ênfase nas atividades de aquisições, licitações e contratos, ensejando economia processual.

3 DA ENTREGA E DO RECEBIMENTO DO OBJETO

ÓRGÃO: Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte / Campus Pau dos Ferros
ENDEREÇO: BR 405, KM 154, S/N, Bairro Chico Cajá, Pau dos Ferros - RN, 59900-000
SETOR DE ENTREGA: Almoxarifado (COMPAT/PF)
TELEFONE PARA CONTATO: (84) 4005-4109 (ramal 6612)
E-MAIL: compat.pf@ifrn.edu.br

4 DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

As quantidades solicitadas foram cadastradas no SIASGNET conforme abaixo:

Item	Descrição	CATSER	Unid. de fornec.	Quant. Mín.	Quant. Máx.	Quant. Total	Valor unit. máximo unitário	Valor total por item

1	Solução de proteção de rede firewall	133132	Unidade	1	1	1	R$ 126.769,08	R$ 126.769,08
VALOR TOTAL								**R$ 126.769,08**

5 MANIFESTAÇÃO DE CONCORDÂNCIA COM AS CONDIÇÕES DO TERMO DE REFERÊNCIA

O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte – Campus Pau dos Ferros, manifesta que aceita as condições contidas no Termo de Referência elaborado pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - Campus Natal Zona Norte.

Kaio Henrique Fonseca Dantas
Demandante

Coordenador de Tecnologia da Informação
IFRN – Campus Pau dos Ferros
Matrícula SIAPE: 3936971

Francisco Anchieta Ferreira Lacerda
Diretor de Administração - Substituto Eventual
Portaria nº 414/2022 - RE/IFRN
IFRN – Campus Pau dos Ferros
Matrícula SIAPE: 1814667

Emanuel Neto Alves de Oliveira
Diretor-Geral / Ordenador de despesas
Portaria n° 1782/2020 - RE/IFRN
IFRN – Campus Pau dos Ferros
Matrícula SIAPE: 1835080

Documento assinado eletronicamente por:

- **Francisco Anchieta Ferreira Lacerda**, **ASSISTENTE EM ADMINISTRACAO**, em 22/06/2022 17:41:40.
- **Emanuel Neto Alves de Oliveira**, **Diretor Geral do Campus Pau dos Ferros - CD0002 - DG/PF**, em 22/06/2022 18:04:52.
- **Kaio Henrique Fonseca Dantas**, **COORDENADOR - FG0002 - CTI/PF**, em 22/06/2022 17:39:07.

Este documento foi emitido pelo SUAP em 22/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417669
Código de Autenticação: b170be1fd7

Estudo Técnico Preliminar - 37/2022

1. Informações Básicas

Número do processo: 23137.001070.2022-59

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede Infovia Potiguar. Visto que atualmente o throghtput máximo de saída do campus é 250 mbps. Tal adequação possibilitará o aumento da banda de comunicação do Campus Pau dos Ferros, visto que é previsto que o projeto Infovia libere no mínimo 1Gbps para acesso ao campus, sem contar o outro link contratados de 100mbps, com previsão de adicionais.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Kaio Henrique Fonseca Dantas

4. Descrição dos Requisitos da Contratação

O prazo de validade na data da entrega não poderá ser inferior a 80% (oitenta por cento) da validade total, recomendada pelo fabricante, a partir da sua data de fabricação.

Em sujeição as normas técnicas, os materiais devem atender aos requisitos mínimos de utilidade, resistência e segurança e atender as normas técnicas aplicáveis ao objeto e divulgadas por órgãos oficiais competentes.

Para o fornecimento dos materiais, objeto deste estudo técnico preliminar, a contratada deverá observar, no que couber, os critérios de sustentabilidade ambiental, contidos na Instrução Normativa n° 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG e no Decreto n.°7.746, de 05/06/2012, da Casa Civil, da Presidência da República.

O material solicitado deverá ser entregue na quantidade descrita na requisição da área responsável, em horário comercial, e no endereço especificado abaixo.

A aquisição constante deste Estudo Técnico Preliminar deverá ser entregue no local indicado a seguir:

LOCAL: Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte –Campus Pau dos Ferros, no seguinte endereço: Rodovia BR 405, km 154, Bairro Chico Cajá, Pau dos Ferros-RN, CEP: 59.900-000.

Caso o material esteja em desconformidade com as especificações exigidas, a Contratada será comunicada e estará obrigada a promover a substituição no prazo máximo de 5 (cinco) dias úteis, sem qualquer custo adicional para a Contratante;

Se a substituição do material não ocorrer no prazo determinado, a Contratada estará sujeita à aplicação das sanções previstas no Edita, Termo de Referência, no Contrato e na legislação atinente à matéria.

A contratada deverá assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica sobre a qualidade e especificação dos materiais que serão entregues;

Fornecer comprovantes/recibos para controle do consumo mensal, em quantidade compatível com o objeto, quando da entrega do material, para fins de controle da CONTRATANTE;

Arcar com todas as despesas decorrentes do fornecimento do objeto, inclusive frete;

Assumir inteira responsabilidade com todas as despesas diretas e indiretas decorrentes do fornecimento do objeto, e ainda as despesas com pessoas utilizadas no fornecimento do material assumido, as quais não terão qualquer vínculo empregatício com a CONTRATANTE;

Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;

Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do Contrato, não excluindo ou reduzindo essa responsabilidade à fiscalização e o acompanhamento da CONTRATANTE;

Aceitar, nas mesmas condições estabelecidas em Contrato, os acréscimos ou supressões até25% (vinte e cinco por cento) do valor inicialmente contratado;

A contratada deverá fornecer diretamente o objeto, não podendo transferir a responsabilidade pelo objeto licitado para nenhuma outra empresa ou instituição de qualquer natureza;

Nos valores propostos deverão estar inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens;

A proposta da contratada deverá ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal. Devera ainda conter a indicação do banco, número da conta e agenda, para fins de pagamento;

Não haverá exigência de garantia de execução para a presente contratação.

DA SUSTENTABILIDADE AMBIENTAL; a empresa deverá apresentar material constituído e embalado com critérios socioambientais vigentes decorrentes da Lei n° 6.938/81 e regulamentos, com os respectivos registros e comprovações oficiais, além de atentar para as exigências da Política de Resíduos Sólidos.

Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

5. Levantamento de Mercado

Diante das necessidades apontadas neste estudo, o atendimento a solução exige a aquisição do item compatível com o objeto pretendido.

Foram analisadas aquisições similares feitas por outros órgãos e entidades, por meio de consultas ao Painel de Preços e consulta de Atas no Comprasnet. Não se observou maiores variações quanto à execução do objeto no que se refere ao papel da empresa a qual se pretende contratar. Assim, a variação se dá pela modalidade de licitação aplicada a cada caso, a depender da permissibilidade normativa.

Logo, a aquisição do item objeto do presente Estudo Técnico Preliminar se constitui, no atual cenário, em objeto de frequente aquisição por órgãos públicos, em todas as suas esferas. Sendo assim, verifica-se a ampla disponibilidade de empresas aptas ao fornecimento dos itens a serem adquiridos, conforme os requisites estabelecidos neste documento.

Diante das pesquisas realizadas e visando atender os interesses da nossa instituição resolvemos participar de uma Intenção de Registro de Preços em andamento para eventual necessidade de contratação objeto deste documento

6. Descrição da solução como um todo

A solução proposta envolve a eventual aquisição de rede firewall, sendo que o material será destinados à Coordenação de Tecnologia da Informação do IFRN Campus Pau dos Ferros.

Assim, a Administração transfere à empresa especializada e ganhadora do item, vencedora da licitação, a atribuição de fornecer conforme as Informações dos itens e quantidades que estão detalhadas no anexo deste documento:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMADA
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	Unidade	1

7. Estimativa das Quantidades a serem Contratadas

Para atendimento das necessidades, o item e sua quantidade foram definidos conforme tabela abaixo. A quantitativo necessária foi estipulados com base em levantamentos das quantidades definidas pela Coordenação de Tecnologia da Informação do IFRN Campus Pau dos Ferros.

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMADA
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	Unidade	1

o item e sua quantidade foram definidos conforme tabela abaixo

8. Estimativa do Valor da Contratação

Valor (R$): 126.769,08

Para a estimativa dos preços referenciais da aquisição, foi utilizada como parâmetros as disposições contidas no seguinte normativo:

1. Instrução Normativa SG/SEDGGD/ME n.° 73, de 5 de agosto de 2020;O custo estimada da contratação é de **R$ 126.769,08** (cento e vinte e seis mil, setecentos e sessenta e nove reais e oito centavos), e encontra-se pormenorizado em preços unitários e totais no processo de aquisição.

Da metodologia aplicada a política de preços:

De acordo com a Instrução Normativa SG/SEDGGD/ME n.° 73, de 05 de agosto de 2020, a qual dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, a pesquisa de preços:

> [...]
>
> Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - Painel de Preços, disponível no endereço eletrônico gov.br/paineldeprecos, desde que as cotações refiram se a aquisições ou contratações firmadas no período de até 1(um) ano anterior à data de divulgação do instrumento convocatório;

II - aquisições e contratações similares de outros entes públicos, firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;

III - dados de pesquisa publicada em mídia especializada, de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6(seis) meses de antecedência da data de divulgação do instrumento convocatório, contendo a data e hora de acesso; ou

IV- pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.

A pesquisa de preço foi realizada utilizando-se, como parâmetros, os incisos acima, em conformidade com as disposições do supracitado normativo, para obtenção do preço de referência. Foi utilizado como método para obtenção do preço estimado a média dos valores obtidos na pesquisa de preços, da qual incidiu sobre um conjunto de três ou mais preços de acordo com o art. 6° da referida instrução normativa.

9. Justificativa para o Parcelamento ou não da Solução

O objeto deverá ser parcelado por ser técnica e economicamente viável, favorecendo assim o melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

10. Contratações Correlatas e/ou Interdependentes

Não se faz necessária a realização de demais aquisições correlatas e ou interdependentes ao objeto pretendido, nem há pretensão de realizar aquisições futuras para que o objetivo desta aquisição seja atingido, razão pela qual este item não será considerado no planejamento.

11. Alinhamento entre a Contratação e o Planejamento

Será feita a verificação se a aquisição do rede firewall foi incluído no Plano Anual de Contratações do ano de 2022. Caso não tenha sido. Devemos providenciar sua inclusão em momento oportuno nas janelas de abertura do sistema PGC.

12. Benefícios a serem alcançados com a contratação

1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

13. Providências a serem Adotadas

Para fins de melhorias quanto ao alcance do objetivo pretendido entendemos ser necessário fazer o correto dimensionamento dos pedidos a serem entregues.

14. Possíveis Impactos Ambientais

Nesta aquisição de item de solução de proteção de rede firewall, não se identifica possíveis impactos ambientais e respectivas medidas de tratamento ou mitigadoras que precisem ser sanadas para conter os riscos ambientais existentes. Ainda assim alertamos para o atendimento, no que couber, dos requisitos citados no último parágrafo do item4, letras a, b, c, deste Estudo Técnico Preliminar.

15. Declaração de Viabilidade

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

15.1. Justificativa da Viabilidade

Diante de toda a análise desenvolvida no presente estudo técnico preliminar, a eventual aquisiç mostra-se viável em termo de disponibilidade de mercado, forma de fornecimento de objeto, competitividade do mercado, não sendo possível observar óbices ao prosseguimento de possível contratação.

16. Responsáveis

Estamos de acordo com a contratação do item na quantidade objeto deste documento, por considerar viável e necessária, em razão de melhorias e manutenções periódicas e necessárias ao campus.

KAIO HENRIQUE FONSECA DANTAS

Coordenação de Tecnologia da Informação

Estamos de acordo com a presente aquisição em razão da necessidade e da viabilidade da mesma.

FRANCISCO ANCHIETA FERREIRA LACERDA

Diretor de Administração - Substituto Eventual

A autoridade competente do Instituto Federal de Educação, Ciências e Tecnologia do Rio Grande do Norte - Campus Pau dos Ferros APROVA o ESTUDO TÉCNICO PRELIMINAR Nº 37/2022.

EMANUEL NETO ALVES DE OLIVEIRA

Diretor Geral/Ordenador de Despesas

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

ETP DIGITAL Nº 37/2022

OBJETO: Aquisição de proteção de rede firewall.

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)
Kaio Henrique Fonseca Dantas
Membro Requisitante

(assinado digitalmente)
Francisco Anchieta Ferreira Lacerda
Membro Administrativo

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o presente Estudo Técnico Preliminar, considerando que o objeto de aquisição está claro e justificado; os requisitos relevantes da aquisição foram adequadamente relacionados e analisados; a análise de mercado foi devidamente realizada e demonstrou haver boa capacidade em atender ao objetivo da aquisição; o modelo de prestação do material sugerido é apropriado e plenamente compatível com a Instituição, especialmente do ponto de vista legal; os riscos e impactos relevantes foram satisfatoriamente levantados e considerados no planejamento. Portanto, demonstra a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de aquisição.

Pau dos Ferros-RN, 22 de junho de 2022.

(assinado digitalmente)
Emanuel Neto Alves de Oliveira
Diretor Geral do IFRN Campus Pau dos Ferros

Documento assinado eletronicamente por:

- **Francisco Anchieta Ferreira Lacerda**, **ASSISTENTE EM ADMINISTRACAO**, em 22/06/2022 17:43:03.
- **Emanuel Neto Alves de Oliveira**, **Diretor Geral do Campus Pau dos Ferros - CD0002 - DG/PF**, em 22/06/2022 18:05:22.
- **Kaio Henrique Fonseca Dantas**, **COORDENADOR - FG0002 - CTI/PF**, em 22/06/2022 17:41:23.

Este documento foi emitido pelo SUAP em 22/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417665
Código de Autenticação: 34bae25b6e

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/PARELHAS

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS AVANÇADO PARELHAS
Rua Dr. Mauro Duarte, S/N, José Clóvis, S/N, 240890405, PARELHAS / RN, CEP 59360-000
Fone: (84) 4005-4115

Termo 120/2022 - DIAD/DG/PAAS/RE/IFRN

Termo de Participação

AO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – CAMPUS NATAL ZONA NORTE

UASG **nº 158368**

IRP nº **03/2022**

1 – OBJETO

1.1. Participação em processo licitatório para **aquisição de material permanente de TI** a ser realizado pelo **Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - Campus Zona Norte (UASG 158368)**, conforme condições, quantidades e exigências estabelecidas no Termo de Referência, referente à **IRP n° 03/2022**.

2 – JUSTIFICATIVA DA NECESSIDADE

2.1. A participação neste certame visa atender às necessidades administrativas e acadêmicas do IFRN Campus Avançado Parelhas, cuja finalidade é a aquisição material Permanente de TI, visando possibilitar a adequação dos equipamentos de Firewall a soluções mais recentes. A não aquisição destes materiais poderá implicar em prejuízos na realização das atividades deste Campus.

2.2 O decreto nº 7.892/2013 regulamenta o procedimento de Intenção de Registro de Preços a fim de permitir a aquisição de materiais/contratação de serviços para atendimento a mais de um órgão ou entidade, trabalhando de forma integrada aspectos técnicos da contratação, estimativas de consumo e minimização de tempo e custos, além de obter melhores preços junto ao mercado e maximizar o poder de compra da Administração Pública;

2.3 Além de melhorar a qualidade técnica dos procedimentos licitatórios, um planejamento integrado de contratação reduz a duplicidade de esforços entre as organizações interessadas e aperfeiçoa o trabalho dos gestores com ênfase nas atividades de aquisições, licitações e contratos, ensejando economia processual.

3 – DA ENTREGA E DO RECEBIMENTO DO OBJETO

3.1. Os serviços serão prestados no IFRN Campus Avançado Parelhas, situado na Rua Dr. Mauro Duarte, S/N, bairro José Clóvis, Parelhas/RN, CEP 59.360-000 – Fone (84) 4005-4115, de segunda a sexta-feira, no horário das 08h às 12h e das 13h às 17h.

4 – DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

4.1. A definição do quantitativo foi baseada no estudo técnico preliminar elaborado pelo setor de TI do Campus, conforme descrição de necessidades técnicas apontadas no referido documento.
4.2. As quantidades solicitadas foram cadastradas no SIASGNET conforme estimativa de consumo para atender às demandas do IFRN Campus Avançado Parelhas, para manutenção de suas atividades.

5 – CONCORDÂNCIA

5.1 O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte – Campus Avançado Parelhas, manifesta que aceita as condições contidas no Termo de Referência elaborado pelo IFRN – Campus Natal Zona Norte, órgão gerenciador do certame.

Parelhas/RN, 27 de junho de 2022

MARCO ANTÔNIO SILVA E ARAÚJO
Coordenador de TI

VICTOR CARVALHO DE ASSIS
Diretor de Administração em Exercício

6 – AUTORIZAÇÃO DO ORDENADOR

6.1 Aprovo o presente documento e autorizo a adesão a referida IRP.

RAMON VIANA DE SOUSA
Diretor-Geral
IFRN Campus Avançado Parelhas

Documento assinado eletronicamente por:

- **Ramon Viana de Sousa, DIRETOR - CD0003 - DG/PAAS**, em 27/06/2022 14:20:44.
- **Victor Carvalho de Assis, DIRETOR - SUB-CHEFIA - DIAD/PAAS**, em 27/06/2022 14:12:30.
- **Marco Antonio Silva e Araujo, TECNICO DE LABORATORIO AREA**, em 27/06/2022 14:38:42.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419136
Código de Autenticação: f0fb139d3f

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS AVANÇADO PARELHAS
Coordenação de Laboratórios do Campus Avançado de Parelhas

DOD 1/2022 - COLAB/DIAC/DG/PAAS/RE/IFRN

27 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Assessoria de Tecnologia da Informação		
Responsável pela demanda:	Marco Antonio Silva e Araújo	**Matrícula/SIAPE:**	1953287
E-mail:	marco.araujo@ifrn.edu.br	**Telefone**	(84) 4005-4115

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Marco Antonio Silva e Araújo	**Matrícula/SIAPE:**	1953287
Cargo:	Técnico Laboratório Área Sistema da Computação	**Lotação:**	ASAL/PAAS
E-mail:	marco.araujo@ifrn.edu.br	**Telefone**	(84) 4005-4115

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Marco Antonio Silva e Araújo.

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Readequação da infraestrutura de TI do IFRN, do aparelho de Firewall. Possibilitando o aumento considerável da banda de comunicação do Campus Parelhas, que poderá chegar aos 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;

ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	M30	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Parelhas do IFRN. O equipamento de firewall em operação, adquirido em 2016 através da Nota de Empenho 2016NE801365, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Parelhas.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de

computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, integrando-se a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* Parelhas;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Marco Antonio Silva e Araújo - Matrícula 1953287.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Carlos Eduardo Pereira Duarte Barreto	**Matrícula/SIAPE:**	**1161547**
Cargo:	Técnico Laboratório Área Manutenção de Computadores	**Lotação:**	ASAL/PAAS
E-mail:	duarte.carlos@ifrn.edu.br	**Telefone**	(84) 4005-4115

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Carlos Eduardo Pereira Duarte Barreto - Matrícula 1161547

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Victor Carvalho de Assis	**Matrícula/SIAPE:**	3040799
Cargo:	Didretor de Administração	**Lotação:**	GABIN/PAAS
E-mail:	catarina.torres@ifrn.edu.br	**Telefone**	(84)4005-4115

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Victor Carvalho de Assis - Matrícula 3040799.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Victor Carvalho de Assis - Matrícula 3040799

Documento assinado eletronicamente por:

- **Carlos Eduardo Pereira Duarte Barreto**, **TECNICO DE LABORATORIO AREA**, em 27/06/2022 15:28:14.
- **Victor Carvalho de Assis**, **DIRETOR - SUB-CHEFIA - DIAD/PAAS**, em 27/06/2022 15:13:24.
- **Marco Antonio Silva e Araujo**, **TECNICO DE LABORATORIO AREA**, em 27/06/2022 15:21:06.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419192
Código de Autenticação: 8643005b80

Estudo Técnico Preliminar - 62/2022

1. Informações Básicas

Número do processo: 23516.000319.2022-44

2. Descrição da necessidade

Readequação da infraestrutura de TI do IFRN Campus Parelhas. Possibilitando a atualização do dispositivo de Firewall para um de modelo mais recente e consequente substituição do aparelho em caso de falhas, visto que já está em funcionamento a mais de cinco anos.

3. Área requisitante

Área Requisitante	Responsável
Assessoria de Tecnologia da Informação	Marco Antonio Silva e Araújo
Diretoria de Administração (DIAD/PAAS)	Victor Carvalho de Assis

4. Descrição dos Requisitos da Contratação

1. Adquirir uma solução de firewall de próxima geração;
2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento
centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e
armazenamento de logs.

3. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
4. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709 /2018) e Marco Civil da
Internet Lei nº 12.965/2014);
5. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;
6. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

7. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;
8. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

5. Levantamento de Mercado

Conforme inciso II do art. 11 , deve-se verificar para composição da análiseda IN SGD /ME nº 1/2019 comparativa:
– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;
– A existência de software público brasileiro;
– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;
– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);
– A possibilidade de aquisição na forma de bens ou contratação como serviço;
– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e
serviços integrantes;
– A ampliação ou substituição da solução implantada. Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual
O firewall do Campus Parelhas se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus,
sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra
ameaças, mantendo assim essa rede íntegra e protegida.
Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se
inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os
serviços administrativos e operacionais do Campus Ceará Mirim. Portanto, manter a solução com suporte e
garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação
24/7 de todo ambiente.

Solução 2: Firewall UTM
Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de
Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é
teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um
único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo,
balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está
no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é
centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o

gerenciamento e a correlação de logs.
Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são
ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes
de pequeno e médio porte, onde o volume de dados é relativamente pequeno.
Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração
É uma plataforma de rede integrada baseada em inspeção profunda ( ), provendodeep packet inspection
múltiplos mecanismos de proteção em um único equipamento, tais como (IPS),Intrusion Prevention System
Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e
Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall
UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para
redes de grande porte. O Firewall de Próxima Geração permite: Instalação sem perda de performance;in-line
Capacidades de firewall de primeira geração (Ex. NAT, , VPN, etc.); IPS;Stateful Inspection Protocol
Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações
criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança
A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área
de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares
trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada
fabricante.
Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor
de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de
empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Ceará Mirim do
IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes
fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.
Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de

diferentes fabricantes
acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o
estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação
dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes,
equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.
Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de
Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES
ID Descrição da solução (ou cenário)
1 Firewall UTM
2 Renovar a solução atual
3 Firewall de Próxima Geração
4 Composição de soluções de segurança

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Asessoria de
Tecnologia da Informação do Campus Parelhasdo IFRN através do Documento Oficial da Demanda.
Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as
licenças de software que possibilitam a ativação das segurança necessárias à proteção da rede de features
computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (deep
), provendo múltiplos mecanismos de proteção em um único equipamento, tais como packet inspection
(IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, Intrusion Prevention System
VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é
a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda
entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line
sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection
, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir aProtocol
identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de
registros de preço do Governo Federal.
A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º

do Artigo 2º da INº 05
/2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E
Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que
atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.
Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda
americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano
de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de
2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às
demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio,
destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da
cotação cambial durante o período licitatório.

6. Descrição da solução como um todo

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Ceará Mirim do
IFRN é a Solução 3: Firewall de Próxima Geração , pois além de melhor custo-benefício em diversas questões técnicas, atende
na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

7. Estimativa das Quantidades a serem Contratadas

A quantidade de soluções necessárias, dado o porte e a demanda do IFRN - Campus Avançado Parelhas é de 1 unidade do dispositivo, visto que atualmente esta mesma quantidade consegue, até o limite de processamento de velocidade (100mbps), atender a demanda do Campus. Dada a previsão de aumento da velocidade dos links e da quantidade de alunos na Instituição, que tende a aumentar, a evolução de hardware e tecnologia desta nova unidade deverá conseguir atender à nova escala, permanecendo a quantidade de 1 equipamento, mas com hardware mais recente.

8. Estimativa do Valor da Contratação

Utilizando os valores da Intenção de Registo de Preço, para os itens necessitados, o valor estimado da contratação é definido conforme tabela abaixo:

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00

150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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	Ano 4	
Solução Viável 1	R$ 126.769,08	-	-	R$ 126.769,08	R$ 253.538,16

9. Justificativa para o Parcelamento ou não da Solução

O objeto, já definido na licitação a qual estamos manifestando interesse, seguirá a necessidade de formação de grupos em virtude serviços correlatos.

10. Contratações Correlatas e/ou Interdependentes

Não se verifica contratações correlatas, nem interdependentes para a viabilidade e contratação desta demanda, visto que diante da necessidade supracitada, a empresa fornecedora deverá apenas entregar os produtos e fornecer o suporte (garantia).

11. Alinhamento entre a Contratação e o Planejamento

Em momento oportuno, quando houver disponibilidade de recursos de aquisição de permanentes, essa Assessoria se compromete de enviar a administração do Campus a solicitação desta demanda. No entanto, faz parte do planejamento deste setor a possibilidade de aquisição.

12. Resultados Pretendidos

Benefícios a serem alcançados com a contratação:

- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
- Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao
  princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as
  condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos

específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este
fim;
- Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra
ameaças;
- Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de
forma granular a utilização dos recursos;
- Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às
exigências do Marco Civil da Internet;
- Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.;
- Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações
como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a
fim de evitar abusos em sua utilização;
- Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por
grupo ou usuário);
- Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

13. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que
pode ser utilizada.

14. Possíveis Impactos Ambientais

O dispositivo a ser substituído a partir da chegada do aparelho desta aquisição deverá ser destinado ao laboratório de redes para estudo ou para outros projetos da Assessoria de Tecnologia da Informação.

15. Declaração de Viabilidade

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

15.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de
firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os
requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do

ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução
compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software
este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de
perímetro de rede utilizados pelos Campi e Reitoria do IFRN.
A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os
seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado
neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista
tecnológico e financeiro, pois preserva o investimento realizado com a longevidade

16. Responsáveis

Aprovado com assinatura eletrônica e conforme estudo descrito neste ETP.

MARCO ANTONIO SILVA E ARAUJO
Técnico de Laboratório Área Sistemas da Informação

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TA-ETP 9/2022 - DIAD/DG/PAAS/RE/IFRN

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

ETP DIGITAL Nº 62/2022

OBJETO: Aquisição de firewall for appliance para o IFRN Campus Avançado Parelhas

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado digitalmente)	(assinado digitalmente)
Marco Antônio Silva e Araújo	**Victor Carvalho de Assis**
Matrícula SIAPE nº 1953287	Matrícula SIAPE nº 3040799
Membro Requisitante	Membro Administrativo

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Aprovo o presente Estudo Técnico Preliminar, considerando que o objeto da contratação está claro e justificado; os requisitos relevantes da aquisição foram adequadamente relacionados e analisados; a análise de mercado foi devidamente realizada e demonstrou haver boa capacidade em atender ao objetivo da contratação; o modelo de aquisição sugerido é apropriado e plenamente compatível com a Instituição, especialmente do ponto de vista legal; os riscos e impactos relevantes foram satisfatoriamente levantados e considerados no planejamento. Portanto, demonstra a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

27 de junho de 2022

(assinado digitalmente)
Ramon Viana de Sousa
Matrícula SIAPE nº 1577384
Diretor Geral do IFRN Campus Avançado Parelhas

Documento assinado eletronicamente por:

- **Ramon Viana de Sousa, DIRETOR - CD0003 - DG/PAAS**, em 27/06/2022 14:19:47.
- **Marco Antonio Silva e Araujo, TECNICO DE LABORATORIO AREA,** em 27/06/2022 14:37:42.
- **Victor Carvalho de Assis, DIRETOR - SUB-CHEFIA - DIAD/PAAS**, em 27/06/2022 14:15:05.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 419156
Código de Autenticação: 1eaa8ebbe3

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/LAJES

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS AVANÇADO LAJES
Rodovia BR 304, Km 120, Centro, S/N, 240670005, LAJES / RN, CEP 59535-000
Fone: (84) 4005-4116

Termo 86/2022 - DIAD/DG/LAJ/RE/IFRN

TERMO DE PARTICIPAÇÃO

AO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – *CAMPUS* NATAL ZONA NORTE

UASG: 158368

IRP N° 03/2022

1. OBJETO

1.1. Participação em processo licitatório para **aquisição de material permanente de TI** a ser realizado pelo **Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - *Campus* Zona Norte (UASG 158368)**, conforme condições, quantidades e exigências estabelecidas no Termo de Referência, referente à **IRP n° 03/2022**.

2. JUSTIFICATIVA DA NECESSIDADE

2.1. O Decreto n° 7.892, de 23 de janeiro de 2013, regulamenta o procedimento de intenção de registro de preços (IRP) com o escopo de incentivar a participação de órgãos ou entidades públicas em um único processo licitatório, a fim de minimizar o tempo e os custos demandados na realização do certame. Ademais, essa participação amplia o poder de compra da Administração Pública com a maximização do quantitativo licitado.

2.2. A participação neste certame visa atender às necessidades administrativas e acadêmicas do IFRN *Campus* Avançado Lajes, cuja finalidade é a **aquisição material Permanente de TI**, visando possibilitar a adequação dos equipamentos de Firewall a soluções mais recentes. A não aquisição destes materiais poderá implicar em prejuízos na realização das atividades deste *Campus*.

3. DA ENTREGA E DO RECEBIMENTO DO OBJETO

3.1. O local de entrega do material será no setor de Almoxarifado do IFRN *Campus* Avançado Lajes, situado na BR 304, km 120, Centro – Lajes/RN – CEP 59535-000 – Fone (84) 4005.4116, de segunda a sexta-feira, no horário das 08h às 12h e das 13h às 16h, e-mail: diad.laj@ifrn.edu.br; cofimpat.laj@ifrn.edu.br

4. DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

4.1. A definição do quantitativo foi baseada no estudo técnico preliminar elaborado pelo setor de TI do Campus, conforme descrição de necessidades técnicas apontadas no referido documento.

4.2. As quantidades solicitadas foram cadastradas no SIASGNET conforme estimativa de consumo para atender às demandas do IFRN *Campus* Avançado Lajes, para manutenção de suas atividades.

5. MANIFESTAÇÃO DE CONCORDÂNCIA COM AS CONDIÇÕES DO TERMO DE

REFERÊNCIA

5.1. O IFRN *Campus* Avançado Lajes manifesta que aceita as condições contidas no Termo de Referência elaborado pelo **IFRN *Campus Natal Zona Norte* (UASG 158368)**, órgão gerenciador do certame.

Lajes/RN, 26 de junho de 2022.

DIOGO EUGENIO DA SILVA CORTEZ

Coordenador da Assessoria de Planejamento e Administração de Tecnologias da Informação

JADER LUIZ LIMA DE FREITAS

Diretor de Administração do IFRN-*Campus* Avançado Lajes

6. AUTORIZAÇÃO DO ORDENADOR

6.1. Aprovo o presente documento e autorizo a adesão à referida IRP.

Lajes/RN, 28 de junho de 2022.

ANDRÉ LUIZ RODRIGUES BEZERRA

Diretor-Geral do IFRN-*Campus* Avançado Lajes

Documento assinado eletronicamente por:

- **Jader Luiz Lima de Freitas**, **DIRETOR - FG0001 - DIAD/LAJ**, em 27/06/2022 13:31:28.
- **Diogo Eugenio da Silva Cortez**, **COORDENADOR - FAG-IFRN - DIAD/LAJ**, em 27/06/2022 11:41:21.
- **Andre Luiz Rodrigues Bezerra**, **DIRETOR - CD0003 - DG/LAJ**, em 27/06/2022 10:28:47.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418935
Código de Autenticação: 8d368c41ae

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS AVANÇADO LAJES
Assessoria de Planejamento e Administração de Tecnologias da Informação do Campus Avançado Lajes

DOD 1/2022 - ASPLADTI/DIAD/DG/LAJ/RE/IFRN

27 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Assessoria de Planejamento e Administração de Tecnologias da Informação		
Responsável pela demanda:	Diogo Eugênio da Silva Cortez	**Matrícula/SIAPE:**	1330507
E-mail:	diogo.eugenio@ifrn.edu.br	**Telefone**	(84) 4005-4116

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Diogo Eugênio da Silva Cortez	**Matrícula/SIAPE:**	1330507
Cargo:	Técnico de tecnologia da informação	**Lotação:**	ASPLADTI/LAJ
E-mail:	diogo.eugenio@ifrn.edu.br	**Telefone**	(84) 4005-4116

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Diogo Eugênio da Silva Cortez

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Ampliação da análise/processamento para prevenção de ameaça, controle do tráfego e proteção da rede. Adequação da infraestrutura de TI para a possibilidade de futura interconexão a Rede GigaNatal. Possibilitando o aumento considerável da banda de comunicação do Campus Avançado Lajes, que sairá de 100Mbps para 1Gbps.

4 - MOTIVAÇÃO/JUSTIFICATIVA
Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas

de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* Avançado Lajes do IFRN. O equipamento de firewall em operação, adquirido em 2016 através da Nota de Empenho 2015NE800299, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Lajes.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, a adequação técnica do Campus para a possibilidade de receber o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, que poderá integrar este campus a Rede GigaNatal, fato que aumentará substancialmente a capacidade de trafego na internet. Para isso, é necessário realizar a compra de um firewall que tenha taxa de transferência de dados (throughput) adequado; posto que o atual firewall só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* avançado Lajes;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI:**L20RLP60MCN**;
- Conta Corrente SIAFI: **171168810000000000449052**.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Diogo Eugênio da Silva Cortez	**Matrícula/SIAPE:**	1330507
Cargo:	Técnico de tecnologia da informação	**Lotação:**	ASPLADTI/LAJ
E-mail:	diogo.eugenio@ifrn.edu.br	**Telefone**	(84)4005-4116

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Diogo Eugênio da Silva Cortez - Matrícula 1330507.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS

Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC

Não se aplica.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa. ANDRÉ LUIZ RODRIGUES BEZERRA Diretoro Geral do Campus Avançado Lajes

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Jáder Luiz Lima de Freitas	**Matrícula/SIAPE:**	3012724
Cargo:	Diretor Administrativo	**Lotação:**	DIAD/LAJ
E-mail:	jader.lima@ifrn.edu.br	**Telefone**	(84)4005-4116

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Jáder Luiz Lima de Freitas- Matrícula 3012724.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Documento assinado eletronicamente por:

- **Jader Luiz Lima de Freitas**, **DIRETOR - FG0001 - DIAD/LAJ**, em 27/06/2022 10:13:09.
- **Andre Luiz Rodrigues Bezerra**, **DIRETOR - CD0003 - DG/LAJ**, em 27/06/2022 10:29:14.
- **Diogo Eugenio da Silva Cortez**, **COORDENADOR - FAG-IFRN - DIAD/LAJ**, em 27/06/2022 10:04:11.

Este documento foi emitido pelo SUAP em 24/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418431
Código de Autenticação: 218b34821f

Estudo Técnico Preliminar - 60/2022

1. Informações Básicas

Número do processo: 23134.001596.2022-69

2. Descrição da necessidade

Adequação da velocidade do nosso link atual, taxa de transferência (TT), que é de 300Mbps à TT para Prevenção de ameaças do Firewall PA. A adequação técnica do Campus para a possibilidade de receber o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, que poderá integrar este campus a Rede GigaNatal, fato que aumentará substancialmente a capacidade de tráfego na internet.

3. Área requisitante

Área Requisitante	Responsável
Assessoria de Planejamento e Administração de Tecnologias da Informação	Diogo Eugênio da Silva Cortez

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Avançado Lajes do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função da adequação da atual velocidade do link de internet e futura expansão, assim como a possibilidade de interligação desse Campus à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus Avançado Lajes já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2015. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a aproximadamente 6 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www. paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Lajes se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Lajes. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte.

O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Lajes do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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 Solução 2 Solução 3 Solução 4	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade,	Seguir um dos princípios	A renovação da atual solução acarretaria		

aderências às especificações técnicas, prazo de entrega, etc.	constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Lajes, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a rede Giga Natal, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-altonetworks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Lajes do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Lajes do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Lajes, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Lajes do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Lajes do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Lajes do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de

2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Lajes do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim.

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

.

19. Responsáveis

Como autoridade competente do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - Campus Avançado Lajes, APROVO o presente Estudo Técnico Preliminar.

ANDRÉ LUIZ RODRIGUES BEZERRA

Diretor - Geral

JADER LUIZ LIMA DE FREITAS

Diretor de Administração

DIOGO EUGENIO DA SILVA CORTEZ

Coordenador da Assessoria de Planejamento e Administração de Tecnologias da Informação

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS AVANÇADO LAJES
Rodovia BR 304, Km 120, Centro, S/N, 240670005, LAJES / RN, CEP 59535-000
Fone: (84) 4005-4116

ESTUDO PRELIMINAR

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – *CAMPUS* AVANÇADO LAJES

ESTUDO TÉCNICO PRELIMINAR DIGITAL 60/2022- ASSINATURA ELETRÔNICA

OBJETO: **Aquisição de SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL para atendimento de demanda do IFRN Campus Avançado Lajes**

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

NOME	MATRÍCULA
DIOGO EUGENIO DA SILVA CORTEZ	1330507
JADER LUIZ LIMA DE FREITAS	3012724

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR DIGITAL 60/2022

A autoridade competente do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - *Campus* Avançado Lajes APROVA o presente Estudo Técnico Preliminar.

Município de Lajes, 27 de junho de 2022

André Luiz Rodrigues Bezerra - Mat. 2211511

Diretor Geral do *Campus* Avançado Lajes

Documento assinado eletronicamente por:

- **Diogo Eugenio da Silva Cortez**, **COORDENADOR - FAG-IFRN - DIAD/LAJ** , em 27/06/2022 11:41:12.
- **Andre Luiz Rodrigues Bezerra**, **DIRETOR - CD0003 - DG/LAJ**, em 27/06/2022 10:28:17.
- **Jader Luiz Lima de Freitas**, **DIRETOR - FG0001 - DIAD/LAJ**, em 27/06/2022 13:31:16.

Este documento foi emitido pelo SUAP em 27/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418951
Código de Autenticação: 375d95e922

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/SANTA CRUZ

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS SANTA CRUZ
Coordenação de Tecnologia da Informação

DOD 3/2022 - CTI/DG/SC/RE/IFRN

23 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Ricardo Luiz Azevedo Cacho	**Matrícula/SIAPE:**	1859799
E-mail:	ricardo.cacho@ifrn.edu.br	**Telefone**	(84) 4005-4110

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Ricardo Luiz Azevedo Cacho	**Matrícula/SIAPE:**	1859799
Cargo:	TECNOLOGO-FORMACAO - GERÊNCIA DE REDES	**Lotação:**	CTI/SC
E-mail:	ricardo.cacho@ifrn.edu.br	**Telefone**	(84) 4005-4110

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Ricardo Luiz Azevedo Cacho

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para possibilidade da ampliação da interconexão ao Datacenter IFRN, Projeto veredas (RNP) ou futura interconexão a Infovia Potiguar. Possibilitando o aumento da banda de comunicação do Campus Santa Cruz, que sairá de 100Mbps para 1Gbps. Além disso, a demanda foca na prevenção contra ataques cibernéticos, investigação de incidentes de segurança e atualização tecnológica.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026

ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade;	**M30**	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
1354	EQUIPAMENTO SEGURANÇA REDE

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus Santa Cruz.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus no momento não possui a possibilidade técnica de ampliação de velocidade dos links de internet, que estão atualmente limitados a 100Mbps com um link de transporte até o datacenter e 100 Mbps pelo projeto veredas. O atual modelo de firewall em atividade não suporta um aumento de taxa de transferência de dados

(throughput) superior a atual (250 Mbps), mas o Campus receberá o link de 1Gbps, por ocasião da ativação da Rede Infovia Potiguar, fato que aumentará substancialmente a capacidade de trafego na internet, desde que tenhamos um firewall que tenha taxa de transferência de dados (throughput) adequado;

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* São Paulo do Potengi;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Ricardo Luiz Azevedo Cacho - Matrícula 1859799.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Elizeu Oliveira do Monte Junior	**Matrícula/SIAPE:**	3152206
Cargo:	TEC DE TECNOLOGIA DA INFORMACAO	**Lotação:**	CTI/SC
E-mail:	elizeu.junior@ifrn.edu.br	**Telefone**	(84)4005-4110

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS

Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Marcelo Revoredo da Silva	**Matrícula/SIAPE:**	1162359
Cargo:	ASSISTENTE EM ADMINISTRACAO	**Lotação:**	DIAD/SC
E-mail:	marcelo.revoredo@ifrn.edu.br	**Telefone**	(84)4005-4110
Nome:	Bruno de Paiva e Silva Castro	**Matrícula/SIAPE:**	1058871
Cargo:	ASSISTENTE EM ADMINISTRACAO	**Lotação:**	COFINC/SC
E-mail:	castro.paiva@ifrn.edu.br	**Telefone**	(84)4005-4110
Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.			

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Estudo Técnico Preliminar - 13/2022

1. Informações Básicas

Número do processo: 23138.000788.2022-18

2. Descrição da necessidade

Adequação da infraestrutura de TI para interconexão a Rede infovia potiguar. Possibilitando o aumento considerável da banda de comunicação do Campus Santa Cruz, que sairá de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação Campus Santa Cruz	Ricardo Luiz Azevedo Cacho

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus Santa Cruz do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de throughput de 1 Gbps ou superior, em função de interligação desse Campus à Infovia Potiguar, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade. Atualmente o Campus Santa Cruz já dispõe de uma solução de firewall da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN. O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software. Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração. Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública; – As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus Santa Cruz se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus Santa Cruz. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL /SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas. Referência:https://www.gartner.com/en /information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus Santa Cruz do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- ANÁLISE COMPARATIVA DE SOLUÇÕES				
				Não

Requisito	Solução	Sim	Não	se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1 Solução 2 Solução 3 Solução 4	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

- COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
	Seguir um dos princípios			

Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à Infovia Potiguar	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus Santa Cruz, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do link de internet que o Campus receberá ao integrar a Infovia potiguar, o que proporcionará uma ampliação da banda de internet dos atuais 100 Mbps para 1Gbps; posto que o throughput da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de intenet. 2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-altonetworks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus Santa Cruz do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus Santa Cruz do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de internet do Campus Santa Cruz, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do Campus Santa Cruz do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo

possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus Santa Cruz do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus Santa Cruz do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das features segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação in-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); IPS; Visibilidade de Aplicativos de

forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

]Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus Santa Cruz do IFRN é a Solução 3: Firewall de Próxima Geração, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
01	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	**01**	R$126.769,08	R$126.769,08
Total				**R$126.769,08**

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

ID	Benefício
01	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

02	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
03	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
04	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
05	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
06	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
07	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
08	Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
09	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade

19. Responsáveis

RICARDO LUIZ AZEVEDO CACHO
TECNOLOGO-FORMACAO REDES/Coordenador de tecnologia da informação Campus Santa Cruz

ELIZEU OLIVEIRA DO MONTE JUNIOR
TEC DE TECNOLOGIA DA INFORMACAO

MARCELO REVOREDO DA SILVA
ASSISTENTE EM ADMINISTRACAO

BRUNO DE PAIVA E SILVA CASTRO
ASSISTENTE EM ADMINISTRACÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/SÃO GONÇALO DO AMARANTE

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS SÃO GONÇALO DO AMARANTE
Rua Prof. Carlos Guedes Alcoforado, S.N., S/N, Centro, SÃO GONÇALO DO AMARANTE / RN, CEP 59291-727
Fone: (84) 4005-4111

Ofício Nº 6/2022 - CTI/DG/SGA/RE/IFRN

23 de junho de 2022

Ao Senhor
Sergio de Carvalho Guedes
Diretor de Administração
IFRN, Campus São Gonçalo do Amarante

Assunto: Aquisição de *firewall*.

Senhor Diretor de Administração,

1. Solicito participação na IRP nº 3/2022 da UASG 158368 - Núcleo de Contratação do Campus Zona Norte do IFRN, para aquisição do material listado na tabela abaixo, no valor estimado de R$ 126.769,08 (cento e vinte e seis mil, setecentos e sessenta e nove reais e oito centavos).

2. Acrescento que esta aquisição visa aumentar a velocidade da conexão do Campus São Gonçalo do Amarante com a Internet, de 100Mbps para 1Gbps, bem como melhorar a segurança da informação, conforme explicado no documento de oficialização de demanda e no estudo técnico preliminar.

Item	Descrição do produto	Unidade	Preço Unitário (R$)	Quantidade	Valor Total (R$)
1	Firewall de próxima geração	Unidade	R$ 126.769,08	1	R$ 126.769,08

Atenciosamente,

Documento assinado eletronicamente por:

- **Marcel Gleidson Bezerra de Freitas, COORDENADOR - FG0002 - CTI/SGA**, em 23/06/2022 14:32:49.

Este documento foi emitido pelo SUAP em 23/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418188
Código de Autenticação: e5f66b9a08

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS SÃO GONÇALO DO AMARANTE
Coordenação de Tecnologia da Informação

DOD 2/2022 - CTI/DG/SGA/RE/IFRN

23 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Marcel Gleidson Bezerra de Freitas	**Matrícula/SIAPE:**	1773680
E-mail:	marcel.freitas@ifrn.edu.br	**Telefone**	(84) 4005-4111

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Marcel Gleidson Bezerra de Freitas	**Matrícula/SIAPE:**	1773680
Cargo:	Tecnólogo-formação: Tecnologia da Informação	**Lotação:**	CTI/SGA
E-mail:	marcel.freitas@ifrn.edu.br	**Telefone**	(84) 4005-4111

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Marcel Gleidson Bezerra de Freitas

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para interconexão à Rede GigaNatal, de modo a possibilitar considerável enlarguecimento da banda de comunicação do Campus São Gonçalo do Amarante, que mudará de 100Mbps para 1Gbps.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
537	Aquisições - permanente - solução TIC - firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, inclusive contra redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros, e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações, ou acabam fazendo uso indevido dessas informações, ilegalmente obtidas, para vantagens próprias (vejamos os recentes ataques às instituições públicas como aos tribunais, STJ, TSE etc).

A constante modernização e ampliação dos aparatos de tecnologia da informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados, e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de *firewall* de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* São Gonçalo do Amarante do IFRN. O equipamento de firewall em operação, registrado com o número de patrimônio 310854, é do mesmo modelo e fabricante do *firewall* utilizado nos outros *campi* do IFRN, estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do *software* de gestão do mesmo fabricante dos *firewalls*, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (*hardware*) e sistema (*software*) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de *firewall* funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do *firewall* apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do Campus São Gonçalo do Amarante.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição de possibilitar que a solução de *firewall* existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, *antimalware*, *IPS*) etc, o *firewall* realiza a checagem do conteúdo acessado na *internet* pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acesso aos dados e sistemas da instituição. Esses *malwares* são criados e disseminados na *internet* a todo momento e, por isso, as bases de dados da solução de *firewall* necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do *firewall* se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do *firewall* existente nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do *Campus*; também, o *Campus* recebeu *link* de 1Gbps, devido à expansão da capacidade da Rede GigaNatal, fato que

aumenta substancialmente a capacidade de trafego na internet, desde que tenhamos um *firewall* com taxa de transferência de dados (*throughput*) adequado; posto que o atual *firewall* só disponibiliza de 100Mbps como taxa de transferência.

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* São Gonçalo do Amarante;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo *worms*, vírus, *malwares* entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de *hackers* através do bloqueio de aplicações como programas de compartilhamento de dados (*P2P*), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de *URL*, portas de serviços *TCP* e *UDP* (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.

Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**; - Conta Corrente SIAFI: **17116881000000000449052.**

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Marcel Gleidson Bezerra de Freitas - Matrícula 1773680.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Igor Wescley Silva de Freitas	**Matrícula/SIAPE:**	1974464
Cargo:	Técnico de Tecnologia da Informação	**Lotação:**	CTI/SGA
E-mail:	igor.freitas@ifrn.edu.br	**Telefone**	(84)4005-4111

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Igor Wescley Silva de Freitas - Matrícula 1974464.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS
Não se aplica.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC
Não se aplica.

ENCAMINHAMENTO
Encaminhe-se à autoridade competente da Área Administrativa, que deverá: I - Decidir motivadamente sobre o prosseguimento da contratação; II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10. **Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação:** André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE
Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO			
Nome:	Sergio de Carvalho Guedes	**Matrícula/SIAPE:**	1961942
Cargo:	Auxiliar em Administração	**Lotação:**	DIAD/SGA
E-mail:	sergio.guedes@ifrn.edu.br	**Telefone**	(84)4005-4111

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Sergio de Carvalho Guedes - Matrícula 1961942.

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Everson Mizael Cortez Silva - Matrícula 1735559 - substituto eventual conforme portaria nº 1306/2020 - RE/IFRN.

Documento assinado eletronicamente por:

- **Marcel Gleidson Bezerra de Freitas**, **COORDENADOR - FG0002 - CTI/SGA**, em 23/06/2022 14:10:00.
- **Sergio de Carvalho Guedes**, **DIRETOR - CD0004 - DIAD/SGA**, em 23/06/2022 15:18:32.
- **Igor Wescley Silva de Freitas**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 23/06/2022 15:06:30.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 23/06/2022 16:43:18.
- **Everson Mizael Cortez Silva**, **DIRETOR - SUB-CHEFIA - DG/SGA**, em 24/06/2022 07:49:47.

Este documento foi emitido pelo SUAP em 23/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 418177
Código de Autenticação: 61d56d78f4

Estudo Técnico Preliminar - 13/2022

1. Informações Básicas

Número do processo: 23425.001102.2022-71

2. Descrição da necessidade

Readequação da infraestrutura de TI para interconexão à Rede GigaNatal, possibilitando aumento considerável da banda de comunicação do Campus São Gonçalo do Amarante, mudando de 100Mbps para 1Gbps.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Marcel Gleidson Bezerra de Freitas

4. Necessidades de Negócio

1. Aquisição de solução de *firewall* de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de *firewall* de próxima geração;

2. Gerenciar a solução de *firewall* de próxima geração de maneira centralizada, a partir do *software* de gerenciamento centralizado, Paloalto Panorama, instalado e em uso na Reitoria do IFRN, otimizando a administração dos *appliances* e armazenamento de *logs*.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido às necessidades do *campus* São Gonçalo do Amarante do IFRN em adquirir uma solução de *firewall* de próxima geração cuja característica técnica atenda à capacidade de *throughput* de 1 Gbps ou superior, em

função de interligação desse *Campus* à Rede Giga Natal, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o *Campus* São Gonçalo do Amarante já dispõe de uma solução de *firewall* de próxima geração da Paloalto, a qual foi adquirido em 2015. Todos os *campi* e a Reitoria do IFRN possuem a *firewall*s de próxima geração da Paloalto, os quais são gerenciados e monitorados de forma centralizada através do *software* de gerenciamento centralizado Paloalto Panorama, instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação por equipamento (*hardware*) e sistema (*software*) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de *firewall* existente no Campus é o modelo PA-500 e está em uso na rede a mais de 6 anos de forma satisfatória, mas se encontra sem suporte e garantia, impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao *site* do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no *website* https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no *website* mencionado, a data final de cobertura de garantia para este modelo de produto é 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de *software*.

Como o *firewall* é um equipamento de extrema importância para proteção e funcionamento da rede, e que possibilita a conexão segura dos usuários remotos através de túneis *VPN*, se inexistente ou indisponível por falha de *hardware* ou *software*, pode comprometer os serviços administrativos e operacionais do *campus*. Portanto, dada a necessidade de modernização da solução de *firewall*, se faz necessária para este projeto a aquisição de solução de *firewall* de próxima geração.

Como o IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de *firewall* de próxima geração a ser adquirida seja compatível com o *software* de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

Grupo	Item	Descrição	Quantidade
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE *FIREWALL*	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do *ePing*, *eMag*, *ePwg*, ICP-Brasil e *e-ARQ* Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O *firewall* do Campus São Gonçalo do Amarante se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de *bugs* e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o *firewall* é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de *hardware* ou *software*, pode comprometer o acesso à *internet* e os serviços administrativos e operacionais do Campus São Gonçalo do Amarante. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: *Firewall UTM*

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O *UTM* é teoricamente uma evolução do *firewall* tradicional, unindo a execução de várias funções de segurança em um único dispositivo: *firewall*, prevenção de intrusões de rede, anti-vírus, *VPN*, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O *firewall UTM* está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do *UTM* é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de *logs*.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, *firewalls UTM* são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: *Firewall* de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *intrusion prevention system (IPS)*, anti-vírus, inspeção a nível de aplicação e usuários, inspeção de *SSL/SSH*, *VPN*, filtro de *websites* e gerenciamento de banda (*QoS*). O firewall de próxima geração nasceu em 2009 e é a evolução do *firewall UTM* , que além de prover a centralização das inspeções e correlação de *logs*, ainda entrega performance para redes de grande porte. O *firewall* de próxima geração permite: instalação *in-line* sem perda de performance; capacidades de *firewall* de primeira geração (ex. *NAT*, *Stateful Inspection Protocol*, *VPN* etc.); *IPS*; visibilidade de aplicativos de forma granular e decriptografia *SSL* para permitir a identificação de aplicações criptografadas indesejadas.

Referência:https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus *hardwares* e *softwares*, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao *Campus* São Gonçalo do Amarante do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não se adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	*Firewall UTM*
2	Renovar a solução atual
3	*Firewall* de próxima geração
4	Composição de soluções de segurança

9. Análise comparativa de soluções

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			
	Solução 3			
	Solução 4			
A solução está disponível no Portal do *Software* Público Brasileiro? (quando se tratar de *software*)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
A solução é composta por software livre ou *software* público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			

	Solução 4			
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo *ePing*, *eMag*, *ePWG*?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

COMPARAÇÃO DAS ALTERNATIVAS				
Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a expansão da Rede Giga-Natal.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de *software* da solução atualmente instalada no Campus São Gonçalo do Amarante, apesar de aparentemente representar a melhor solução em função da economia, encontra obstante por duas questões: 1) a atual caixa (PA-500) não atenderia a atualização do *link* de *internet* que o *Campus* recebe ao integrar a rede Giga Natal, atualização esta que proporciona uma ampliação da banda de *internet* dos atuais 100Mbps para 1Gbps; posto que o *throughput* da atual caixa limita-se aos 100 Mbps, o que impossibilitaria o uso dos recursos da atualização da banda de *internet*. 2) Não será possível valer-se do programa *Tech Refresh* ou *Hardware Refresh* da Paloalto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog /opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc),
pelo qual a Paloalto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no *Campus* será descontinuada pela Paloalto em agosto de 2023.

Solução 2: *Firewall UTM*

Para atender as necessidades do *Campus* São Gonçalo do Amarante do IFRN, o *UTM* deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do *Campus* São Gonçalo do Amarante do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que *softwares* de gerência são

proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de *captive portal*. O *UTM* não possui recursos para integração transparente com bases de usuário *LDAP*/*Active Directory* ou *captive portal*.

Quanto à atualização do *software* da caixa atualmente instalada já se verificou a impossibilidade de atendimento da atualização da banda de *internet* do *Campus* São Gonçalo do Amarante, que sairá do patamar de 100Mbs para 1Gbps.

E por fim, com o intuito de proteger os investimentos do *Campus* São Gonçalo do Amarante do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o *firewall UTM* não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus *hardwares* e *softwares*, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, a CTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o *Campus* São Gonçalo do Amarante do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de *Firewall* de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do *Campus* São Gonçalo do Amarante do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, das licenças de *software* que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do *Campus* - sendo uma

plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *intrusion prevention system* (*IPS*), anti-vírus, inspeção a nível de aplicação e usuários, inspeção de *SSL/SSH*, *VPN*, filtro de *websites* e gerenciamento de banda (*QoS*). O firewall de próxima geração nasceu em 2009 e é a evolução do *firewall UTM*, que além de prover a centralização das inspeções e correlação de *logs* ainda entrega performance para redes de grande porte. O *firewall* de próxima geração permite: instalação *in-line* sem perda de performance; capacidades de *firewall* de primeira geração (ex. *NAT*, *Stateful Inspection Protocol*, *VPN* etc.); *IPS*; visibilidade de aplicativos de forma granular e decriptografia *SSL* para permitir a identificação de aplicações criptografadas indesejadas.

Fez-se a pesquisa de preços com base no site de registros de preço do Governo Federal. A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05/2014 da Secretária de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar estadunidense, e tendo a moeda estadunidense sofrido intensa oscilação em relação ao real, principalmente no ano de 2020, e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da pandemia de COVID-19 e às demais instabilidades globais, como a guerra da Ucrânia, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidade)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o *Campus* São Gonçalo do Amarante do IFRN é a **solução 3: *firewall* de próxima geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: firewall de próxima geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, *software* este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos *campi* e Reitoria do IFRN.

A solução de *firewall* de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de *UTM*, conforme demonstrado neste estudo, o que torna a solução de *firewall* de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1) Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente.

2) Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim.

16. Benefícios a serem alcançados com a contratação

ID	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da *Internet*.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
	Criação de políticas de proteção da rede contra ataques de *hackers* através do bloqueio ou sancionamento de aplicações

8	como programas de compartilhamento de dados (*P2P*), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de *URL*, portas de serviços *TCP* e *UDP* (por grupo ou usuário);
10	Filtro de conteúdo *URL*, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de *firewall* de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e *logs* intuitivos para análises especificas e sendo tal solução compatível com o *software* de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, *software* este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos *campi* e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de *UTM*, conforme demonstrado neste estudo, o que torna a solução de *firewall* de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

Aprovação válida com assinatura eletrônica da autoridade máxima da área de TIC.

ANDRÉ GUSTAVO DUARTE DE ALMEIDA

Diretor de Gestão de Tecnologia da Informação

Aprovação válida com assinatura eletrônica do integrante requisitante neste documento.

MARCEL GLEIDSON BEZERRA DE FREITAS

Coordenador de Tecnologia da Informação

Aprovação válida com assinatura eletrônica do integrante técnico neste documento.

IGOR WESCLEY SILVA DE FREITAS

Técnico de Tecnologia da Informação

Documento Digitalizado Público

ETP 13/2022

Assunto: ETP 13/2022
Assinado por: Marcel Freitas
Tipo do Documento: Estudo preliminar - contratos
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Marcel Gleidson Bezerra de Freitas**, **COORDENADOR - FG0002 - CTI/SGA** , em 24/06/2022 10:12:32.

Este documento foi armazenado no SUAP em 24/06/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1104791
Código de Autenticação: d719c3ff12

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

IFRN/SÃO PAULO DO POTENGI

DOCUMENTAÇÃO DE PARTICIPAÇÃO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS SÃO PAULO DO POTENGI
Coordenação de Tecnologia da Informação

DOD 1/2022 - CTI/DG/SPP/RE/IFRN

21 de junho de 2022

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução. **Referência: Art. 10 da IN SGD/ME nº 01/2019.**

1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE			
Área Requisitante	Coordenação de Tecnologia da Informação		
Responsável pela demanda:	Alex Augusto de Souza Santos	**Matrícula/SIAPE:**	1928999
E-mail:	alex.santos@ifrn.edu.br	**Telefone**	(84) 4005-4112

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE			
Nome:	Alex Augusto de Souza Santos	**Matrícula/SIAPE:**	1928999
Cargo:	Técnico Laboratório/ Área	**Lotação:**	CTI/SPP
E-mail:	alex.santos@ifrn.edu.br	**Telefone**	(84) 4005-4112

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Requisitante neste documento: Alex Augusto de Souza Santos

3 - IDENTIFICAÇÃO DA DEMANDA
Necessidade da Contratação
Adequação da infraestrutura de TI para possibilidade da ampliação da interconexão ao Datacenter IFRN, Projeto veredas (RNP) ou futura interconexão a Rede GigaNatal. Possibilitando o aumento da banda de comunicação do Campus São Paulo do Potengi com a Internet para velocidades superiores ao que podem ser alcançadas hoje em dia. Além disso, a demanda foca na prevenção contra ataques cibernéticos, investigação de incidentes de segurança e atualização tecnológica.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
Objetivos Estratégicos		**Nome do documento <vigência>**
GI-4	Consolidar a gestão de TI. Garantir a conectividade, a disponibilidade e a melhoria contínua dos sistemas de informação para prover suporte às atividades acadêmicas e de gestão.	PDI 2019-2026
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.	PDI 2019-2026

O-11	Garantia da segurança das plataformas de governo digital e de missão crítica	EGD 2020-2022

Legenda:
GI-4: Objetivo 4 da Perspectiva Gestão e Infraestrutura do Plano de Desenvolvimento Institucional do IFRN;
ES-3: Objetivo 3 da Perspectiva Estudante e Sociedade do Plano de Desenvolvimento Institucional do IFRN;
O-11: Objetivo 11, da Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020).

ALINHAMENTO AO PDTIC 2021-2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	Desenvolver projeto para avaliação de solução de conectividade;	**M30**	Prover o serviço de links de conectividade e internet institucionais.
A2	Realizar licitação/aquisição de links de conectividade.	**M30**	Prover o serviço de links de conectividade e internet institucionais.

ALINHAMENTO AO PAC 2022	
Item	**Descrição**
44	Materiais e Serviços - Firewall

4 - MOTIVAÇÃO/JUSTIFICATIVA

Com o avanço constante da tecnologia cibernética, os hackers também avançam e desenvolvem novas técnicas de ataques maliciosos, sejam em redes corporativas, de instituições públicas ou privadas, com o objetivo de sequestrar arquivos, roubar dados pessoais ou informações corporativas privilegiadas e importantes. Os criminosos virtuais podem ter diversos objetivos obscuros e atingiram tal ponto de ousadia que muitas vezes chegam a manter informações ou dados muito importantes criptografados como reféns, até que a pessoa ou instituição pague um determinado valor (geralmente em criptomoeda) como resgate pela liberação destas informações ou acabam fazendo uso indevido dessas informações ilegalmente obtidas para vantagens próprias (vejamos os recentes ataques às instituições públicas como os tribunais - STJ, TSE, etc).

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição faz crescer a preocupação dos gestores de segurança da informação sobre a proteção da rede, dos dados trafegados e da privacidade dos seus colaboradores. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, que descreve aprimoramentos e regras de segurança no ambiente de TI visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que instituições públicas e privadas invistam cada vez mais em recursos tecnológicos para aprimorar sua segurança da informação.

A contratação de suporte técnico especializado em soluções de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do *Campus* São Paulo do Potengi do IFRN. O equipamento de firewall em operação, adquirido em 2016 através da licitação 27/2015 - UASG 158155, é do mesmo modelo e fabricante do firewall utilizado nos outros *Campi* do IFRN e estando todos os equipamentos gerenciados e monitorados, de forma centralizada, através do software de gestão, do mesmo fabricante dos firewalls, instalado na Reitoria do IFRN, sendo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O sistema de firewall funciona como um filtro eletrônico que examina o tráfego de dados da rede, sinalizando e protegendo as operações de transmissão ou recebimento de dados conforme regras, permissões e perfis de proteção que são realizadas dentro de suas configurações. Devido a essa característica, o adequado funcionamento do firewall apresenta-se como um elemento crucial para operação e segurança cibernética dos serviços tecnológicos no âmbito do campus São Paulo do Potengi.

A demanda evidenciada pela equipe de tecnologia da informação do *Campus* tem como base as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

Ademais, por ser uma solução de firewall de próxima geração, que possui controle de aplicações em camada 7, identificação de usuários, gerenciamento unificado de ameaças (anti-vírus, anti-malware, IPS), etc., o firewall realiza a checagem do conteúdo acessado na internet pelos usuários, internos e externos, protegendo os componentes envolvidos de ameaças que podem causar interrupção no funcionamento dos computadores da rede local e, consequentemente, causar a interrupção das atividades de acessos aos dados e sistemas da instituição. Esses malwares são criados e disseminados na internet a todo momento e, por isso, as bases de dados da solução de firewall necessitam de uma constante atualização junto ao fabricante.

Portanto, a atualização das assinaturas dos serviços de suporte/garantia e das proteções contra ameaças presentes na solução existente se mostra de extrema importância, pois garante que a base de dados, assinaturas e correções do sistema operacional do firewall se mantenham atualizadas e íntegras.

Sendo assim, para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos, se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no *Campus* protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus no momento não possui a possibilidade técnica de ampliação de velocidade dos links de internet, que estão atualmente limitados a 150Mbps com um link de transporte até o datacenter e 100 Mbps pelo projeto veredas. O atual modelo de firewall em atividade não suporta um aumento de taxa de transferência de dados (throughput) superior a atual (250 Mbps).

5 - RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

1. Adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3. Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4. Atualizações constantes das proteções da rede do *Campus* São Paulo do Potengi;
5. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
6. Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
7. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
8. Geração de relatórios dos acessos realizados por IP, grupo, aplicação ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
9. Criação de políticas de proteção da rede contra-ataques de hackers através do bloqueio de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
10. Regras de bloqueio e liberação de aplicações de camada 7, categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
11. Ampliação da satisfação da comunidade do IFRN com ampliação da capacidade do link de Internet, a partir da ampliação da banda de comunicação do Campus.
12. Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

6 - FONTE

MC - Rotinas da Administração – PROAD

Código 4 - Etapa: Aquisição de material permanente

Origem de Recursos SUAP: **MA.20RL.171168.4** - Otimização dos gastos com contratos continuados; PI: **L20RLP60MCN**;
- Conta Corrente SIAFI: **171168810000000044905 2**.

ENCAMINHAMENTO

Encaminhe-se ao Diretor de Gestão de Tecnologia da Informação e Comunicação para providências.

Encaminhamento válido com assinatura eletrônica do titular da Área Requisitante da Demanda: Alex Augusto de Souza Santos - Matrícula 1928999.

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:	Alex Augusto de Souza Santos	**Matrícula/SIAPE:**	1928999
Cargo:	Técnico Laboratório /Área	**Lotação:**	CTI/SPP

E-mail:	alex.santos@ifrn.edu.br	**Telefone**	(84)4005-4112

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Técnico neste documento: Alex Augusto de Souza Santos - Matrícula 1928999.

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS

Acúmulo dos papéis de integrante requisitante e integrante técnico ocorre devido a não existência de outro servidor lotado no campus na área de TI.

JUSTIFICATIVA PARA A DESIGNAÇÃO DE DIRIGENTE DA ÁREA DE TIC

Não se aplica.

ENCAMINHAMENTO

Encaminhe-se à autoridade competente da Área Administrativa, que deverá:

I - Decidir motivadamente sobre o prosseguimento da contratação;

II - Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e

III - Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10.

Encaminhamento válido com assinatura eletrônica do titular da Área de Tecnologia da Informação: André Gustavo Duarte de Almeida - Matrícula 1577655.

8 - DECISÃO DA AUTORIDADE COMPETENTE

Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante e indico o representante abaixo para a área administrativa.

9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Nome:	Gabriel Lacerda de Paula	**Matrícula/SIAPE:**	2825343
Cargo:	Administrador	**Lotação:**	DIAD/SPP
E-mail:		**Telefone**	(84)4005-4112

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

Declaração válida com assinatura eletrônica do Integrante Administrativo neste documento: Gabriel Lacerda de Paula - Matrícula 2825343

Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o inciso IV do art. 2º e o inciso III do §2º do art. 10, da IN SGD/ME nº 01/2019.

Conforme o art. 29, §8º da IN SGD/ME nº 01/2019, a equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato / emissão da nota de empenho.

Declaração válida com assinatura eletrônica da Autoridade Competente da Área Administrativa neste documento: Gabriel Lacerda de Paula - Matrícula 2825343

Documento assinado eletronicamente por:

- **Alex Augusto de Souza Santos**, **COORDENADOR - FG0002 - CTI/SPP**, em 21/06/2022 12:02:31.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 21/06/2022 12:09:23.
- **Gabriel Lacerda de Paula**, **ADMINISTRADOR**, em 22/06/2022 08:55:30.

Este documento foi emitido pelo SUAP em 21/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417130
Código de Autenticação: 85d48565e7

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS SÃO PAULO DO POTENGI
RN-120, Km 2, Novo Juremal, S/N, 241260905, SÃO PAULO DO POTENGI / RN, CEP 59460-000
Fone: (84) 4005-4112

Termo 4/2022 - CTI/DG/SPP/RE/IFRN

TERMO DE PARTICIPAÇÃO

AO IFRN, CAMPUS NATAL Z NORTE
UASG nº: 158368 - IRP n°. 03/2022

1. OBJETO

Esta Unidade Gestora, em atendimento ao que preconiza o Art. 6º do Decreto n° 7.892/2013, manifesta total concordância com o objetivo a ser licitado, bem como todas as condições estabelecidas no Termo de Referência do órgão gestor, referente à IRP n° 03/2022, cujo objeto é a aquisição de solução de firewall de próxima geração.

2. JUSTIFICATIVA DA NECESSIDADE

Aquisição de firewall de próxima geração (NGFW) atender as necessidades do campus São Paulo do Potengi. Para manter o bom nível de segurança da rede de computadores e a consequente disponibilidade dos serviços de tecnologia ofertados para os seus usuários, internos e externos. se faz necessária a atualização do firewall existentes nessa instituição, por outro de mesma tecnologia e gerenciável pelo Panorama, com o intuito de manter a rede de computadores e as informações armazenadas no Campus protegidas e preservar o investimento realizado pela instituição. A necessidade de substituição alinha-se a duas condições: o atual modelo PA-500 será descontinuado pelo fabricante em 2023, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI do Campus; também, o Campus no momento não possui a possibilidade técnica de ampliação de velocidade dos links de internet, que estão atualmente limitados a 150Mbps com um link de transporte até o datacenter e 100 Mbps pelo projeto veredas. O atual modelo de firewall em atividade não suporta um aumento de taxa de transferência de dados (throughput) superior a atual (250 Mbps).

Em observância ao princípio da eficiência, dessa forma optamos em aderir, junto a esse Órgão Gerenciador de licitação, na situação de “PARTICIPANTE”, em virtude da economia de meios, praticidade e das vantagens econômicas proporcionadas pelo Sistema de Registro de Preços.

3. DA ENTREGA E DO RECEBIMENTO DO OBJETO

O local de prestação do serviço será: IFRN- São Paulo do Potengi RN 120, Km 2, Bairro: Novo Juremal, São Paulo do Potengi/RN , CEP: 59460-000, contatos pelo telefone (84) 4005-4112 Ramal 7649 – e-mail institucional: fagner.castro@ifrn.edu.br

4. DEMONSTRATIVO E JUSTIFICATIVA DAS NECESSIDADES

As quantidades solicitadas foram cadastradas no SIASGNET conforme abaixo:

N° do Item	Tipo de Item	Item
1	Material	481646-Equipamento Segurança Rede

5. MANIFESTAÇÃO DE CONCORDÂNCIA COMAS CONDIÇÕES DO TERMO DE REFERÊNCIA

O Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte – Campus São Paulo do Potengi, manifesta que aceita as condições contidas no Termo de Referência elaborado pelo órgão gerenciador do certame.

Alex Augusto de Souza Santos (1928999)
Responsável Solicitante

Renato Dantas Rocha da Silva (1923399)
Ordenador de Despesas

Documento assinado eletronicamente por:

- **Renato Dantas Rocha da Silva**, **Diretor-Geral do Campus São Paulo do Potengi - CD0002 - DG/SPP**, em 22/06/2022 11:39:22.
- **Alex Augusto de Souza Santos**, **COORDENADOR - FG0002 - CTI/SPP**, em 22/06/2022 09:56:42.

Este documento foi emitido pelo SUAP em 22/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417575
Código de Autenticação: af124330e9

Estudo Técnico Preliminar - 10/2022

1. Informações Básicas

Número do processo: 23515.000972.2022-13

2. Descrição da necessidade

Aquisição de Solução de Firewall de Próxima Geração para o campus São Paulo do Potengi. A solução prevê adequação da infraestrutura de TI para possibilidade da ampliação da interconexão ao Datacenter IFRN, Projeto veredas (RNP) ou futura interconexão a Rede GigaNatal. Possibilitando o aumento da banda de comunicação do Campus São Paulo do Potengi com a Internet para velocidades superiores ao que podem ser alcançadas hoje em dia.

Além disso, a demanda foca na prevenção contra ataques cibernéticos, investigação de incidentes de segurança e atualização tecnológica.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação	Alex Augusto de Souza Santos

4. Necessidades de Negócio

1. Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;

2. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

3. Manter a integridade dos dados e das informações sensíveis dos sistemas do campus;

4. Melhorar o nível de qualidade ser serviço das aplicações internas do campus.

5. Necessidades Tecnológicas

1. Adquirir uma solução de firewall de próxima geração;

2. Gerenciar a solução de firewall de próxima geração de maneira centralizada, a partir do software de gerenciamento centralizado Palo Alto Panorama em uso e instalado na Reitoria do IFRN, otimizando a administração dos appliances e armazenamento de logs.

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

1. Aproveitar todo conhecimento sobre a solução existente já desprendido pelo departamento de TI da instituição;

2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7. Estimativa da demanda - quantidade de bens e serviços

Devido as necessidades do campus São Paulo do Potengi do IFRN em adquirir uma solução de firewall de próxima geração cuja característica técnica atenda a capacidade de *throughput* de 1 Gbps ou superior, em função de necessidade atual e futura de interligação desse Campus à redes de maiores velocidades, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Atualmente o Campus São Paulo do Potengi já dispõe de uma solução de firewall de próxima geração da Palo Alto, a qual foi adquirido em 2016. Todos os campi e a Reitoria do IFRN possuem a solução de firewall de próxima geração da Palo Alto, os quais são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na Reitoria do IFRN, constituindo assim uma plataforma de segurança da informação constituída por equipamento (hardware) e sistema (software) que objetiva a proteção da rede de computadores de todo o IFRN.

O modelo de equipamento de firewall existente no Campus é o modelo PA-500 e está em uso na rede a mais de 3 anos de forma satisfatória, mas se encontra sem suporte e garantia impossibilitando o acionamento de suporte técnico especializado em caso de problema. Em consulta ao site do fabricante foi verificado que tal equipamento foi descontinuado, conforme pode ser consultado no website https://www.paloaltonetworks.com /services/support/end-of-life-announcements/hardware-end-of-life-dates, e, conforme informação constante no website mencionado, a data final de cobertura de garantia para este modelo de produto será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração.

Como a IFRN possui um sistema unificado de gestão centralizada das configurações e monitoramento dos equipamentos, o que traz maior agilidade e rapidez nas atividades do uso diário e administração da solução, geração de relatórios e nas atividades de investigação caso ocorra algum incidente de segurança, é necessário que solução de firewall de próxima geração a ser adquirida seja compatível com o software de gerenciamento centralizado instalado e em uso na Reitoria do IFRN.

GRUPO	Item	Descrição	QTD
1	1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	1

8. Levantamento de soluções

Conforme inciso II do art. 11 da IN SGD/ME nº 1/2019, deve-se verificar para composição da análise comparativa:

– A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

– As alternativas do mercado;

– A existência de software público brasileiro;

– As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

– As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

– A possibilidade de aquisição na forma de bens ou contratação como serviço;

– Os diferentes modelos de prestação do serviço;

– Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

– A ampliação ou substituição da solução implantada.

Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

Solução 1: Renovar a solução atual

O firewall do Campus São Paulo do Potengi se encontra operante e em conformidade com suas especificações, porém desatualizado em relação a suporte, garantia, atualizações do sistema operacional, para correção de bugs e novas funcionalidades, bem como proteções contra ameaças. Isso colocando em risco a rede do Campus, sendo necessária a aquisição de licenças para a renovação de suporte e garantia e das proteções contra ameaças, mantendo assim essa rede íntegra e protegida.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede, se inexistente ou indisponível, por falha de hardware ou software, pode comprometer o acesso à internet e os serviços administrativos e operacionais do Campus São Paulo do Potengi. Portanto, manter a solução com suporte e garantia ativos e vigentes é de extrema importância para a instituição, mantendo assim a proteção e operação 24/7 de todo ambiente.

Solução 2: Firewall UTM

Unified Threat Management (UTM), que é na tradução literal para o português "Central Unificada de Gerenciamento de Ameaças", é uma solução abrangente, criada para o setor de segurança de redes. O UTM é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede. O Firewall UTM está no mercado desde 2004, e desde então tem ganhado muito espaço. A principal característica do UTM é centralizar diversas funcionalidades de segurança em um único equipamento, facilitando dessa forma o gerenciamento e a correlação de logs.

Sua principal fraqueza é a performance, onde em muitos casos quando todos os módulos de inspeção são ativados simultaneamente, o equipamento trava. Sendo assim, firewalls UTM são muito bem aceitos em redes de pequeno e médio porte, onde o volume de dados é relativamente pequeno.

Referência: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

Solução 3: Firewall de Próxima Geração

É uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall

UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

Referência: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários treinamentos para cada fabricante.

Por contar com uma quantidade de funcionários reduzida, o que inviabilizaria a administração da rede, o setor de TI, para suportar as demandas da segurança da informação, dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus ao Campus São Paulo do Potengi do IFRN. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato. Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes, equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Além disso, esta solução não adequa às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

IDENTIFICAÇÃO DAS SOLUÇÕES	
ID	**Descrição da solução (ou cenário)**
1	**Firewall UTM**
2	**Renovar a solução atual**
3	**Firewall de Próxima Geração**
4	**Composição de soluções de segurança**

9. Análise comparativa de soluções

- 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			
	Solução 3			

	Solução 4			
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 Solução 2 Solução 3 Solução 4			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da soluçao abranger documentos arquivísticos)	Solução 1 Solução 2 Solução 3 Solução 4			X

3 - COMPARAÇÃO DAS ALTERNATIVAS

Critérios	**Justificativa para o critério**	**Avaliação da Alternativa 1**	**Avaliação da Alternativa 2**	**Avaliação da Alternativa 3**
Economicidade, aderências às especificações técnicas, prazo de entrega, etc.	Seguir um dos princípios constitucionais que regem a Administração Pública: efetividade; do qual decorre a economicidade para a coisa pública.	A renovação da atual solução acarretaria descumprimento ao princípio da eficiência e economicidade; uma vez que não solucionaria a necessidade de alteração da taxa de transmissão, para atender a interligação à redes de velocidades superiores a 250 Mbps.	-	-

10. Registro de soluções consideradas inviáveis

Solução 1: Renovar a solução atual

A renovação da licença de software da solução atualmente instalada no Campus São Paulo do Potengi, apesar de aparentemente representar a melhor solução em função da economia, encontra obste por duas questões:

1) a atual caixa (PA-500) não atenderia um upgrade de velocidade, estando defasada tecnologicamente; posto que o throughput da atual caixa limita-se aos 100 Mbps com recursos de segurança ativados.

2) Não será possível valer-se do programa Tech Refresh ou Hardware Refresh da Palo Alto, conforme se verifica no site (https://insights-cvdgroup-com.translate.goog/opinions/palo-alto-networks-hardware-refresh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc), pelo qual a Palo Alto atualizaria a caixa de PA-500 para PA-850; uma vez que a burocracia decorrente do processo público inviabilizou o enquadramento no período mínimo necessário para realização do programa (mínimo de 3 anos de renovação da licença). Considerando que a caixa hoje existente no Campus será descontinuada pela Palo Alto em agosto de 2023.

Solução 2: Firewall UTM

Para atender as necessidades do Campus São Paulo do Potengi do IFRN, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais com estoque de sobressalentes e treinamentos, já que este último não está disponível na localidade do Campus São Paulo do Potengi do IFRN, envolvendo custos indiretos de deslocamento e diárias, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de equipamentos de terceiros, ou seja, seria necessária a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução;

Outro ponto elencado como uma das necessidades desta solução é a integração da solução com uma base de usuários ou criação de captive portal. O UTM não possui recursos para integração transparente com bases de usuário LDAP / Active Directory ou captive portal.

Quanto a atualização do software da caixa atualmente instalada já se verificou a impossibilidade de atendimento de eventual atualização da banda de Internet do Campus São Paulo do Potengi.

E por fim, com o intuito de proteger os investimentos do Campus São Paulo do Potengi do IFRN para adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

Solução 4: Composição de soluções de segurança

A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. São necessários diversos treinamentos para operação dos equipamentos, que apesar de similares trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada fabricante.

Por contar com um quantitativo reduzido de funcionários para a administração da rede, o NTI dependeria constantemente da contratação de empresas especializadas para solucionar problemas técnicos, o que traria ônus para o Campus São Paulo do Potengi do IFRN.

Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.

Manter e gerenciar uma solução totalmente redundante com diversos equipamentos de fabricantes diferentes acarreta custo operacional elevado, bem como alto custo de renovação de contrato.

Dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

11. Análise comparativa de custos (TCO)

A única solução viável é a solução 3 - Aquisição de Firewall de Próxima Geração.

Solução Viável 1
Custo Total de Propriedade - Memória de Cálculo

O presente estudo contempla toda solução necessária para atender a demanda requisitada pela Coordenação de Tecnologia da Informação do Campus São Paulo do Potengi do IFRN através do Documento Oficial da Demanda.

Dado que a solução a ser contratada consiste na aquisição de um equipamento e, consequentemente, as licenças de software que possibilitam a ativação das *features* segurança necessárias à proteção da rede de computadores do Campus - sendo uma plataforma de rede integrada baseada em inspeção profunda (*deep packet inspection*), provendo múltiplos mecanismos de proteção em um único equipamento, tais como *Intrusion Prevention System* (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O Firewall de Próxima Geração permite: Instalação *in-line* sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, *Stateful Inspection Protocol*, VPN, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas - se fez a pesquisa de preços com base no site de registros de preço do Governo Federal.

A pesquisa de preços atende aos pré-requisitos definidos nos incisos I, II e parágrafo 2º do Artigo 2º da INº 05 /2014 da Secretária De Logística E Tecnologia Da Informação Do Ministério Do Planejamento, Orçamento E Gestão. Tendo sido encontrado apenas 3 aquisições semelhantes no âmbito da Administração Pública e que atendesse aos critérios anteriormente citados, a metodologia utilizada foi a da média dos valores encontrados.

Além disso, cabe destacar que se trata de uma solução importada e, portanto, cotada em dólar, e tendo a moeda americana sofrido intensa oscilação, principalmente no ano de 2020 e com uma forte tendência de alta no ano de 2021 e período inicial do ano de 2022, tendo registrado tendência de baixa no final do mês de Março de 2022, no entanto, devido ao cenário de instabilidade econômica resultante da Pandemia de COVID-19 e às demais instabilidades globais como a Guerra da Ucrânia e inflação global, que resultam em maior volatilidade do câmbio, destacamos que os preços encontrados podem apresentar defasagens, para mais ou para menos, a depender da cotação cambial durante o período licitatório.

UASG	PREGÃO	ITEM	DATA HOMOLOGAÇÃO	R$
154419	22/2021	2	29/12/2021	R$113.000,00
150182	75/2021	4	09/02/2022	R$149.707,25
153103	62/2020	3	13/10/2021	R$117.600,00
Total				R$380.307,25
Preço médio estimado por unidade				R$126.769,08
Preço médio total estimado a ser contratado (1 unidades)				R$126.769,08

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**	**Ano 4**	
Solução Viável 1	R$ 126.769,08	-	-	R$126.769,08	**R$ 253.538,16**

12. Descrição da solução de TIC a ser contratada

Como visto no estudo das análises comparativas de custos, a melhor e mais viável solução para o Campus São Paulo do Potengi do IFRN é a **Solução 3: Firewall de Próxima Geração**, pois além de melhor custo-benefício em diversas questões técnicas, atende na totalidade os requisitos esperados pela Coordenação de Tecnologia da Informação.

13. Estimativa de custo total da contratação

Valor (R$): 126.769,08

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO				
ID	Bem / Serviço	Quantidade	Valor unitário estimado	Valor total estimado
1	SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL	01	R$126.769,08	R$126.769,08
Total				R$126.769,08

14. Justificativa técnica da escolha da solução

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software

este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

15. Justificativa econômica da escolha da solução

1. Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;

Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;

16. Benefícios a serem alcançados com a contratação

D	Benefício
1	Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2	Economia com gastos desnecessários de capacitação da equipe de TI, aproveitando legado existente;
3	Padronização da tecnologia, conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), facilitando a administração da solução em casos específicos de suporte, assistência ou algo do gênero, não sendo necessário administrar vários pontos de contato para este fim;
4	Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
5	Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
6	Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
7	Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
8	Criação de políticas de proteção da rede contra ataques de hackers através do bloqueio ou sancionamento de aplicações como programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
9	Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
10	Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

17. Providências a serem Adotadas

Não há necessidade de adequação, tendo em vista que já existe todo uma estrutura pronta e em uso para solução PA-500 que pode ser utilizada.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Solução 3: Firewall de Próxima Geração

Como demonstrado ao longo deste estudo, a melhor e mais viável solução seria adquirir uma solução de firewall de próxima geração que atenda aos requisitos técnicos de performance, considerando ainda todos os requisitos de proteções contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises especificas e sendo tal solução compatível com o software de gerenciamento centralizado em uso e instalado na Reitoria do IFRN, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pelos Campi e Reitoria do IFRN.

A solução de firewall de próxima geração não apresenta problema de performance quando habilitados todos os seus recursos de inspeção, sendo este um problema conhecido das soluções de UTM, conforme demonstrado neste estudo, o que torna a solução de firewall de próxima geração mais duradoura do ponto de vista tecnológico e financeiro, pois preserva o investimento realizado com a longevidade.

19. Responsáveis

Aprovação válida com assinatura eletrônica da Autoridade Máxima da Área de TIC conforme Portaria nº 657/2022 - RE/IFRN.

ALEX AUGUSTO DE SOUZA SANTOS

Integrante técnico / Membro requisitante

ANDRE GUSTAVO DUARTE DE ALMEIDA

Diretor de Gestão de TI

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
REITORIA
Rua Dr. Nilo Bezerra Ramalho, 1692, Tirol, Natal/RN - CEP 59015-300
Fone: (84) 4005-0768, (84) 4005-0750

TERMO DE APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

PROCESSO Nº 23515.000972.2022-13

Estudo preliminar 10/2022 - DIAD/DG/SPP/RE/IFRN

OBJETO: Solução de firewall de próxima geração

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

(assinado eletronicamente)
Alex Augusto de Souza Santos
Matrícula SIAPE nº 1928999

Membro Requisitante / Técnico

(assinado eletronicamente)
Andre Gustavo Duarte de Almeida
Matrícula SIAPE nº 1577655
Diretor de Gestão de TI

Autoridade máxima da Área de TIC

Documento assinado eletronicamente por:

- **Alex Augusto de Souza Santos**, **COORDENADOR - FG0002 - CTI/SPP**, em 21/06/2022 15:35:57.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 21/06/2022 16:22:52.

Este documento foi emitido pelo SUAP em 21/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 417303
Código de Autenticação: 077bd81cd9

Documento Digitalizado Público

Documentação dos participantes da IRP

Assunto: Documentação dos participantes da IRP
Assinado por: Ives Silva
Tipo do Documento: Relatório
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original e Cópia

Documento assinado eletronicamente por:

- **Ives Bruno de Lima Silva**, **ASSISTENTE EM ADMINISTRACAO**, em 29/06/2022 08:39:12.

Este documento foi armazenado no SUAP em 29/06/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifrn.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1108491
Código de Autenticação: 154b6e691b