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

IFRN/ZONA NORTE

ESTUDO TÉCNICO PRELIMINAR

P.S. O IFRN/Zona Norte é o órgão gerenciador do processo. Ele é o responsável pelo Polo Metropolitano. O presente processo foi aberto pelo IFRN/Ceará-Mirim, pertencente ao polo metropolitano, contudo as quantidades e o ETP do IFRN/Zona Norte foram ignorados, até agora.

Estudo Técnico Preliminar - 16/2022

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

Aquisição de Solução de Firewall de Próxima Geração para o campus Natal-Zona Norte. 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 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	Manoel Soares do Couto Neto (1672943)

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 Natal-Zona Norte 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 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 Natal-Zona Norte 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 Natal-Zona Norte 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	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			
	Solução 2			X
	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

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 Natal-Zona Norte, 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 Natal-Zona Norte 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 Natal-Zona Norte 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.

E por fim, com o intuito de proteger os investimentos do Campus Natal-Zona Norte 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 Natal-Zona Norte 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 Natal-Zona Norte do IFRN.

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 Natal-Zona Norte 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

Após todas as considerações registradas nos itens anteriores, esta Comissão de Planejamento aponta como viável a contratação considerando a essencialidade da demanda, o alinhamento com o Plano Anual de Contratações (PAC) do IFRN, e pelo fato da solução apontada revelar-se calcada nos normativos que regem a matéria, resguardando assim a imprescindível legalidade e o interesse público, consoante o inciso XIII, art 7º da IN 40 de 22 de maio de 2020, da SEGES /ME. Por fim, o atendimento desta demanda será por meio de Intenção de Registro de Preço, conduzida pela que se encontra aberta para manifestação, tornando o campus Natal - Zona Norte órgão participante.

19. Responsáveis

MANOEL SOARES DO COUTO NETO

Coordenador de Tecnologia da Informação - Substituto Eventual

ABINOAM SOARES DA SILVA

Diretor de Administração

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS NATAL - ZONA NORTE
Rua Brusque, Conjunto Santa Catarina, 2926, Potengi, NATAL / RN, CEP 59112-490
Fone: (84) 4006-9505

ESTUDO PRELIMINAR

PARTICIPAÇÃO NA INTENÇÃO DE REGISTRO DE PREÇO Nº 03/2022

UASG 158368 - POLO METROPOLITANO

ESTUDO TÉCNICO PRELIMINAR Nº 16/2022- ASSINATURA DIGITAL

OBJETO: **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.**

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

NOME	MATRÍCULA
Manoel Soares do Couto Neto	1672943
Abinoam Soares da Silva	1845427

APROVAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

A autoridade competente do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - Campus Natal-Zona Norte, APROVA o presente Estudo Preliminar.

_____

EDMILSON BARBALHO CAMPOS NETO
Diretor Geral
Campus Natal-Zona Norte

Documento assinado eletronicamente por:

- **Edmilson Barbalho Campos Neto**, **DIRETOR GERAL - CD0002 - DG/ZN**, em 27/06/2022 08:48:56.
- **Manoel Soares do Couto Neto**, **COORDENADOR - SUB-CHEFIA0002 - CTI/ZN**, em 23/06/2022 15:11:35.
- **Abinoam Soares da Silva**, **Diretor de Administração - CD0004 - DIAD/ZN**, em 23/06/2022 15:12:20.

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: 417800
Código de Autenticação: 08be12c817

Documento Digitalizado Público

ETP do IFRN/Zona Norte

Assunto: ETP do IFRN/Zona Norte
Assinado por: Ives Silva
Tipo do Documento: Relatório
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Ives Bruno de Lima Silva**, **ASSISTENTE EM ADMINISTRACAO**, em 27/06/2022 13:57:07.

Este documento foi armazenado no SUAP em 27/06/2022. 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: 1106396
Código de Autenticação: db8d35c045