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

TR 16/2022 - DIAD/DG/CM/RE/IFRN

22 de agosto de 2022

Ministério da Educação

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
CAMPUS CEARÁ-MIRIM

Coordenação de Tecnologia de Informação

22 de agosto de 2022

Anexo I - 2022 do Edital

TERMO DE REFERÊNCIA

Processo Administrativo nº 23516.000319.2022-44

Solução de firewall de próxima geração

COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO - CTI

Histórico de Revisões

Data	Versão	Descrição	Autor
23/03/2022	1.0	Finalização da primeira versão do documento	Catarina de Oliveira Torres
01/04/2019	2.0	Revisão do documento após análise jurídica	Iuri Charles da Silva Ataide
22/08/2022	3.0	Revisão do documento após parecer jurídico	Catarina de Oliveira Torres

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1 - OBJETO DA CONTRATAÇÃO

Esta licitação tem por objeto o Registro de Preços para contratação de solução de firewall de próxima geração para segurança da informação de perímetro 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* conforme quantidades e exigências estabelecidas neste instrumento.

2 - DESCRIÇÃO DA SOLUÇÃO DE TIC

Devido as necessidades do Campus Ceará Mirim do IFRN em adquirir uma solução de firewall de próxima geração, as quantidades abaixo foram estimadas neste estudo técnico preliminar para compor o projeto em sua totalidade.

Além disso, tal solução deve ser 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.

2.1 Bens e serviços que compõem a solução

ID	DESCRIÇÃO	CATMAT	QUANTIDADE	UNIDADE
1	Solução de proteção de rede firewall	133132	21	unidade

2.1.1. O objeto da presente contratação trata-se de solução de Tecnologia da Informação e Comunicação (TIC), de natureza comum.

3 - JUSTIFICATIVA PARA CONTRATAÇÃO

3.1 Contextualização e Justificativa da Contratação

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

A constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição, faz crescer a preocupação de todos sobre a proteção dos dados e da privacidade dos seus cidadãos. 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 e manter informações sensíveis protegidas.

Atualmente o Campus Ceará Mirim 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 composta 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.

O firewall de próxima geração tem a capacidade de prover visibilidade granular e analisar as ameaças de todo o tráfego de dados a nível de aplicação (camada 7), garantindo ainda mais segurança para a rede, com relação as ameaças que trafegam por estas aplicações.

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 foidescontinuado, 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. Além da premente necessidade de atualização por decurso tecnológico, outra urgência se mostra importante para a atualização do firewall de próxima geração existente no Campus Ceará Mirim; posto que este passará a integra a Rede Giga-Natal, com capacidade de tráfego da banda de internet da ordem de 1Gbps, em substituição aos atuais 100Mbps. Ocorre que o modelo PA-500 dispõe de um *throughput* (taxa de transferência) de 100Mbps; não sendo suficiente para possibilitar o uso adequado da ampliação de banda de internet que o Campus receberá, ao integrar a Rede Giga-Natal, que necessita de um firewall que disponha de *throughput* (taxa de transferência) de aproximadamente 1Gbps.

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 centralizado instalado e em uso na Reitoria do IFRN.

Além disso, a aquisição via Sistema de Registro de Preços se justifica pela possibilidade de aquisição futura pelos demais campi do IFRN para que possam integrar à rede de gerenciamento já em uso na Reitoria.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS 2019 - 2026	
ID	**Objetivos Estratégicos**
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.
ES-3	Promover a apropriação da institucionalidade pela comunidade interna e pela sociedade.
O-11	Garantia da segurança das plataformas de governo digital e de missão crítica

	ALINHAMENTO AO PDTIC 2021 - 2024		
	Ação do PDTIC	**ID**	**Meta do PDTIC associada**

ID			
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**

3.3. Estimativa da Demanda

Com base no Estudo Técnico Preliminar foram estimadas as seguintes quantidades a serem adquiridas:

UASG	Órgão	Situação	Quantidade
158368	IFRN/Natal Zona Norte	**Gerenciador**	1
158371	IFRN/Apodi	Participante	1
158366	IFRN/Currais Novos	Participante	1
154840	IFRN/São Paulo do Potengi	Participante	1
158374	IFRN/Pau dos Ferros	Participante	1
158155	IFRN/Parelhas	Participante	1
158155	IFRN/Lajes	Participante	1
158372	IFRN/Santa Cruz	Participante	1
152756	IFRN/Parnamirim	Participante	1
154582	IFRN/São Gonçalo do Amarante	Participante	1
158367	IFRN/Ipanguaçu	Participante	1

158375	IFRN/Macau	Participante	1
154839	IFRN/Canguaretama	Participante	1
158373	IFRN/João Câmara	Participante	1
158370	IFRN/Caicó	Participante	2
152757	IFRN/Nova Cruz	Participante	1
152711	IFRN/Natal Cidade Alta	Participante	2
158365	IFRN/Mossoró	Participante	1
154838	IFRN/Ceará-Mirim	Participante	1
Total			**21**

3.4. Parcelamento da Solução de TI

Os equipamentos e licenças que constituem a solução, aqui proposta, interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão.

A eventual divisão do objeto em grupos diversos poderia ocasionar uma situação onde um proponente "A", por não conhecer a solução, não teria condições de fornecer eventual licenciamento correto para tal ou mesmo propor equipamentos compatíveis. Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote, de todos os itens deste processo, visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações, evitando assim que um fornecedor venha a prejudicar a execução de outro. Ainda, conforme disposto no inciso 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), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, todos os itens deverão ser do mesmo fabricante.

3.5. Resultados e Benefícios a serem alcançados

Os benefícios a serem alcançados com a execução deste projeto são:

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;

4 - ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus e spywares, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta.

Item	Descrição	Qnt
1	**SOLUÇÃO DE PROTEÇÃO DE REDE FIREWALL** Características técnicas mínimas: 1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, *spywares* e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN; 2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico; 3. O equipamento deve ser fornecido com kit que	21

	permita a sua montagem em rack 19"; 4. Deve possuir *throughput* de, no mínimo, 3 (três) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir; 5. Deve possuir *throughput* de, no mínimo, 1.5 (um ponto cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti- Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os *throughput* aferidos com tráfego HTTP ou*blend* de protocolos definidos pelo fabricante como tráfego real; 6. Deve suportar, no mínimo, 290.000 (duzentos e noventa mil) conexões simultâneas; 7. Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo; 8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45; 9. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento; 10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar; 11. Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs; 12. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 a 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento; 13. Deve suportar, no mínimo, 1.000 (hum mil) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim; 14. Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim; 15. Deve possuir suporte à criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (hum mil) VLANs; 16. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol; 17. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group); 18. Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro		

	prefixo IPv6 prevenindo problemas de roteamento assimétrico; 19. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF *graceful restart* e BGP; 20. Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuído a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links; 21. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS; 22. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo; 23. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego; 24. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas; 25. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré- definidos; 26. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego; 27. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação; 28. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva; 29. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no		

	mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado; 30. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante; 31. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação; 32. Deve permitir bloquear sessões TCP que utilizarem variações do *three- way handshake* como *four-way* e o *five-way split handshake*, prevenindo assim possíveis tráfegos maliciosos; 33. Deve permitir bloquear conexões que contenham dados no *payload* dos pacotes TCP SYN e TCP SYN-ACK durante o *three-way handshake*; 34. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas; 35. Deve ser possível a criação de assinaturas customizadas de ameaças; 36. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados; 37. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2; 38. Deve possuir proteção contra-ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets; 39. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego); 40. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e		

faixas de endereços IP;

41. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

42. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

43. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

44. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;

45. A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

46. A solução de firewall deve possuir integração com LDAP, MS Active Directoy e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

47. A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

48. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

49. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos *site-to-site* e *client-to-site* e suportar IPSEc – Internet Protocol Security e SSL – Secure Sockets Layer;

50. O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

51. O recurso de VPN SSL deve permitir que o usuário

	remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo; 52. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password; 53. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compativel para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10 e MacOS; 54. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações; 55. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall; 56. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros; 57. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento; 58. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regas (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas; 59. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados; 60. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service		

	mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário; 61. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU; 62. Deve ser possível configurar o envio de alertas do sistema via e-mail; 63. Deve suportar o monitoramento via SNMPv3; 64. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico; 65. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 66. A solução de Proteção de Rede Firewall ofertada deve ser homologada e totalmente compativel com o software de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em uso no IFRN; 67. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale; 68. Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema; 69. A solução de firewall deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.	

Condições Gerais
GARANTIA E SUPORTE

Deve possuir garantia do fabricante com validade mínima de 36 (trinta e seis) meses;

Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;

Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);

Os chamados poderão ser abertos diretamente com o fabricante;

A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;

A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help-desk para abertura de chamados de suporte técnico;

A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

A contratada deverá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações à contratante;

A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;

As horas de atendimento serão realizadas normalmente em horário comercial, no período compreendido entre 08:00 e 18:00h, em dias de semana (segunda à sexta).

CONDIÇÕES DE ENTREGA

O prazo de entrega dos produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato;

A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

Habilitação e Qualificação do Fornecedor

Deve ser apresentado atestado de capacidade técnica ou declaração emitida pelo fabricante do equipamento, comprovando que a licitante é apta a instalar, configurar e prestar suporte técnico das soluções referente a este edital;

A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compativel com o objeto deste termo de referência;

A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

CONDIÇÕES DE ACEITE

Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re- manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

Não será admitida a adesão a ata de registro de preço.

4.1. Requisitos 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;

4.2. Requisitos de Capacitação

Os técnicos do Campus Ceará Mirim do IFRN possuem conhecimento no tipo de solução a ser adquirida, bem como gozam do suporte técnico da Diretoria de Gestão de Tecnologia da Informação – DIGTI, visto que é um tipo de solução já utilizada por este Campus e por todos os demais campi do IFRN, não sendo necessário a realização de capacitação técnica.

4.3. Requisitos Legais

Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da 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° 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

Deverão ser cumpridas, no que couber, as exigências:

Do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;

Do art. 6º da Instrução Normativa MPOG n° 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

Da Portaria N° 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO.

4.4. Requisitos de Manutenção

1. Todos os itens deste processo devem possuir garantia do fabricante com validade mínima de 36 (trinta e seis) meses;
2. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
3. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
4. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);
5. Os chamados poderão ser abertos diretamente com o fabricante;
6. A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;
7. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de help-desk para abertura de chamados de suporte técnico;

4.5. Requisitos Temporais

O prazo de entrega de produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato;

A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

4.6. Requisitos de Segurança

A Contratada deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.

4.7. Requisitos Sociais, Ambientais e Culturais

A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

Em conformidade com a IN SLTI/MPOG n. 01/2010, a Contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:

Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

Que os bens não contenham substâncias perigosas em concentração acima da

recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

4.8. Requisitos de Arquitetura Tecnológica

Conforme disposto no inciso 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), os equipamentos a ser adquiridos, por questões de compatibilidade, gerência, suporte e garantia, devem ser homologados e totalmente compativeis com o software de gerenciamento centralizado Palo Alto Panorama atualmente instalado e em uso no 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; conforme descrição constante do item 4.

4.9. Requisitos de Projeto e de Implementação

Não se aplica, pois, a implantação será realizada pela equipe técnica do Campus, com auxílio do suporte da Reitoria.

4.10. Requisitos de Implantação

A implantação será realizada pela equipe técnica do IFRN Campus Ceará-Mirim, com auxílio do suporte da Reitoria.

4.11. Requisitos de Garantia

Toda solução deste termo de referência deverá considerar período de garantia por um prazo de até 3 anos, para hardware e licenças de software;

Recomendável manter o contrato de suporte e garantia com o fabricante vigente, a fim de minimizar riscos em caso de falhas de hardware e bugs de sistema. Dentre as vantagens de possuir um contrato de manutenção ativo, destacam-se:

Hardware: possibilidade de troca de equipamento ou peça no caso de falha, possibilidade de atualização de firmware para melhoria de operação ou utilização de novos recursos do equipamento, suporte do fabricante na resolução de problemas graves;

Software: possibilidade de atualização do software durante o período de garantia. As atualizações são úteis para resolução de problemas (bugs), correções de segurança e implantação de novos recursos/funcionalidades da solução.

4.12. Requisitos de Experiência profissional

Não se aplica, pois, a implantação será realizada pela equipe técnica do Campus, com auxílio do suporte da Reitoria.

4.13. Requisitos de formação da equipe

Não se aplica, pois, a implantação será realizada pela equipe técnica do Campus, com auxílio do suporte da Reitoria.

4.14. Requisitos de Metodologia de trabalho

A Contratante será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação do suporte técnico. A metodologia de trabalho relacionado aos serviços prestados deverá observar os preceitos do ITIL V4 quando aplicável.

4.15. Requisitos de Segurança da Informação

A solução contratada deverá respeitar a 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).

A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

A Contratada deverá manter a integridade da rede de dados e das informações do IFRN durante a prestação dos serviços.

A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações do IFRN bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato. A Contratada deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, deverá ser assinado por um representante da Contratada e encontra-se no ANEXO I. A Contratada deverá providenciar a assinatura do Termo de Ciência, disponível no ANEXO II, por todos os seus colaboradores que estejam relacionados com a execução do projeto. O Termo de Compromisso e o Termo de Ciência deverão ser entregues assinados durante a reunião inicial.

Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse da Contratante mesmo após o uso, após dano à unidade ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deverá ser realizada no prédio do IFRN Ceará-Mirim e imediatamente entregue a Contratante;

Caso haja necessidade de manutenção fora das dependências do IFRN Ceará-Mirim, as unidades de armazenamento deverão ser removidas dentro das dependências do IFRN Ceará-Mirim e deverão ficar sob responsabilidade da Contratante enquanto perdurar o conserto.

5 - Responsabilidades

5.1. Deveres e responsabilidades da CONTRATANTE

a. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

c. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

f. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g. Definir produtividade ou capacidade mínima de fornecimento de tráfego da solução de TIC por parte da contratada, com base na necessidade do link de internet do Campus (acima de 1Gbps), isso com todas as '*features*' de segurança ativas;

5.2. Deveres e responsabilidades da CONTRATADA

a. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

b. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

c. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

d. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

e. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

f. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

g. Manter a produtividade ou capacidade mínima de fornecimento de tráfego da solução de TIC por parte da contratada, com base na necessidade do link de internet do Campus (acima de 1Gbps), isso com todas as '*features*' de segurança ativas;

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

a. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

b. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

c. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
    1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

    2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

d. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
    1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

    2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada; e

    3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica;

6 - MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

Realização da Reunião Inicial

1. Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou de forma remota. Na reunião inicial:
   - O representante legal da contratada deverá entregar o Termo de Compromisso e o Termo de Ciência, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade;
   - Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

Prazos, horários de fornecimento de bens ou prestação dos serviços

1. A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

2. O(s) equipamento(s) deverão ser entregues e instalados nas coordenações de Tecnologia da Informação do Instituto Federal do Rio Grande do Norte. A entrega deverá ser realizada em dias úteis no horário das 08:00 às 12:00 e das 14:0 às 17:00. Segue abaixo o endereço dos locais de entrega:

Órgão	**Local de Entrega**
IFRN/Natal Zona Norte	Rua Brusque, 2926, Conjunto Santa Catarina, Potengi | Natal-RN | CEP: 59112-490.
IFRN/Apodi	RN 233, Km 02, Sítio Lagoa do Clementino, S/N. Zona Rural - Apodi/RN - CEP 59.700-000.
IFRN/Currais Novos	Rua Manoel Lopes Filho, nº 773. Valfredo Galvão | Currais Novos-RN | CEP: 59380-000.
IFRN/São Paulo do Potengi	RN-120, Km 2, Novo Juremal, São Paulo do Potengi/RN CEP 59460-000.
IFRN/Pau dos Ferros	BR 405, KM 154, S/N, Bairro Chico Cajá, Pau dos Ferros/RN, CEP 59900-000.
IFRN/Parelhas	Rua Dr. Mauro Duarte, S/N, José Clóvis | Parelhas/RN | CEP: 59.360-000.
IFRN/Lajes	Rodovia BR 304, Km 120 Centro, Lajes-RN CEP: 59535-000
IFRN/Santa Cruz	Rua São Braz, 304, Bairro Paraíso | Santa Cruz-RN | CEP: 59200-000.
IFRN/Parnamirim	Rua Antônia de Lima Paiva, 155 - Bairro Nova Esperança, Parnamirim - CEP: 59143-455.
IFRN/São Gonçalo do Amarante	Rua Prof. Carlos Guedes Alcoforado, S.N., Centro, São Gonçalo do Amarante-RN | CEP: 59291-727.
IFRN/Ipanguaçu	RN 118, S/N, Povoado Base Física, Zona Rural | Ipanguaçu-RN | CEP: 59508-000.
	Rua das Margaridas, 300, Conjunto COHAB Macau/RN - CEP:

IFRN/Macau	59.500-000.
IFRN/Canguaretama	BR-101, Km 160, S/N, Areia Branca, Canguaretama - RN, CEP: 59190-000.
IFRN/João Câmara	BR 406, Km 73, nº 3500, Perímetro Rural, João Câmara-RN | CEP: 59550-000.
IFRN/Caicó	RN 288, s/n, Nova Caicó | Caicó-RN | CEP: 59300-000.
IFRN/Nova Cruz	Av. José Rodrigues de Aquino Filho, Nº 640, RN 120, Alto de Santa Luzia | Nova Cruz-RN | CEP: 59215-000.
IFRN/Natal Cidade Alta	Rua das Donzelas, 151, Rocas - CEP: 59012-190.
IFRN/Mossoró	Rua Raimundo Firmino de Oliveira, 400 - Conj. Ulrick Graff Mossoró-RN, CEP: 59.628-330.
IFRN/Ceará-Mirim	BR-406, Km 145, Bairro Planalto, Ceará-Mirim/RN, CEP: 59570-000.

3. A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.

4. O suporte técnico deverá ser de, no mínimo, 3 anos.

Documentação mínima exigida

1. A Contratada deverá fornecer:
    - Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;

    ● Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas.

    - Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

Não se aplica.

6.3. Mecanismos formais de comunicação

As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone, aplicativo de mensagens ou outro meio informatizado que armazene o histórico da tramitação das solicitações e respostas.

6.4. Manutenção de Sigilo e Normas de Segurança

A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

O Termo de Compromisso , contendo declaração de manutenção de sigilo e respeito às

normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência , a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS I e II.

7 - MODELO DE GESTÃO DE CONTRATO

7.1. Critérios de Aceitação

Somente serão aceitos equipamentos novos e sem uso prévio. Não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste termo de referência;

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvidas ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão;

7.2. Procedimentos de Teste e Inspeção

Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo Coordenador de Tecnologia da Informação acompanhados dos fiscais do contrato.

Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou

disponibilizados de alguma forma e da análise de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:

1. Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;

2. Verificar se o equipamento está novo e sem uso;

3. Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;

4. Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;

5. Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);

6. Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);

7. Verificar se os equipamentos foram recebidos de forma que funcionem na tensão elétrica 220 V.

Após, deverá ser conduzida a inspeção através da verificação da conformidade do funcionamento do equipamento em relação aos requisitos exigidos nas especificações técnicas. Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes.

Para esta etapa deve-se observar a seguinte lista de verificação:

1. Conectar cabos de alimentação e verificar funcionamento dos equipamentos;
2. Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;
3. Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS);
4. Realizar a criação de objetos, de políticas de segurança e regras de firewall;
5. Realizar a configuração do serviço DHCP;
6. Configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;
7. Verificar a sincronização entre equipamentos (firewall ativo e passivo);
8. Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;
9. Caso o software de gerenciamento seja entregue em appliance virtual, verificar a compatibilidade com o hypervisor KVM, criar máquina virtual e realizar as configurações necessárias;
10. Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;
11. Realizar a configuração do software de gerenciamento centralizado e armazenamento de logs, e verificar a integração e sincronismo entre os o firewall e o software;
12. Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
13. Testar as seguintes funcionalidades no firewall:
    - Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;
    - Decriptografar tráfego SSL para inspeção de conteúdo;
    - Permitir inspeção em camada 7 (nível de aplicação);
    - Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;
    - Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;
    - Realizar a tradução de endereços IP: NAT (Network Address Translation);
    - Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;
    - Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;
    - Permitir que a autenticação da rede sem fio seja integrada (single sign on) com a solução de WIFI existente, marca Cisco, controladora modelo 5508;
    - Deverá ser analisada a performance da solução na infraestrutura da UFSM, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;
    - Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;
    - Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:

- O cumprimento dos prazos e outras obrigações assumidas pela contratada;
- Entrega da documentação exigida;
- Atendimento dos critérios de aceitação;
- Execução dos procedimentos corretos para que haja o recebimento dos bens e a

atestação dos serviços prestados no suporte técnico e;

- A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;
- Durante a vigência do suporte técnico, A fiscalização técnica dos contratos avaliará constantemente a prestação do serviço e usará como indicador a tabela disponível no item 7.3. Níveis Mínimos de Serviço Exigidos;
- A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

7.3. Níveis Mínimos de Serviço Exigidos

Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade abaixo:

a. Crítica: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deverá ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

- b. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deverá ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

- c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem- sucedida. Para este nível de severidade o tempo de resposta deverá ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

- d. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deverá ser de até 8 (oito) horas, em horário comercial.

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 1% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 10% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.

4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 10% (dez porcento) sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão do contrato.Contratual. Aplicação de multa de 5% (cinco porcento) sobre o valor
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 8 (oito) horas úteis.	Multa de 0,1% (um décimo porcento) sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 7 (sete) dias úteis.
		Após o limite de 7 (sete) dias úteis, aplicar-se-á multa de 1% (um porcento) do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
		A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo

11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Atraso na resolução de chamados de suporte técnico	Chamados de suporte técnico com severidade Baixa: Advertência.
		Chamados de suporte técnico com severidade Média: Multa de 0,11% do valor total do Contrato.
		Chamados de suporte técnico com severidade Alta: Multa de 0,30% do valor total do Contrato.
		Chamados de suporte técnico com severidade Crítica: Multa de 1% do valor total do Contrato.
14	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10% (dez porcento) do valor total do Contrato.

7.5. Do Pagamento

O pagamento será efetuado mediante a apresentação da Nota Fiscal, devidamente certificada, acusando o recebimento, por parte do responsável pelo órgão solicitante.

O prazo para pagamento será de no máximo 30 (trinta) dias a partir da data de sua entrega , desde que não haja impedimento legal.

8 - ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Id.	Descrção	Quantidade	Unidade	Valor unitário máximo (R$)	Valor total máximo (R$)

1	Solução de proteção de rede firewall	21	unidade	126.769,08	2.662.150,68

9 - ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

Trata-se de Sistema de Registro de Preços e a fonte de recursos deverá ser informada no momento da contratação.

10 - DA VIGÊNCIA DO CONTRATO (GARANTIA)

A garantia será de 36 meses, a contar da data de aceitação da solução pela contratante, na modalidade expressa nos itens 6.1 (item Prazos, horários de fornecimento de bens ou prestação de serviços, subitem 4) e 7.3.

11 - DO REAJUSTE DE PREÇOS

Não se aplica em razão do pagamento da solução ser único.

12 - DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

O certame se realizará na forma licitação para REGISTRO DE PREÇOS, na modalidade PREGÃO eletrônico, do tipo MENOR PREÇO.

12.2. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

Durante a apresentação da proposta, a licitante deverá demonstrar que o produto ofertado atende às exigências solicitadas nesta especificação. Para esta comprovação, serão aceitos catálogos, datasheets, manuais, sites ou outra documentação oficial onde se possa identificar de maneira inequívoca o modelo de equipamento proposto.

Em caso de dúvidas na comprovação da especificação, poderão ser solicitados por meio de diligência, esclarecimentos sobre a especificação dos produtos cotados pela licitante.

A licitante deverá apresentar declaração de que o produto atende a todas especificações exigidas.

Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

a) Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

a.1) bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

a.2) bens e serviços com tecnologia desenvolvida no País; e

a.3) bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

b) Os licitantes classificados que estejam enquadrados no item 7.25.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

c) Caso a preferência não seja exercida na forma do item a.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item a.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item a.3 caso esse direito não seja exercido.

d) As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

12.3. Critérios de Qualificação Técnica para a Habilitação

Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:

a. Atestado de Capacidade Técnica demonstrando que a proponente forneceu equipamentos, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação de solução de firewall de próxima geração compatível com o objeto deste termo de referência;

b. O atestado acima referido deverá conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente do atestado de que o serviço foi realizado a contento.

c. O atestado deverá ser em nome da LICITANTE, e elaborados em papel timbrado da empresa emitente, contendo os seguintes dados mínimos e obrigatórios:

    a. Razão Social, CNPJ e endereço completo da empresa emitente;

    b. Razão Social da LICITANTE;

    c. Vigência: de __/__ /_a __/__ /__;

    d. Objeto do contrato;

    e. Descrição do objeto do contrato: (descrição detalhada dos serviços prestados);

    f. Local e Data de emissão do Atestado;

    g. Nome, assinatura do signatário, telefone e e-mail de contato da empresa emitente.

d. A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compativel com o objeto deste termo de referência;

1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

13 - DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

A Equipe de Planejamento da Contratação foi instituída pela PORTARIA Nº 76/2022 - DG/CM/RE/IFRN , de 20 de abril de 2022.

Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

_____ Integrante Requisitante Iuri Charles da silva Téc. Lab. Área Sistema da computação 1731894	_____ Integrante Técnico Ronaldo Ferreira de Souza Téc. Lab. Área Sistema da computação 1584794	_____ Integrante Administrativo Catarina de Oliveira Torres Administradora 1962027

Autoridade Máxima da Área de TIC

André Gustavo Duarte

Diretor de Gestão de Tecnologia da Informação

1577655

Natal, 22 de agosto de *2022*.

14. APROVAÇÃO DO TERMO DE REFERÊNCIA

14.1. Considerando que esta licitação tem por objeto o Registro de Preços para contratação de solução de firewall de próxima geração para segurança da informação de perímetro 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* conforme quantidades e exigências estabelecidas neste instrumento.

14.2. Considerando que se encontram presentes os elementos essenciais para que a o pregão eletrônico via sistema de registro de preços seja realizada, com apresentação de orçamentos de prestação de serviços de empresas distintas, comprovando a escolha do menor preço entre as empresas pesquisadas para a realização do serviço e demais documentos que atende as exigências legais.

14.3. Assim, APROVO e AUTORIZO o presente Termo de Referência, uma vez que se apresenta de forma

conveniente e oportuna para atendimento da solicitação de contratação desse objeto, através de processo de **pregão eletrônico via sistema de registro de preços**, fundamentado no Art. 3º, parágrafos III e IV do Decreto nº 7.892/2013 e lei 8.666/96 e IN 1/2022 - PROAD/RE/IFRN.

Assinado eletronicamente

Edmilson Barbalho Campos Neto

SIAPE 1835439

Diretor-Geral IFRN/Zona Norte

Documento assinado eletronicamente por:

- **Edmilson Barbalho Campos Neto**, **DIRETOR GERAL - CD0002 - DG/ZN**, em 22/08/2022 17:37:48.
- **Ronaldo Ferreira de Souza**, **TECNICO DE LABORATORIO AREA**, em 22/08/2022 19:44:27.
- **Catarina de Oliveira Torres**, **ADMINISTRADOR**, em 22/08/2022 15:52:12.
- **Iuri Charles da Silva Ataide**, **COORDENADOR - FG2 - CTI/CM**, em 23/08/2022 07:48:52.
- **Andre Gustavo Duarte de Almeida**, **Diretor de Gestão de Tecnologia da Informação - CD0003 - DIGTI**, em 08/09/2022 16:13:48.

Este documento foi emitido pelo SUAP em 22/08/2022. 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: 440091
Código de Autenticação: 3a4113abcd