Termo de Referência 80/2023

Informações Básicas

Número do TR	UASG	Editado por	Atualizado em
80/2023	154050-MEC-UNIVERSIDADE FEDERAL/SE	ANDRES IGNACIO MARTINEZ MENENDEZ	01/09/2023 15:52 (v 4.0)

Status

CONCLUIDO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação.	246/2022	23113.011753/2023-73

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. A presente 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* , nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE	ITEM	ESPECIFICAÇÃO	CATMAT	MÉTRICA OU UNIDADE DE MEDIDA	CÓDIGO PMC-TIC	QUANT. UFS	QUANT. PARNAIBA	VALOR UNITÁRIO	VALOR TOTAL
01	**01**	Solução de Segurança de Rede Firewall Tipo I	609340	UNIDADE	NÃO PADRONIZADO	03	1	R$ 442.972,57	R$ 1.771.890,28
	02	Solução de Segurança de Rede Firewall Tipo II	609340	UNIDADE	NÃO PADRONIZADO	02	0	R$ 156.540,92	R$ 313.081,84
	03	Solução de Segurança de Rede Firewall Tipo III	609340	UNIDADE	NÃO PADRONIZADO	02	0	R$ 71.795,95	R$ 143.591,90
	04	Software de Gerenciamento e Armazenamento de Logs	27472	UNIDADE	NÃO PADRONIZADO	01	0	R$ 113.512,64	R$ 113.512,64
		Serviço de Instalação e							

	05	Configuração de Firewall	27014	SERVIÇO	NÃO PADRONIZADO	07	1	R$ 40.192,81	R$ 321.542,48
	06	Treinamento Oficial de Firewall de Próxima Geração	16837	SERVIÇO	NÃO PADRONIZADO	04	2	R$ 17.889,33	R$ 107.335,98

1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.3. O objeto desta contratação é caracterizado como **comum** uma vez que os padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, estando em conformidade com o art. 1º da Lei 10.520/02.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de TIC consiste em (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*.

Devido as necessidades da UFS em adquirir uma solução de firewall de próxima geração para a proteção contra ataques cibernéticas a sua infraestrutura de TI, as quantidades foram estimadas no estudo técnico preliminar para compor o projeto em sua totalidade, adequadas a infraestrutura de TIC da instituição.

Além disso, para que toda solução deste projeto armazene logs por mais tempo, seja administrada e configurada de maneira centralizada, facilitando e otimizando sua administração de acordo com as melhores práticas de TI, está previsto a contratação de software de gestão centralizada.

2.1. DESCRIÇÃO DETALHADA DA SOLUÇÃO DE TIC

GRUPO	ITEM	DESCRIÇÃO
1	**1**	**Solução de Segurança de Rede Firewall TIPO I** *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 fornecido deve ser próprio para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação; 4. Deve possuir throughput de, no mínimo, 6 (seis) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

		5. Deve possuir throughput de, no mínimo, 3 (três) 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, 900.000 (novecentos mil) conexões simultâneas; 7. Deve suportar, no mínimo, 90.000 (noventa mil) novas conexões por segundo; 8. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1 Gbps do tipo RJ-45; 9. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1 Gbps do tipo SFP; 10. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 10 Gbps do tipo SFP+; 11. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento; 12. Deve possuir, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade; 13. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar; 14. Deve possuir, no mínimo, 120 (cento e vinte) GB de armazenamento interno para o sistema operacional e registro de logs; 15. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento (hot-swappable); 16. Deve suportar, no mínimo, 1.000 (um mil) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim; 17. Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim; 18. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs; 19. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol; 20. 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); 21. 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; 22. 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; 23. 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; 24. 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; 25. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo /ativo;

26. 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;

27. 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;

28. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

29. 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;

30. 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;

31. 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;

32. 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;

33. 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;

34. 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;

35. 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;

36. Deve permitir bloquear conexões que contenham dados no *payload* dos pacotes TCP SYN e TCP SYN-ACK durante o *three-way handshake*;

37. 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;

38. Deve ser possível a criação de assinaturas customizadas de ameaças;

39. 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;

40. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

41. Deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP;

42. 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;

43. 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);

44. A solução de firewall de possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego tanto TCP quanto UDP;

45. 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;

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

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

48. Deve prover análise em tempo real dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;

49. 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;

50. 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;

51. 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;

52. 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;

53. 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;

54. 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;

55. 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;

56. 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;

57. 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;

58. 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;

59. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10, MS Windows 11 e MacOS;

60. 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;

61. 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;

62. 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;

63. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

64. 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, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

65. 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;

66. 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;

67. 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;

68. Deve ser possível configurar o envio de alertas do sistema via e-mail;

69. Deve suportar o monitoramento via SNMPv3;

70. 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;

71. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

72. 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;

73. 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; 74. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.
	2	**Solução de Segurança de Rede Firewall TIPO II** *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 permita a sua montagem em rack 19"; 4. Deve possuir throughput de, no mínimo, 2.8 (dois ponto oito) 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 à 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, 500 (quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim; 14. Deve suportar, no mínimo, 100 (cem) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim; 15. Deve possuir suporte a 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 funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP;

39. 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;

40. 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);

41. A solução de firewall de possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego tanto TCP quanto UDP;

42. 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;

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

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

45. Deve prover análise em tempo real dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução;

46. 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;

47. 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;

48. 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;

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

50. 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;

		51. 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; 52. 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; 53. 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; 54. 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; 55. 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; 56. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10 e MacOS; 57. 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; 58. 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; 59. 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; 60. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento; 61. 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; 62. 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; 63. 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; 64. 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;

		65. Deve ser possível configurar o envio de alertas do sistema via e-mail; 66. Deve suportar o monitoramento via SNMPv3; 67. 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; 68. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 69. 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; 70. 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; 71. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.
	3	**Solução de Segurança de Rede Firewall TIPO III** *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 permita a sua montagem em rack 19"; 4. Deve possuir throughput de, no mínimo, 2 (dois) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir; 5. Deve possuir throughput de, no mínimo, 850 (oitocentos e cinquenta) Mbps 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, 190.000 (cento e noventa mil) conexões simultâneas; 7. Deve suportar, no mínimo, 35.000 (trinta e cinco 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, 120 (cento e vinte) 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 à 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, 500 (quinhentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

14. Deve suportar, no mínimo, 100 (cem) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

15. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um 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 funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP; 39. 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; 40. 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); 41. A solução de firewall de possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego tanto TCP quanto UDP; 42. 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; 43. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias; 44. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas; 45. Deve prover análise em tempo real dos websites acessados pelos usuários realizando a inspeção do seu conteúdo, detectando assim conteúdos que possam ser uma ameaça e realizando a categorização da URL como maliciosa e bloqueando tal URL, mesmo que ela não esteja presente e devidamente categorizada na base de dados de URL da solução; 46. 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; 47. 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;

48. 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;

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

50. 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;

51. 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;

52. 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;

53. 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;

54. 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;

55. 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;

56. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 10, MS Windows 11 e MacOS;

57. 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;

58. 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;

59. 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;

60. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

61. 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, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

62. 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; 63. 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; 64. 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; 65. Deve ser possível configurar o envio de alertas do sistema via e-mail; 66. Deve suportar o monitoramento via SNMPv3; 67. 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; 68. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 69. 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; 70. 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; 71. A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.
	4	**SOFTWARE DE GERENCIAMENTO E ARMAZENAMENTO DE LOGS** *Características técnicas mínimas:* 1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos. 2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança. 3. Deve ser homologado e totalmente compatível com a SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL TIPO I, com a SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL TIPO II e com a SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL TIPO III, itens 1, 2 e 3, respectivamente, especificados neste Termo de Referência para permitir o gerenciamento centralizado e armazenamento de logs da quantidade total dos itens mencionados, estando devidamente licenciado para este fim. 4. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções. 5. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi; 6. Deve permitir o armazenamento de logs sem limite de tempo nem limite da quantidade de logs diários a ser recebido ou armazenado. Caso seja necessário licenciamento adicional, deverá ser entregue licenciado com a maior capacidade suportada;

		7. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança; 8. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição; 9. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls; 10. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios; 11. Deve permitir a criação de objetos e políticas compartilhadas; 12. Deve consolidar logs e relatórios de todos os dispositivos administrados; 13. Deve permitir exportar backup de configuração automaticamente via agendamento; 14. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls; 15. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado; 16. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento; 17. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta; 18. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa; 19. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux; 20. O gerenciamento deve permitir/possuir: 20.1. Criação e administração de políticas de firewall e controle de aplicação; 20.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware; 20.3. Criação e administração de políticas de Filtro de URL; 20.4. Monitoração de logs; 20.5. Ferramentas de investigação de logs; 20.6. Debugging; 20.7. Captura de pacotes; 21. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador; 22. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI. 23. Deve possuir mecanismo de busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo; 24. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

25. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

26. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

27. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

28. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

29. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

30. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

31. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

32. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

33. Criação de regras que fiquem ativas em horário definido;

34. Criação de regras com data de expiração;

35. Backup das configurações e rollback de configuração para a última configuração salva;

36. Suportar Rollback de Sistema Operacional para a última versão local;

37. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

38. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

39. Validação de regras antes da aplicação;

40. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação;

41. 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;

42. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

43. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;

44. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);

45. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

46. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

47. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

48. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

49. Deve permitir a criação de *Dash-Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sand-box e tráfego bloqueado;

50. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

51. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, Anti-spyware, Filtro de URL e filtro de arquivos em uma única tela;

52. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-spware), etc;

53. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-spware), e URLs que passaram pela solução;

54. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

55. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;

56. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar 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;

57. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

58. Deve ser possível exportar os logs em CSV;

59. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

60. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

61. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

61.1. Situação do dispositivo e do cluster;

61.2. Principais aplicações;

61.3. Principais aplicações por risco;

61.4. Administradores autenticados na gerência da plataforma de segurança;

61.5. Número de sessões simultâneas;

61.6. Status das interfaces;

61.7. Uso de CPU;

62. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

62.1. Resumo gráfico de aplicações utilizadas;

62.2. Principais aplicações por utilização de largura de banda de entrada e saída;

62.3. Principais aplicações por taxa de transferência de bytes;

		62.4. Principais hosts por número de ameaças identificadas; 62.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-spware), de rede vinculadas a este tráfego; 62.6. Deve permitir a criação de relatórios personalizados; 63. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IPs distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa; 64. Gerar alertas automáticos via: 64.1. Email; 64.2. SNMP; 64.3. Syslog; 65. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP; **66. Caso o Software de Gerenciamento e Armazenamento Logs ofertado seja o mesmo já existente na UFS, a empresa deverá fornecer a renovação da garantia e suporte compreendendo a atualização do software para obter novas funcionalidades e correção de bugs e demais itens da garantia conforme descrito nas "Condições Gerais", pelo período de 60 (sessenta) meses, da solução existente descrita abaixo:** **66.1. Modelo: Palo Alto Panorama** **66.2. Número de série: 000702941877** **66.3. PN: PAN-SVC-BKLN-PRA-25-5YR-R** 67. Deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a atualização do software para obter novas funcionalidades e correção de bugs. Demais itens referentes a garantia estão descritos nas "Condições Gerais" deste Termo de Referência.
	5	**SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL** *Características técnicas mínimas:* 1. A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos: 1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação; 1.2. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Deve considerar também a instalação em modo Alta Disponibilidade (ativo/passivo); 1.3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já́ existentes e instalados; 1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; 1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

		1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução; 1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas; 2. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças; 3. As atividades de configuração da solução, migração de regras e demais atividades necessárias para a configuração do sistema poderão ser realizadas de forma remota; 4. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances; 5. Repasse de informação das configurações realizadas no formato hands-on de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;
	6	**TREINAMENTO OFICIAL DE FIREWALL DE PROXIMA GERAÇÃO** *Características técnicas mínimas:* 1. A contratada deverá disponibilizar um voucher individual para participação no treinamento oficial do fabricante do item Solução de Segurança de Rede Firewall ofertado; 2. O treinamento deve ser ministrado abrangendo teoria e prática de configuração e administração de solução de firewall de próxima geração, bem como assuntos teóricos relacionados; 2.1. Deve conter, no mínimo, a seguinte ementa: 2.2. Arquitetura e Plataforma; 2.3. Configuração da Solução; 2.4. Políticas de Segurança e NAT; 2.5. Políticas de segurança baseada em aplicação; 2.6. Identificação de Aplicações; 2.7. Identificação de Usuário; 2.8. Bloqueio de ameaças; 2.9. Bloqueio de ameaças desconhecidas; 2.10. Bloqueio de ameaças em de tráfego criptografado; 2.11. Análise das informações de tráfego e ameaças detectadas; 2.12. Demais assuntos pertinentes a solução; 3. A duração do curso será de 5 dias em horário comercial; 4. Deve ser emitido um único certificado de conclusão cobrindo todo o curso para o participante; 5. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais; 6. O treinamento deve estar disponível na modalidade presencial nas instalações do fabricante ou da autorizada ou ministrado de forma remota; 7. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso;

		8. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação. Esses custos serão de responsabilidade da Contratante;

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

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

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

Atualmente a UFS conta com equipamentos de firewall de próxima geração da Palo Alto dos modelos PA-3060, PA-3020 e PA-500 instalados em todos os campi e reitoria protegendo toda sua infraestrutura de rede de computadores e data center. Todos os equipamentos são gerenciados e monitorados de forma centralizado através do software de gerenciamento centralizado Palo Alto Panorama instalado na rede da UFS, constituindo assim uma plataforma de segurança da informação composta por equipamento (hardware) e sistema (software) que objetiva a proteção da infraestrutura da rede de computadores e data center da UFS. Todos os componentes desta solução foram adquiridos entre os anos de 2016 e 2017.

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 da UFS.

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.

Os modelos de equipamento de firewall PA-3060, PA-3020 e PA-500 foram descontinuado pelo seu fabricante, 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 os modelos PA- 3060 PA-3020 será 31 de outubro de 2024 e para o modelo PA-500 será 31 de outubro de 2023. Após esta data o equipamento não terá mais garantia, suporte e atualizações de software disponibilizados.

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 da universidade. 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.

Optou-se por se fazer o referido certame através de **Sistema de Registro de Preço**, haja vista o quantitativo da Solução de Firewall, em especial os equipamentos, ser de difícil mensuração, uma vez que a quantidade de equipamentos depende do crescimento da demanda, do volume de acessos a internet e do tamanho da rede, a qual está em processo de contínua ampliação de sua infraestrutura, estando assim em conformidade com o preconizado no inciso V, do artigo 3º do Decreto n° 11.462, de 31 de março de 2023.

3.1. O objeto da contratação está previsto no Plano de Contratações Anual , conforme detalhamento a seguir: 3.1.1. ID PCA no

PNCP: **13031547000104-0-000001/2023**

3.1.2. Data de publicação no PNCP: 19/05/2023

3.1.3. Id do item no PCA: 2004

3.1.4. Classe/Grupo: *7050* - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

3.1.5. Identificador da Futura Contratação: 154050-246/2022

3.2. O objeto da contratação também está alinhado com a Estratégia de Governo Digital e em consonância com o Plano Diretorde Tecnologia da Informação e Comunicação (PDTIC) do , conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
06	Manter atualizada toda a infraestrutura de TIC da UFS
N07	Ampliar oferta de serviços de rede
N10	Avaliar a segurança da rede e dos recursos
N21	Melhorar o gerenciamento dos serviços de TIC
N29	Implementar priorização de tráfego

ALINHAMENTO AO PDTIC - 2021- 2024			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A2	Elaborar especificação dos equipamentos de TIC para abertura de registro de preços	M1	Otimizar os recursos e serviços de TIC para atender as demandas da UFS
A29	Manter solução de firewall atualizada	M3	Manter Continuidade dos serviços TIC
A36	Realizar verificação de vulnerabilidades e testes de penetração visando um panorama situacional da segurança da rede e de seus recursos	M4	Melhorar a segurança de TIC
A46	Implantar priorização de tráfego	M5	Melhorar a qualidade dos serviços de TIC

3.3. De acordo com o inciso III do art. 6º da Instrução Normativa SGD/ME nº 94, de 2022, caso o objeto trate da oferta digital de serviços públicos, deverá haver integração à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016. Assim sendo, por NÃO se tratar de oferta de serviços públicos digitais, o objeto da contratação não será integrado à Plataforma Gov.br.

4. REQUISITOS DA CONTRATAÇÃO

4.1. SUSTENTABILIDADE

4.1.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos, no que couber, os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

1. bens constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448- 1 e 15448-2;
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;
3. 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; e
4. 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 difenilpolibromados (PBDEs).

4.2. INDICAÇÃO DE MARCAS OU MODELOS (Art. 41, inciso I, da Lei nº 14.133, de 2021)

4.2.1. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares:

4.2.1.1. Palo Alto

4.3. DA EXIGÊNCIA DE CARTA DE SOLIDARIEDADE

4.3.1. Considerando a relevância da contratação e os prejuízos que poderá sofrer a Instituição em razão da não execução plena da contratação em questão, em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

4.4. SUBCONTRATAÇÃO

4.4.1. Não é admitida a subcontratação do objeto contratual.

4.5. REQUISITOS DE NEGÓCIO

4.5.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

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

4.5.1.2. 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);

4.5.1.3. Manter a integridade dos dados e das informações sensíveis dos sistemas da UFS;

4.5.1.4. Melhorar o nível de qualidade ser serviço das aplicações internas da UFS;

4.6. REQUISITOS DE CAPACITAÇÃO

4.6.1. Será necessário treinamento à equipe que atuará com a solução. Os requisitos exigidos para a capacitação estão presentes no item 6 da tabela contida no Subitem 2.1 "DESCRIÇÃO DETALHADA DA SOLUÇÃO DE TIC" deste Termo de Referência.

4.7. REQUISITOS LEGAIS

4.7.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.8. REQUISITOS DE MANUTENÇÃO

4.8.1. Todos os itens deste processo devem possuir garantia do fabricante com validade mínima de 60 (sessenta) meses;

4.8.2. Os chamados poderão ser abertos ou diretamente com o fabricante ou com a autorizada oficial do fabricante no Brasil durante a vigência da garantia;

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

4.8.4. 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);

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

4.8.6. 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;

4.9. REQUISITOS TEMPORAIS

4.9.1. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de **120 (cento e vinte)** dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

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

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

4.9.4. O prazo para execução dos serviços de Instalação e Configuração do Firewall é de até **45 (quarenta e cinco)** dias corridos a contar do recebimento dos equipamentos, podendo este prazo ser prorrogado por igual período a critério da Administração.

4.10. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

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

4.11. REQUISITOS DA ARQUITETURA TECNOLÓGICA

4.11.1. 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 UFS, otimizando a administração dos *appliances* e armazenamento de logs.

4.11.2. Aproveitar todo conhecimento sobre a solução existente na UFS (firewall de próxima geração do fabricante Palo Alto) já desprendido pela Área de TI da instituição;

4.11.3. Conforme disposto na alínea "a" do Inciso V do artigo 40 da lei 14133/2021 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho) os equipamentos e softwares, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante, bem como os equipamentos adquiridos devem ser , por questões de compatibilidade, gerência, suporte e garantia, devem ser homologados e totalmente compatíveis com o software de gerenciamento centralizado **Palo Alto** atualmente instalado e em uso no UFS, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pela UFS.

4.12. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

4.12.1. A solução deve ser compatível com o padrão estabelecido na rede da UFS.

4.13. REQUISITOS DE IMPLANTAÇÃO

4.13.1. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.13.1.1. A implantação deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida que lhes confiram as competências necessárias para a realização dos respectivos serviços de implantação, ou pelo próprio fabricante.

4.13.1.2. Deverá abranger a configuração de quaisquer funcionalidades suportadas pelos equipamentos / softwares. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela CONTRATADA após alinhamento do escopo de trabalho definido entre CONTRATADA e CONTRATANTE.

4.14. REQUISITOS DE GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

4.14.1. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, **60 (sessenta) meses**, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.14.2. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.14.3. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

4.14.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.14.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.14.6. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até **05 (cinco)** dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.14.7. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.14.8. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.14.9. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.14.10. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.14.11. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.14.12. Os chamados poderão ser abertos ou diretamente com o fabricante ou com a autorizada oficial do fabricante no Brasil durante a vigência da garantia;

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

4.14.14. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição, obedecendo a modalidade NBD (Next Business Day);

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

4.14.16. 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;

4.14.17. 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;

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

4.14.19. 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;

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

4.14.21. 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).

4.15. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

4.15.1. Os serviços de instalação e configuração dos itens relacionados neste termo de referência deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, com certificação oficial do fabricante, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

4.15.2. A contratada deverá possuir, pelo menos, um técnico certificado oficialmente pelo fabricante da solução.

4.16. REQUISITOS DE FORMAÇÃO DA EQUIPE

4.16.1. Não serão exigidos requisitos de formação da equipe para a presente a contratação.

4.17. REQUISITOS DE METODOLOGIA DE TRABALHO

4.17.1. O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.17.2. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.17.3. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento mínimo de **24** horas por dia e **7** dias por semana de maneira eletrônica e **mínimo de 8** horas por dia e **5** dias (segunda à sexta) por semana por via telefônica.

4.17.4. O andamento do fornecimento dos equipamentos dever ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.17.5. 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.

4.18. REQUISITOS DE SEGURANÇA E PRIVACIDADE

4.18.1. 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).

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

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

4.18.4. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações do UFS 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.

4.18.5. 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 A. A Contratada deverá providenciar a assinatura do Termo de Ciência, disponível no ANEXO B, 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.

4.18.6. 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 da UFS e imediatamente entregue a Contratante;

4.18.7. Caso haja necessidade de manutenção fora das dependências da UFS, as unidades de armazenamento deverão ser removidas dentro das dependências da UFS e deverão ficar sob responsabilidade da Contratante enquanto perdurar o conserto.

4.19. OUTROS REQUISITOS APLICÁVEIS 4.19.1.DO 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. Conforme o inciso II do § 3º do art. 40 da Lei 14.133/2021 o parcelamento não será adotado quando o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido, 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 na alínea "a" do inciso V, do artigo 40 da lei 14.133/2021 (atendimento aos princípios: da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho) estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, todos os itens deverão ser do mesmo fabricante.

5. INFORMAÇÕES RELEVANTES PARA APRESENTAÇÃO DA PROPOSTA

5.1. A proposta deve observar o § 4º do art. 12 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que preconiza que nas **licitações por preço global,** cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 26 da Lei nº 14.133, de 2021.

6. PAPÉIS E RESPONSABILIDADES

6.1. São obrigações da CONTRATANTE:

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

6.1.2. 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;

6.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

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

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

6.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;

6.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

6.2. São obrigações do CONTRATADO:

6.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

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

6.2.3. 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;

6.2.4. 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, desde que motivadas as causas e justificativas desta decisão;

6.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

6.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

6.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

6.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços, quando for o caso;

6.3. São obrigações do ÓRGÃO GERENCIADOR do registro de preços:

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

6.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

6.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

6.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

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

6.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

6.3.4.1 a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

6.3.4.2. 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 pelo Contratado; e

6.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. ROTINAS DE EXECUÇÃO

7.1.1. DO ENCAMINHAMENTO FORMAL DE DEMANDAS

7.1.1.1 O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados..

7.1.1.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas naOFB.

7.1.2. Os bens serão recebidos provisoriamente, quando da entrega integral do objeto (incluindo todas as parcelas), pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.1.3. Os bens serão recebidos definitivamente no prazo de **10 (dez)** dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado, desde que estejam de acordo com os critérios de aceitação constante da seção **8.9** deste Termo de Referência.

7.2. FORMA DE EXECUÇÃO E ACOMPANHAMENTO DOS SERVIÇOS

7.2.1. CONDIÇÕES DE ENTREGA

7.2.1.1. O prazo de entrega dos bens é de até **120 (cento e vinte)** dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, em remessa única.

7.2.1.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos **10 (dez)** dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

7.2.1.3. Os bens deverão ser entregues no endereço Av. Marcelo Deda Chagas, Bairro Jardim Rosa Elze, CEP: 49.107-230 – São Cristovão – SE, de Segunda a Sexta, em dias úteis, das 08:00hs às 12:00hs e das 14:00 às 17:00hs.

7.2.1.4. A entrega do órgão participante será no endereço: Universidade Federal Delta do Parnaíba – UFDPar, Campus Ministro Reis Veloso, Av. São Sebastião, 2819, Bairro Nossa Senhora de Fátima, Parnaíba-PI, CEP: 64202-020, nos dias úteis, das 7:00h às 11:00h e das 12:00h às 16:00h.

7.3. FORMAS DE TRANSFERÊNCIA DE CONHECIMENTO

7.3.1. Não será necessária transferência de conhecimento devido às características do objeto.

7.4. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

7.4.1. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

7.5. QUANTIDADE MÍNIMA DE BENS OU SERVIÇOS PARA COMPARAÇÃO E CONTROLE

7.5.1. Não se aplica.

7.6. MECANISMOS FORMAIS DE COMUNICAÇÃO

7.6.1. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

a) Ordem de Fornecimento de Bens;

b) Ofício;

c) Sistema de abertura de chamados;

d) E-mails;

e) Telefone, caso esta possa ser gravada e forneça número de protocolo.

7.7. FORMAS DE PAGAMENTO

7.7.1. Os critérios de medição e pagamento serão tratados no item **8.13** e seguintes deste Termo de Referência.

7.8. MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

7.8.1. O Contratado 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.

7.8.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos **ANEXOS A e B**.

8. MODELO DE GESTÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
8.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
8.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
8.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
8.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.
8.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.
8.7. A pauta desta reunião observará, pelo menos:

8.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;
8.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
8.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

8.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
8.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

8.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

8.8.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

8.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);[A1]
8.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);
8.8.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).
8.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).
8.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22,VII).
8.8.7. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).
8.8.8. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).
8.8.9. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).
8.8.10. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).
8.8.11. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).
8.8.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

8.8.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).
8.8.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22,VII).
8.8.15. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

8.9. CRITÉRIOS DE ACEITAÇÃO

8.9.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

8.9.1.1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais
de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).
8.9.1.2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.
8.9.1.3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada

e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

8.9.1.4. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

8.9.1.5. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos,

sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

8.9.1.6. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

8.9.1.7. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões "shareware" ou "trial". O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

8.9.1.8. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

8.9.1.9. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa

será convocada a refazer todos os serviços rejeitados, sem custo adicional.

8.1.9.10. 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 dias úteis após a solicitação até 15 (quinze) 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);

8.10. PROCEDIMENTOS DE TESTE E INSPEÇÃO

8.10.1. 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.

8.10.2. 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:

8.10.2.1. 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;

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

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

8.10.2.4. 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;

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

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

8.10.2.7. Verificar se os equipamentos foram recebidos de forma que funcionem na tensão elétrica entre 120 à 240 V.

8.10.3. 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:

8.10.3.1. Conectar cabos de alimentação e verificar funcionamento dos equipamentos;

8.10.3.2.. Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;

8.10.3.3. Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS);

8.10.3.4. Realizar a criação de objetos, de políticas de segurança e regras de firewall;
8.10.3.5. Realizar a configuração do serviço DHCP;
8.10.3.6. Configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;
8.10.3.7. Verificar a sincronização entre equipamentos (firewall ativo e passivo);
8.10.3.8. Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;
8.10.3.9. 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;
8.10.3.10. Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;
8.10.3.11. 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;
8.10.3.12. Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
8.10.3.13. Testar as seguintes funcionalidades no firewall:

a) Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;

b) Decriptografar tráfego SSL para inspeção de conteúdo;
c) Permitir inspeção em camada 7 (nível de aplicação);
d) Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;
e) Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;
f) Realizar a tradução de endereços IP: NAT (Network Address Translation);
g) Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;
h) Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;
i) Permitir que a autenticação da rede sem fio seja integrada (single sign on) com a solução de WIFI existente.
j) Deverá ser analisada a performance da solução na infraestrutura da UFS, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;
k) Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;
l) Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

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

8.10.4.1. O cumprimento dos prazos e outras obrigações assumidas pela contratada;
8.10.4.2. Entrega da documentação exigida;
8.10.4.3. Atendimento dos critérios de aceitação;
8.10.4.4. Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico e;
8.10.4.5. 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;
8.10.4.6. 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;
8.10.4.7. 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.

8.11. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS

8.11.1. 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).
8.11.2. O suporte deverá respeitar os seguintes tempos de resposta para os níveis de severidade abaixo:
8.11.2.1. 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);
8.11.2.2. 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;

8.11.2.3. 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;
8.11.2.4. 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.
8.12. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO
8.12.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	***Ocorrência***	***Glosa / Sanção***
1	Atraso na entrega do objeto da contratação.	Glosa de (0,05) % sobre o valor da parcela em atraso por dia útil de atraso até o limite de 30 (trinta) dias úteis. Após 30 dias úteis, será aplicada a multa de 3% sobre a parte inadimplida, 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 14133/2021.
2	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, multa de 0,1**%** sobre o valor total do Contrato.
3	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 (24) horas úteis.	Multa de (0,1) % 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) % do valor total do Contrato.
4	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 14133/2021.
5	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 14133/2021.
6	Comprometer intencionalmente a integridade,	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades

	disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	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 14133/2021.
7	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 14133/2021.
8	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 0,1% 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.
9	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 2 (dois) % do valor total do Contrato.

8.12.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:
8.12.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
8.12.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;
8.13. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO8.13.1.RECEBIMENTO DO OBJETO

Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.
Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de dias, a contar da notificação do Contratado, às suas custas, sem prejuízo 30 (trinta) da aplicação das penalidades.
O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.
Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 05 (cinco) dias úteis. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.13.4. LIQUIDAÇÃO

Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.
O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.
Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;
b) a data da emissão;
c) os dados do contrato e do órgão Contratante;
d) o período respectivo de execução do contrato;
e) o valor a pagar; e
f) eventual destaque do valor de retenções tributárias cabíveis.

Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta ao SICAF ou, na impossibilidade de on- line acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

8.13.3. PRAZO DE PAGAMENTO

8.13.3.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.13.3.2. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IGP-M de correção monetária.

8.13.4. FORMA DE PAGAMENTO

8.13.4.1 O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.
8.13.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
8.13.4.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
8.13.4.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
8.13.4.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.13.5. CESSÃO DE CRÉDITO

8.13.5.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.
8.13.5.2. As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.
8.13.5.3. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.
8.13.5.4. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.
8.13.5.5. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.
A cessão de crédito não afetará a execução do objeto Contratado, que continuará sob a integral responsabilidade do Contratado

9. DO REAJUSTE

9.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECED

10.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

10.1.1 O fornecedor será selecionado por meio da realização de procedimento de **LICITAÇÃO**, na modalidade **PREGÃO**, sob a forma **ELETRÔNICA**, com adoção do critério de julgamento pelo **menor preço**.

10.1.2. O regime de execução do contrato será por **empreitada por preço global**.

10.2. EXIGÊNCIAS DE HABILITAÇÃO

10.2.1. Habilitação jurídica

Para fins de habilitação jurídica, deverá o licitante comprovar os seguintes requisitos:

a) Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

b) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

c) Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br /empreendedor;

d) Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

e) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

f) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

g) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

h) Sociedade cooperativa**:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

i) Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.2.2. Habilitação fiscal, social e trabalhista

Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

Prova de inscrição no cadastro de contribuintes *Estadual e/*ou *Municipal,* relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

Prova de regularidade com a Fazenda *Estadual e/*ou *Municipal* do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

Caso o fornecedor seja considerado isento dos tributos *Estadual e/*ou *Municipal* relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.2.3. Qualificação Econômico-Financeira

Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I- Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);

II- Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e

III- Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% do valor total estimado da contratação ou valor total estimado da parcela pertinente, conforme o caso. A adoção de um percentual do patrimônio líquido para qualificação, foi motivada pelo entendimento de este seria a melhor forma de garantia visto que trata-se da situação patrimonial líquida da empresa.

As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

10.2.4. Qualificação Técnica

10.2.4.1. Deve ser apresentado atestado de capacidade técnica comprovando que a licitante é apta a instalar, configurar e prestar suporte técnico nas soluções referentes a este termo de referência. A Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, se dará por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

a) Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

b) O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

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

a) 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.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de R$ 2.770.955,12 (dois milhões, setecentos e setenta mil, novecentos e cinquenta e cinco reais e doze centavos), conforme custos unitários apostos na tabela do subitem 1.1.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. Por se tratar de Registro de Preços a dotação orçamentária será definida no momento da contratação:

13. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado digitalmente
gov.br
DILTON DANTAS DE OLIVEIRA
Data: 04/09/2023 16:34:21-0300
Verifique em https://validar.iti.gov.br

DILTON DANTAS DE OLIVEIRA

Integrante Requisitante

Documento assinado digitalmente
gov.br
ERIC BERNARDES CHAGAS BARROS
Data: 04/09/2023 16:14:17-0300
Verifique em https://validar.iti.gov.br

ERIC BERNARDES CHAGAS BARROS

Integrante Técnico

Documento assinado digitalmente
gov.br
HELLEN DEISE LOPES DOS SANTOS
Data: 01/09/2023 16:01:07-0300
Verifique em https://validar.iti.gov.br

HELLEN DEISE LOPES DOS SANTOS

Integrante Administrativo

UNIVERSIDADE FEDERAL DE SERGIPE
Assinado de forma digital por
ANDRES MENENDEZ:49863690597
Dados: 2023.09.04 17:20:15 -03'00'

ANDRES IGNACIO MARTINEZ MENENDEZ

Autoridade Máxima de TI