MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PIAUÍ
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

(Processo Administrativo n° 23.111.025660/2024-05)

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de **FIREWALL DE PRÓXIMA GERAÇÃO (NGFW),** para Universidade Federal do Piauí - UFPI por processo de Adesão à Ata de Registro de Preços n° 03/2024 do Pregão Eletrônico n° 90003/2024 da Universidade Federal de Sergipe - UFS (Processo Administrativo n° 23.113.011753/2023-73), nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATMAT	MÉTRICA OU UNIDADE DE MEDIDA	CÓD. PMC-TIC	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Aquisição de solução de segurança de rede Firewall tipo II, NGFW Palo Alto PA-460	609340	Unidade	Não padronizado	1	155.000,00	155.000,00
2	Solução de segurança de rede Firewall tipo III, NGFW Palo Alto PA-450	609340	Unidade	Não padronizado	1	71.700,00	71.700,00

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. Os bens objetos desta contratação são caracterizados como comuns, 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.

1.4. O prazo de vigência da contratação será o mesmo previsto no edital da contratação;

1.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

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

2.1 DESCRIÇÃO DETALHADA DA SOLUÇÃO DE TIC

1	**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.
2	**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.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

Conforme justificativa já inclusa no ETP digital, 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 inclusive 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 exemplo de ataques sofridos pelos STJ, TSE entre outros).

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

A contratação da solução de firewall de próxima geração possui o intuito de manter protegido o tráfego dos dados eletrônicos da rede do UFPI. A solução de firewall objeto desta contratação é do mesmo fabricante (Palo Alto) do firewall já utilizado na UFPI, porém os atuais modelos utilizados pela universidade (PA - 820, PA - 3020 e PA - 5520) já estão sendo descontinuados fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI da Universidade.

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 UFPI.

Como o firewall é um equipamento de extrema importância para proteção e funcionamento da rede e que possibilita a conexão segura dos usuários remotos através de túneis VPN e que se inexistente ou indisponível por falha de hardware ou software, isso pode comprometer os serviços administrativos e operacionais do campus. Portanto, dada a necessidade de modernização da solução de firewall, se faz necessário para este projeto a aquisição de solução de firewall de próxima geração. A demanda evidenciada pela equipe de tecnologia da informação do Campus tem como base ainda as necessidades da instituição em proporcionar que a solução de firewall existente esteja coberta por uma garantia do fabricante e de contar com um serviço de suporte técnico especializado, que poderá ser acionado em casos de problemas e dúvidas quanto à implementação e sugestões de melhorias.

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

A necessidade de substituição alinha-se a duas condições: os atuais modelos utilizados pela UFPI PA-820, PA-3020 e PA-5520 já foram descontinuados pelo fabricante, fato que acarretará impossibilidade de suporte técnico adequado e renovação das licenças de proteção de rede necessárias à segurança de TI da Universidade.

3.1. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

3.1.1. ID PCA no PNCP: 06.517.387/0001-34;

3.1.2. Data de publicação no PNCP:11/10/2023;

3.1.3. Id do item no PCA: 2321 e 2322;

3.1.4. Classe/Grupo: 7050;

3.1.5. Identificador da Futura Contratação: 154048-31/2024

3.2. O objeto da contratação também está alinhado com a Estratégia de Governo Digital e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2019 - 2022 da STI/ UFPI, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS

ID	Objetivos Estratégicos
IE22	Manutenção e expansão da Infraestrutura de hardware, como disponibilização e ampliação do serviço de rede cabeada e sem fio; provimento de máquinas virtuais e migração para Cloud; monitoramento eletrônico de ambientes; consolidação das políticas de segurança de TIC, processos e boas práticas de gerenciamento de serviços e de engenharia de software.

ALINHAMENTO AO PDTIC 2019 - 2022			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A01	Planejar a aquisição de solução de segurança digital	**N106**	Manter em pleno funcionamento a solução de segurança digital (Firewall)
A23	Implantar as soluções planejadas e adquiridas	**N127**	Aderir às políticas e boas práticas de segurança da informação
A90	Planejar e monitorar os contratos de aquisição/manutenção de equipamentos de segurança eletrônica	**N105**	Manter em pleno funcionamento a solução de segurança digital

3.3. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

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

4.1.2. 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);

4.1.3. Manter a integridade dos dados e das informações sensíveis dos sistemas da UFPI;

4.1.4. Melhorar o nível de qualidade ser serviço das aplicações internas da UFPI;

Requisitos de Capacitação

4.1.5. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

Requisitos Legais

4.2. 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;

Requisitos de Manutenção

4.3. Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela Contratada, visando à manutenção da disponibilidade da solução;

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

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

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

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

4.9. 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;

Requisitos Temporais

4.10. 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;

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

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

4.13. 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.

Requisitos de Segurança e Privacidade

4.14. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, e 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)

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

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

4.17. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações da UFPI 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. 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 UFPI e imediatamente entregue a Contratante;

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

Requisitos Sociais, Ambientais e Culturais

4.20. 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).

Requisitos da Arquitetura Tecnológica

4.21. Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos a seguir:

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

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

III - 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 na UFPI, software este responsável por administrar as configurações e monitorar todos os equipamentos de segurança de perímetro de rede utilizados pela UFPI.

Requisitos de Projeto e de Implementação

4.22. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.23. A solução deve ser compatível com o padrão estabelecido na rede da UFPI.

Requisitos de Implantação

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

4.25. 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.

4.26. 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.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.27. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, **60 (sessenta) meses**, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.28. 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.

4.29. 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.

4.30. 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.

4.31. 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.

4.32. 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.

4.33. 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.

4.34. 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.

4.35. 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.

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

4.37. 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.

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

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

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

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

4.42. 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;

4.43. 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;

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

4.45. 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;

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

4.47. 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).

4.48. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

Requisitos de Experiência Profissional

4.49. 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;

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

Requisitos de Formação da Equipe

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

Requisitos de Metodologia de Trabalho

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

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

4.54. 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.

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

4.56. 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.

Requisitos de Segurança da Informação e Privacidade

4.57. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.58. 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).

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

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

4.61. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações do UFPI 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.

4.62. 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 UFPI e imediatamente entregue a Contratante;

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

Sustentabilidade

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

I - bens constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

II - 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;

III - 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

IV - 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).

Indicação de marcas ou modelos *(Art. 41, inciso I, da Lei nº 14.133, de 2021):*

4.65. 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: **Palo Alto**.

Da exigência de carta de solidariedade

4.66. Não se aplica.

Subcontratação

4.67. Não é admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.68. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

4.69. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

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

5.1.2. 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;

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

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

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

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

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

5.1.8. 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;

5.2. São obrigações do CONTRATADO:

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

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

5.2.3. 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 do contrato pela Contratante;

5.2.4. 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;

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

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

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

5.2.8. 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;

5.2.9. 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 do contrato, quando for o caso;

5.3. São obrigações do Órgão Gerenciador do Registro de Preços:

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

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

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

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

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

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

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

5.3.4.2. 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

5.3.4.3. 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.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

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

6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

6.3. 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.

6.4. 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.

Forma de execução e acompanhamento do contrato

Condições de Entrega

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

6.6. 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.

6.7. Os bens deverão ser entregues na **DIVISÃO DE PATRIMÔNIO/ UFPI no** seguinte endereço: Campus Universitário Ministro Petrônio Portella, Bairro Ininga - Teresina - PI, CEP: 64049-550; nos dias úteis de 8h às 12h e das 14h às 18h.

Formas de transferência de conhecimento

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

Procedimentos de transição e finalização do contrato

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

Quantidade mínima de bens ou serviços para comparação e controle

6.10. Não se aplica.

Mecanismos formais de comunicação

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

6.11.1. Ordem de Fornecimento de Bens;

6.11.2. Ata de Reunião;

6.11.3. Ofício;

6.11.4. Sistema de abertura de chamados;

6.11.5. E-mails e Cartas;

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

Formas de Pagamento

6.12. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.13. 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 do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.14. 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.

7. MODELO DE GESTÃO DO CONTRATO

7.1. 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.

7.2. 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.

7.3. 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.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Reunião Inicial

7.5. 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.

7.6. 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.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.4. 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;

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

7.8. 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.

Fiscalização Técnica

7.9. 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);

7.9.1. 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);

7.9.2. 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);

7.9.3. O fiscal técnico do contrato informará ao gestor do contrato, 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).

7.9.4. 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).

7.9.5. 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).

Fiscalização Administrativa

7.10. 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).

7.10.1. Caso ocorra 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).

Gestor do Contrato

7.11. 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).

7.12. 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).

7.13. 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).

7.14. 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).

7.15. 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).

7.16. 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).

7.17. O gestor do contrato deverá elaborar 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).

Critérios de Aceitação

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

7.19. 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).

7.20. 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.

7.21. 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.

7.22. 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.

7.23. 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.

7.24. 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.

7.25. 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.

7.26. 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.

7.27. 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.

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

Procedimentos de Teste e Inspeção

7.29. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

7.29.1. 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.

7.29.2. 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:

7.29.3. 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;

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

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

7.32. 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;

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

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

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

7.36. 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:

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

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

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

7.40. Realizar a criação de objetos, de políticas de segurança e regras de firewall;

7.41. Realizar a configuração do serviço DHCP;

7.42. Configurar modo de alta disponibilidade, com um firewall em modo ativo e outro em modo passivo;

7.43. Verificar a sincronização entre equipamentos (firewall ativo e passivo);

7.44. Verificar o funcionamento do modo de alta disponibilidade, através da simulação de falta de conexão no firewall configurado em modo ativo;

7.45. 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;

7.46. Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;

7.47. 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;

7.48. Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;

7.49. Testar as seguintes funcionalidades no firewall:

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

7.51. Descriptografar tráfego SSL para inspeção de conteúdo;

7.52. Permitir inspeção em camada 7 (nível de aplicação);

7.53. Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e desconhecidos;

7.54. Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;

7.55. Realizar a tradução de endereços IP: NAT (Network Address Translation);

7.56. Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;

7.57. Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;

7.58. Permitir que a autenticação da rede sem fio seja integrada (single sign on) com a solução de WIFI existente.

7.59. 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;

7.60. Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;

7.61. Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

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

7.63. O cumprimento dos prazos e outras obrigações assumidas pela contratada;

7.64. Entrega da documentação exigida;

7.65. Atendimento dos critérios de aceitação;

7.66. Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico e;

7.67. 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;

7.68. 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;

7.69. 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.

Níveis Mínimos de Serviço Exigidos

7.69.1. 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).

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

7.69.3. 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);

7.69.4. 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;

7.69.5. 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;

7.69.6. 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.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.69.7. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, 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.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	“Em relação a Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento, os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 - MEC-UNIVERSIDADE FEDERAL/SE”
3	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.
4	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, multa de 0,1% sobre o valor total do Contrato.
5	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, 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.
6	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.
7	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.
8	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	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.
9	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.
10	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.
11	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. "Em relação a Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento, os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 - MEC-UNIVERSIDADE FEDERAL/SE"

7.70. 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 p Contratado:

7.70.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.70.2. 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. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

8.1. 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.

8.2. 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 **30 (trinta)** dias, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

8.3. 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.

8.4. 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.

8.5. 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.

8.6. 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.

8.7. 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.

8.8. 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.

Liquidação

8.9. 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.

8.9.1. 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.

8.10. 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:

8.10.1. o prazo de validade;

8.10.2. a data da emissão;

8.10.3. os dados do contrato e do órgão Contratante;

8.10.4. o período respectivo de execução do contrato;

8.10.5. o valor a pagar; e

8.10.6. eventual destaque do valor de retenções tributárias cabíveis.

8.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a 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;

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

8.13. 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 (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

8.14. 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.

8.15. 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.

8.16. 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.

8.17. 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.

Prazo de pagamento

8.18. 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.

8.19. 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.

Forma de pagamento

8.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.22. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.23. 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.

8.24. 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.

Cessão de crédito

8.25. 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.

8.26. As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.

8.27. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.28. 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.

8.29. 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. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos)

8.30. 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 FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de Adesão à Ata de Registro de Preços.

10.2. O regime de execução do contrato será o mesmo regime de execução do Órgão Gerenciador.

Exigências de habilitação

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

Habilitação jurídica

10.4. Seguirá as disposições do pregão da UFS. Os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 UNIVERSIDADE FEDERAL DE SERGIPE - UFS.

Habilitação fiscal, social e trabalhista

10.5. Seguirá as disposições do pregão da UFS. Os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 UNIVERSIDADE FEDERAL DE SERGIPE - UFS.

Qualificação Econômico-Financeira

10.6. Seguirá as disposições do pregão da UFS. Os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 UNIVERSIDADE FEDERAL DE SERGIPE - UFS.

Qualificação Técnica

10.7. Seguirá as disposições do pregão da UFS. Os critérios e determinações permanecem conforme as previstas no edital e seus anexos PE 90003/2024, UASG 154050 UNIVERSIDADE FEDERAL DE SERGIPE - UFS.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de **R$ 226.700,00** (Duzentos e vinte e seis mil e setecentos reais) conforme custos unitários apostos na [tabela acima] OU [em anexo].

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. A contratação será atendida pela seguinte dotação:

12.2.1. Estrutura Orçamentária: UO 26279;
12.2.2. PTRES: 230948;
12.2.3. Fonte de Recurso: 1000;
12.2.4. UGR: 156180;
12.2.5. Natureza da Despesa: 33.90.40;

12.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Documento assinado digitalmente ANTONIO PERICLES BONFIM SARAIVA DE OLIVE Data: 18/07/2024 18:10:33-0300 Verifique em https://validar.iti.gov.br **Integrante Requisitante** *Antônio Péricles Bonfim Saraiva de Oliveira* *Coordenador de Infraestrutura* **1167800**	Documento assinado digitalmente ARINALDO LOPES DA SILVA Data: 19/07/2024 10:56:36-0300 Verifique em https://validar.iti.gov.br **Integrante Técnico** *Arinaldo Lopes da Silva* *Analista de Tecnologia da Informação* *2475760*	FLORA DANIELLE RIBEIRO GALVAO DE SA:05493788390 Assinado de forma digital por FLORA DANIELLE RIBEIRO GALVAO DE SA:05493788390 Dados: 2024.07.19 11:16:16 -03'00' **Integrante Administrativo** *Flora Danielle Ribeiro Galvão de Sá* *Assistente em Administração* *3212013*

Autoridade Máxima da Área de TIC
Documento assinado digitalmente Cledjan Torres da Costa Data: 19/07/2024 11:52:12-0300 Verifique em https://validar.iti.gov.br *Clédjan Torres da Costa* *Superintendente de Tecnologia da Informação - STI* ***1821747***

Teresina, 18 de julho de 2024.

Aprovo,

Autoridade Competente
Documento assinado digitalmente EVANGELINA DA SILVA SOUSA Data: 19/07/2024 11:58:53-0300 Verifique em https://validar.iti.gov.br *Evangelina da Silva Sousa* *Pró-Reitora de Administração - PRAD* ***2630268***