

Termo de Referência 15/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
15/2024	153115-MEC-UFRJ-UNIVERSID.FED.DO RIO DE JANEIRO/RJ	ALFREDO ROBERTO SOUZA TEIXEIRA	02/05/2024 13:19 (v 3.1)
Status	CONCLUIDO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC	106/2024	23079.204276/2024-32

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de equipamentos de rede, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATMAT	UND	QUANT	R\$ UNITÁRIO	R\$ TOTAL
1	SOLUÇÃO DE SEGURANÇA DE REDES NGFW - Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux; - Deverá ser entregue em equipamento único, para atender as funcionalidades exigidas; - Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses para suporte, garantia, atualização de firmware e atualização automática de bases de dados, incluindo as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de	609340	UND	01	550.925,65	550.925,65

Intrusos (IPS), VPN IPsec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention.

- Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários;
- Deverá incluir licença para a funcionalidade de VPN SSL;
- Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.
- Deverá incluir licença de atualização para filtro de conteúdo Web;
- Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;
- Deverá possuir licença para número ilimitado de usuários e endereços IP;
- Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual;
- Deverá possuir um relatório de uso de mídia social;
- Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

FUNCIONALIDADES DE FIREWALL

- Deverá possuir controle de acesso à internet por endereço IP de origem e destino;
- Deverá possuir controle de acesso à internet por subrede;
- Deverá suportar tags de VLAN (802.1q);
- Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
- Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá suportar single-sign-on para Active Directory, Citrix e RADIUS;
- Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP);
- Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address

	Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT; • Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana; • Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br; • Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT; • Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4; 3.1.2.14. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay; • Deverá suportar aplicações multimídia, como: H. 323 e SIP; • Deverá possuir tecnologia de firewall do tipo Statefull; • Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões; • Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego; • Deverá suportar PBR – Policy Based Routing; • Deverá permitir a criação de VLANs no padrão IEEE 802.1q; 3.1.2.21. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando); • Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2; • Deverá permitir forwarding de camada 2 para protocolos não IP; • Deverá suportar forwarding multicast; • Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode; • Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP; • Deverá permitir o agrupamento de serviços; • Deverá permitir o filtro de pacotes sem a utilização de NAT;					
--	--	--	--	--	--	--

- Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Deverá possuir mecanismo de anti-spoofing;
- Deverá permitir criação de regras definidas pelo usuário;
- Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;
- Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;
- Deverá possuir a funcionalidade de balanceamento e contingência de links;
- Deverá suportar sFlow;
- Solução deve ser capaz de prover Zero Touch provisioning.
- Deverá possuir Módulo de plataforma confiável (TPM).
- A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.
- O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.
- Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;
- Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
- Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

- Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
- Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
- Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
- Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
- Deverá suportar SIP, H.323 e SCCP NAT Traversal;
- Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
- Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes, criação de filas de prioridade, gerência de congestionamento e QoS;
- Deverá permitir modificação de valores DSCP para o DiffServ;
- Deverá permitir priorização de tráfego e suportar ToS;
- Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;
- Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

- Deverá permitir, na funcionalidade de AntiSpam, verificação do cabeçalho SMTP do tipo MIME;
- Deverá possuir filtragem de e-mail por palavras chaves;
- Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- Deverá possuir, para a funcionalidade de AntiSpam, o recurso de RBL;
- Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;
- Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs.

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

- Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
- Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
- Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras;
- Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;
- Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
- Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
- Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas /scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
- Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
- Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

- Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
- Deverá filtrar o conteúdo baseado em categorias em tempo real;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
- Deverá permitir a criação de regras para acesso /bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso /bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso /bloqueio por subrede de origem;
- Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
- Deverá permitir o bloqueio de redirecionamento HTTP;
- Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
- Deverá possuir Proxy Explícito e Transparente;
- Deverá implementar roteamento WCCP e ICAP;
- Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

- Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
- Deverá estar orientado à proteção de redes;
- Deverá permitir funcionar em modo transparente, sniffer e router;

- Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- Deverá permitir a criação de padrões de ataque manualmente;
- Deverá possuir integração à plataforma de segurança;
- Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Deverá possuir mecanismos de detecção /proteção de ataques;
- Deverá possuir reconhecimento de padrões;
- Deverá possuir análise de protocolos;
- Deverá possuir detecção de anomalias;
- Deverá possuir detecção de ataques de RPC (Remote Procedure Call);
- Deverá possuir proteção contra-ataques de Windows ou NetBios;
- Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
- Deverá possuir proteção contra-ataques DNS (Domain Name System);
- Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
- Deverá possuir métodos de notificação de detecção de ataques;
- Deverá possuir alarmes na console de administração;
- Deverá possuir alertas via correio eletrônico;
- Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

- Deverá ter a capacidade de resposta/logs ativa a ataques;
- Deverá prover a terminação de sessões via TCP resets;
- Deverá armazenar os logs de sessões;
- Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- Deverá mitigar os efeitos dos ataques de negação de serviços;
- Deverá permitir a criação de assinaturas personalizadas;
- Deverá possuir filtros de ataques por anomalias;
- Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Deverá permitir filtros de anomalias de protocolos;
- Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Deverá suportar verificação de ataque na camada de aplicação;
- Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;
- Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

FUNCIONALIDADE DE VPN

- Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
- Deverá possuir suporte a VPNs IPSec Site-to-Site e VPNs IPsec Client-to-Site;
- Deverá possuir suporte a VPN SSL;
- Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

- A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X; 3.1.7.9.
- Deverá permitir a arquitetura de VPN hub and spoke;
- Deverá possuir suporte a inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;
- Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P; Transferência de arquivos; VoIP;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso /bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso /bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso /bloqueio por endereço IP de origem;
- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá permitir a criação de regras para acesso /bloqueio por subrede de origem e destino;

- Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
- Deverá permitir criação de padrões de aplicação manualmente;

FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

- O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados confidenciais e ou de identificação pessoal não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;
- Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;
- Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;
- Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;
- Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;
- Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
- Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes /saintes possui um tamanho máximo especificado pelo administrador;
- Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;
- Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

- Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;
- Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

- Deverá permitir a criação de endereços IPs virtuais;
- Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
- Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
- Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted Round Robin, First Alive e HTTP host;
- Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;
- Deverá permitir que seja mantido o IP de origem;
- Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;
- Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
- Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

FUNCIONALIDADE DE SD-WAN

- A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.
- A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.
- A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.
- Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.
- A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site.
- A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15.
- Reconhecimento em camada 7 totalmente segregado da camada 4.
- Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.
- O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)
- A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6.

- A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
- A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SDWAN.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
- A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

CARACTERÍSTICAS ESPECÍFICAS

- Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable.
- A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.
- IPS com capacidade mínima de processamento de 12 (doze) Gbps.
- Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 10 (dez) Gbps.
- Caso o fabricante divulgue múltiplos valores para este requisito, somente o de menor valor será aceito;

	- Inspeção SSL Throughput com capacidade mínima de processamento de 9 (nove) Gbps. - VPN com capacidade de, pelo menos, 55 (cinquenta e cinco) Gbps de tráfego IPSec. - VPN SSL com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego. - Suportar no mínimo throughput de 100 Mpps (milhões de pacotes por segundo) - Deverá suportar 8.000.000 (oito milhões) de sessões concorrente. - Deverão ser licenciados para suportar, pelo menos, 8.000 (oito mil) usuários de VPN SSL. - Deverá suportar, pelo menos, 500.000 (quinhentas mil) novas conexões por segundo. - Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site. - Deverá suportar, pelo menos, 40.000 (quarenta mil) túneis de VPN Client-Site. - Deverá possuir, pelo menos, 04 (quatro) interfaces SFP28 25GE. - Deverá possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE. - Deverá possuir, pelo menos, 14 (quatorze) interfaces 1 GE RJ 45. - Deverá possuir porta USB 3.0 para conexão de modem 3G/4G. Deverá acompanhar 2 SFP+ 10 Gbps multimodo para interligação aos equipamentos adjacentes. - Deverá possuir homologação junto a ANATEL; - Desejável que seja capaz de gerenciar equipamentos de pontos de acesso sem fio, via funcionalidade de Controladora Wireless. - Desejável que seja capaz de gerenciar switches, via funcionalidade de Controladora Switch. - Treinamento para equipe técnica sobre solução adquirida. Migração de configurações para o equipamento adquirido. APENAS COMO REFERÊNCIA: FORTNET FORTGATE 600F SERIES					
2	Roteador Modular com as seguintes especificações:	611580	UND	01	290.160,60	290.160,60

- Possuir no mínimo, 30 (Trinta) portas de 10Gb/1Gb SFP+.
- Possuir, no mínimo, 6 (Seis) portas de 100Gb/40Gb QSFP28.
- Deverá possuir capacidade de switching, de pelo menos, 2.2 Tbit/s.
- Deverá possuir 5 anos de garantia on site 5x8 (NBD);
- Deverá possuir licenciamento para pleno funcionamento por pelo menos 5 anos;
- Deverá possuir controladora redundante;
- Deve possuir capacidade de encaminhamento de pacotes de pelo menos 450 Mpps.
- O equipamento deverá ocupar a altura máxima de 3 (Três) unidades de rack (3U).
- Deve ser fornecido com módulos de ventilação no corpo do equipamento com capacidade suficiente para resfriar o equipamento.
- O equipamento deverá possuir largura que possibilite a instalação em rack padrão 19" (482,6 mm). Para tal instalação, deverá ser fornecido kit completo de suporte para montagem em rack padrão 19".
- O equipamento deverá possuir pelo menos duas fontes redundantes internas ao chassi do tipo AC e hot-swappable.
- O equipamento deverá possuir módulos de ventiladores redundantes e hot-swappable.
- O Roteador deve suportar pelo menos 16G de memória RAM
- Possuir capacidade de comutação igual ou superior à soma das capacidades de todas as portas solicitadas.
- Possuir suporte a IPv4/IPv6 Dual Stack.
- Deve possuir pelo menos 2.000.000 (dois milhões) de rotas IPv4 e 1.000.000 (um milhão) de rotas IPv6 em FIB.
- Possuir suporte a QoS Hierárquico (H-QoS).
- Possuir suporte a DiffServ Model, WRED ou similar, PQ, WFQ ou similar.
- Possuir suporte a traffic shaping e policy.

- Possuir suporte a L2TP.
- Possuir suporte a GRE.
- Possui suporte a IPSec.
- Possui suporte SNMP v1, v2 e v3 acompanhado de todas as MIBs disponíveis.
- Realizar Roteamento IPv4 com, no mínimo, os protocolos: OSPFv2, IS-IS e RIPv2.
- Deve suportar pelo menos 32 áreas OSPF.
- Deve suportar as seguintes RFC's relativas ao protocolo OSPFv2:

RFC 2328 – OSPF Version 2;

RFC 3101 – The OSPF NSSA Option;

RFC 2370 – The OSPF Opaque LSA Option;

- - Deve suportar pelo menos 500 adjacências OSPF.
 - Realizar Roteamento IPv6 com, no mínimo, os protocolos: OSPFv3, IS-ISv6 e RIPv6.
 - Possuir suporte para BGP (IPv4 e IPv6), com capacidade mínima para estabelecer simultaneamente vizinhança BGP com duas concessionárias de serviços de telecomunicações em portas distintas do equipamento.
- - Deve suportar as seguintes RFC's relativas ao protocolo BGP:
 - RFC 4271 – A Border gateway Protocol (BGPv4);
 - RFC 4724 – Graceful Restart Mechanism for BGP-4;
 - RFC 4360 – BGP Extended Communities Attribute;
 - RFC 4456 – BGP Route Reflection;
 - RFC 1997 – BGP Communities Attribute;
 - RFC 2283 – Multiprotocol Extension for BGP-4
- Deve implementar autenticação BGP, com no mínimo o algoritmo MD5.
- Deve ser capaz de suportar pelo menos 1.000 (mil) vizinhanças ou peers BGP.

- Possuir suporte a Roteamento Multicast: IGMP, PIM-SM, PIM-SSM.
- Possuir suporte VRRP e VRRPv6.
- Possuir mecanismo de exportação de flows de tráfego: Netflow, Sflow, Netstream ou similar.
- Possuir suporte à tecnologia de telemetria.
- Possuir suporte, em sua configuração nativa, para filtragem IPv4 e IPv6 em função dos endereços de origem/destino e portas TCP e/ou UDP de origem/destino, seja por intermédio de ACLs, seja por mecanismo equivalente.
- Possuir suporte a pelo menos 2.000 (duas mil) ACL's.
- Possuir suporte para NAT.
- Deve possuir suporte para NAT 1:N, N:N, PAT ou NATPT;
- Possuir suporte a VxLAN.
- Suporte aos mecanismos L2:
 - STP;
 - RSTP;
 - MSTP;
 - Implementar 4000 VLANs simultaneamente;
 - Implementar sub-interfaces VLAN 802.1q;
- Possuir suporte a 802.3ad (LACP).
- Possuir suporte a 802.1ad (QinQ).
- Deve possuir capacidade de pelo menos 2.000 (duas mil) VRF's.
- Deve possuir mecanismo de importação de rotas entre diferentes VRF's;
- Possuir suporte a MPLS, MPLS QoS, MPLS LDP e MPLS TE.
- Possuir suporte a MPLS L2VPN VPLS e VPWS.
- Possuir suporte a MPLS L3VPN.
- Deve implementar SRv6, SRv6-TE e SRv6-BE.
- Possuir suporte a PCEP.
- Possuir suporte a Ethernet virtual private network (EVPN) e às seguintes implementações:
 - EVPN L3VPN
 - EVPN VXLAN
 - EVPN sobre SR-MPLS
- Deve possuir suporte a integração BGP MPLS (MP-BGP, BGP4+ ou similar).
- Possuir suporte a URPF.
- Deve implementar NTP ou SNTP.
- Deve implementar PBR - Policy Based Routing.

	• Possuir, no mínimo, mecanismo de configuração do equipamento baseado em linhas de comando (CLI). Poderá, adicionalmente, suportar mecanismo de configuração e gerência baseado em GUI e/ou MIB. A comunicação nesses casos deverá oferecer suporte de encriptação por intermédio de SSHv2 e SNMPv3; • O equipamento deve ter a capacidade de efetuar teste de níveis de serviços (SLA) especificados. Devem ser suportadas no mínimo as seguintes operações de teste: ◦ ICMP echo; ◦ TCP connect (em porta TCP indicada pelo administrador); ◦ UDP echo (em porta UDP indicada pelo administrador); • Possuir suporte a IEEE 1588v2. • Suporte a Ethernet OAM • Possuir suporte a ZTP (Zero touch provisioning) • Deve possuir suporte a rollback de configuração. • O equipamento deve possuir espaço de armazenamento suficientes para pelo menos duas instâncias ou imagens do sistema operacional. • Suporte a SNMP Dying Gasp, ou mecanismo semelhante, que permita que seja identificado quando um dispositivo fica offline devido a desligamento ou queda de energia. • Caso algum dos itens seja dependente de licenciamento específico, este licenciamento deverá acompanhar o equipamento/software. • Possuir homologação junto a ANATEL; • O sistema operacional do roteador deve suportar configuração de scripts para automação de tarefas. • Treinamento para equipe técnica sobre a solução adquirida. • Migração de configurações para o equipamento adquirido. APENAS COMO REFERÊNCIA: HUAWEI NE8000 – M8					
3	Switch 24 portas 10/100/1000 + 4 SFP+, com as seguintes especificações:	463274	UND	04	14.910,96	59.643,84

Conectividade

- Deve possuir 24 portas padrão Gigabit Ethernet 10/100/1000Base-T em conector RJ45;
- Deve possuir 4 portas ativas 10 Gigabit Ethernet padrão SFP+;
- **Cada equipamento deverá acompanhar 2 SFP+ 10Gbps multimodo para interligação ao roteador core;**
- As portas 10/100/1000Base-T deverão suportar autonegociação de velocidade, modo de operação e detecção MDI-MDIX quando operando em 10 /100Base-TX;
- Deve possuir porta console serial padrão RS-232 com conector DB-9 ou RJ45 acompanhado do respectivo cabo para conexão ao PC;

Controle

- Deve suportar Jumbo Frames de 9K;
- Deve suportar 4K VLANs ativas segundo o protocolo IEEE 802.1Q;
- Deve suportar 2.000 regras de ACL;
- Deve suportar implementação de Voice VLANs;
- Deve implementar suporte a QinQ;
- Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;
- Implementar QoS com base no protocolo 802.1p CoS;
- Deve implementar IGMP Snooping v1, v2 e v3;
- Deve possibilitar a limitação de Broadcast, Multicast e Unicast;
- Deve implementar o gerenciamento de banda;
- Deve implementar os mecanismos de controle de fila: SP (Strict Priority) ou PQ (Priority Queuing) ou WRR (Weighted Round Robin) por porta;

Disponibilidade

- Implementar o protocolo Spanning Tree (802.1D);
- Implementar o protocolo Rapid Spanning Tree (802.3w);
- Deve implementar o protocolo Multiple Spanning Tree (802.1s) com suporte a pelo menos 16 instâncias ou MSTI's;
- Deve suportar detecção de loop (loopback detection);
- Deve implementar BPDU Guard;
- Deve suportar agregação dinâmicos no padrão LACP ou estático.
- Deve suportar protocolo de resiliência em anel ERPS ITU-T G.8032;
- Deve permitir empilhar até 8 switches;

Gerenciamento

- Deve suportar gerenciamento SNMP v1, v2c e v3;
- Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;
- Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPS;
- Deve permitir acesso local a console CLI;
- Deve possuir capacidade para medição ou aferição da qualidade da rede através de IPSLA ou NQA ou outros mecanismos similares capazes de realizar testes de: ICMP Echo, TCP e UDP
- Deve implementar cliente DNS;
- Deve suportar o protocolo LLDP e LLDP-MED (IEEE 802.1ab);
- Deve permitir upgrade de firmware;
- Deve permitir a atualização de firmware via HTTP, TFTP ou FTP;
- Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;

- Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;
- Deve implementar mecanismos de Telemetria;
- Deve suportar SNMP;
- Deve suportar HTTP;
- Deve implementar programabilidade com linguagem de script Python ou Java ou outras linguagens para fins de automação;
- Deve suportar NTP ou SNTP;
- Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;

Segurança

- Deverá possuir proteção a ataques DOS;
- Deverá possuir proteção a CPU;
- Deverá suportar autenticação local e através de servidor RADIUS ou TACACS+ ou HWTACACS;
- Deve suportar VLAN e política de QoS;
- Deve possuir suporte a AAA (Authentication, Authorization and Account) em servidores RADIUS TACACS+ ou HWTACACS;
- Deve suportar implementação de VLANs para visitantes;
- Deve permitir filtragem de pacotes identificados por cabeçalho ethernet ou IP através de ACL;
- Deve suportar DHCP snooping;
- Deve suportar IP Source Guard;
- Desempenho
- Deve possuir capacidade de vazão de ao menos 128 Gbps;
- Deve chavear no mínimo 96 Mpps;
- Tabela de endereços MAC com capacidade para no mínimo 32.000 endereços;

- Deve prover roteamento IP para no mínimo 1000 interfaces VLAN;
- Deve suportar pelo menos 2.000 rotas IPv4 em FIB;
- Deve suportar pelo menos 1.000 rotas IPv6 em FIB;
- Funcionalidades L2 e padrões
- Deve ser compatível com os seguintes padrões:
- IEEE 802.1D (STP)
- IEEE 802.1p (COS)
- IEEE 802.1Q (VLAN)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.1X (Security)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ad (Link aggregation)
- IEEE 802.3i(10BASE-T)
- IEEE 802.3u (Fast Ethernet)
- IEEE 802.3x (Flow control)
- IEEE 802.3z (Gigabit)
- IEEE 802.1AB (Link Layer Discovery Protocol)

Funcionalidades Multicast/Layer 3

- Deve suportar PIM-SM e PIM-DM;
- Deve permitir roteamento entre VLANs via sub-interface ou interface VLAN;
- Deve implementar os protocolos de roteamento dinâmico OSPFv2, OSPFv3, single e multi-area;
- Deve implementar VRRP e VRRP6 para prover redundância de gateway;

Gerais

• Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente; • Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19; • O equipamento deverá ocupar uma unidade de rack; • A proponente deverá apresentar declaração do fabricante comprovando que ela é instaladora credenciada; • Deve possuir temperatura de operação de 0° C a 50° C; • Possuir homologação junto a ANATEL; • Deve acompanhar a licença de gerenciamento segundo a especificação do Software de gerenciamento. • Alertas automáticos sobre eventos importantes, como dispositivos de rede que ficam offline. • Treinamento para equipe técnica sobre a solução adquirida. • Deverá possuir 5 anos de garantia on site 5x8 (NBD) • Deverá possuir licenciamento para pleno funcionamento por pelo menos 5 anos; APENAS COMO REFERÊNCIA: HUAWEI CLOUD ENGINE S5735 – L24T4X					
---	--	--	--	--	--

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.

1.3.1. O prazo de vigência da contratação é de 01 (hum) ano para todos os itens, na forma do artigo 105 da Lei nº 14.133, de 2021, com garantia de 05 (cinco) anos para os itens 01, 02 e 03 on site (5 X 8 NBD), contados do(a) aceite definitivo do objeto.

1.4. 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

2.1 A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A necessidade premente de substituição dos firewalls e roteador de borda da UFRJ fundamenta-se na vitalidade desses equipamentos para as atividades acadêmicas e administrativas essenciais. Os sistemas cruciais, tais como o Sistema Eletrônico de Informações (SEI), Sistema de Matrícula e Controle Acadêmico (SIGA), Sistema de Pessoal (SISUFRJ e SIRHU), Ambiente Virtual de Aprendizagem (AVA UFRJ), SIAC (Sistema de Gestão da Semana de Integração Acadêmica), Sistema de Gestão de Cursos e Eventos (SGCE), serviços de e-mail, entre outros, dependem diretamente da integridade e disponibilidade da infraestrutura de rede.

O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2023 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2023 do Universidade Federal do Rio de Janeiro, conforme demonstrado abaixo:

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Capacitação

- 4.1 Será necessário treinamento à equipe que atuará com a solução e deverá ser com o mínimo de horas necessárias para a perfeita capacitação da equipe, com duração conforme especificação do fabricante do equipamento.
- 4.2 O treinamento necessário será aplicado aos itens 01, 02 e 03 deste termo;
- 4.3 Deverá ser do tipo oficial do fabricante da solução ofertada;
- 4.4 Deverá ser realizado para uma turma de até 15 alunos, com carga horária mínima de 40 hs para o item 01 e 20 hs para o item 02 e 20 hs para o item 03;
- 4.5 Deverá ser ministrado por instrutor certificado pelo fabricante do equipamento, com nível profissional de certificação;
- 4.6 Deverá ocorrer no formato presencial;
- 4.7 Deverá ser realizado em datas previamente agendadas entre a CONTRATANTE e CONTRATADA;
- 4.8 Deverá ocorrer em dias úteis, dentro do horário comercial;
- 4.9 Deverá ocorrer nas dependências da UFRJ, Cidade Universitária – Rio de Janeiro – RJ, devendo estar previsto pela CONTRATADA os custos relativos ao transporte, hospedagem e refeições do instrutor, no Rio de Janeiro.

Requisitos Legais

- 4.10 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

- 4.11 Devido às características da solução, há necessidade de realização de manutenções corretivas pela Contratada, visando à manutenção da disponibilidade da solução, sempre que for necessário, no período de garantia;

Requisitos Temporais

4.12 A Entrega dos equipamentos deverá ser efetivada no prazo máximo de até 15 (quinze) dias corridos para as capitais dos estados, a contar do recebimento da Nota de Empenho, emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

Requisitos de Segurança e Privacidade

4.13 A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, a ser informada no momento da instalação dos bens.

Requisitos de Implantação

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

4.14.1. Para os itens 01 e 02:

4.14.1.1. Licenciamento de, no mínimo, 05 (cinco) anos para plena utilização;

4.14.1.2. Treinamento para equipe técnica para a solução adquirida, conforme subitem 4.1 deste termo;

4.14.1.3. Migração de configurações do equipamento atual para o equipamento adquirido.

4.14.2. Para o item 03:

4.14.2.1. Licenciamento de, no mínimo, 05 (cinco) anos para plena utilização;

4.14.2.2. Treinamento para equipe técnica para a solução adquirida, conforme subitem 4.1 deste termo;

Requisitos de Garantia, Manutenção e Assistência Técnica

4.15 O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (ses-senta) meses on site (5 X 8 NBD), ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.16 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.

4.17 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.

4.18 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.

4.19 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.

4.20 Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 02 (dois) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.21 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.

4.22 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.

4.23 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.

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

4.25 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.

Requisitos de Experiência Profissional

4.26 Os serviços de assistência técnica, suporte e garantia, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

Requisitos de Metodologia de Trabalho

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

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

4.29 O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 08 horas por dia e 5 dias por semana de maneira eletrônica e 08 horas por dia e 5 dias por semana por via telefônica.

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

Sustentabilidade

4.31 Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos previstos nos estudos Técnicos Preliminares, anexo deste Termo.

Da exigência de carta de solidariedade

4.32 Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

4.33 Não é admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.34 Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

4.35 Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.36 A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.37 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;

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

6.1. O gestor do contrato emitirá a Nota de Empenho para a entrega dos bens desejados.

6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na Nota de Empenho.

6.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.

Forma de execução e acompanhamento do contrato

Condições de Entrega

6.4 O prazo de entrega dos bens é de até 15 (quinze) dias, contados do(a) emissão da Nota de Empenho, em remessa única.

6.5 Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 02 (dois) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.6 Os bens deverão ser entregues no seguinte endereço: Rua Paulo Emídio Barbosa, s/n – Cidade Universitária – Ilha do Fundão, Rio de Janeiro – RJ – Divisão de Almoxarifado Central.

Formas de transferência de conhecimento

6.7 A transferência do conhecimento deverá ser realizada observando-se o que segue (somente itens 01, 02 e 03):

6.8 Durante o curso para a equipe técnica, que deverá estar 100% satisfeita quanto a essa transferência.

Procedimentos de transição e finalização do contrato

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

Mecanismos formais de comunicação

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

6.11 Ordem de Fornecimento de Bens;

6.12 Ata de Reunião;

6.13 Ofício;

6.14 Sistema de abertura de chamados;

6.15 E-mails e Cartas;

6.16 Outros meios legais de comunicação.

Formas de Pagamento

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

Manutenção de Sigilo e Normas de Segurança

6.18 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.

6.19 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, encontra-se no ANEXO 01.

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 02(dois) 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);

7.10 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 regula-rização 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);

7.11 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);

7.12 O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.13 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).

7.14 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

7.15 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).

7.16 Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

7.17 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).

7.18 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).

7.19 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).

7.20 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).

7.21 O gestor do contrato tomará providências para a formalização de processo administrativo de res-ponsabilização 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).

7.22 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).

7.23 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).

Crítérios de Aceitação

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

7.24.1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.24.2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisas, 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.

7.24.3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma orga-nizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

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

7.24.5. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

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

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

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

7.24.9. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades pre-vistas 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.

Níveis Mínimos de Serviço Exigidos

7.25 Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.	
Meta a cumprir	IAE < 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.

Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	IAE = <u>TEX – TEST</u> Onde: IAE – Indicador de Atraso de Entrega da OFB; TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB. A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB. A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quando o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: Menor ou igual a 0 – Pagamento integral da OFB; De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.

	Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.
--	---

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.26. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Con-tratante, 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 05 (cinco) horas úteis.	Multa de 0,5 (zero virgula cinco) % 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 10 (dez) dias úteis.
		Após o limite de 10 (dez) dias úteis, aplicar-se-á multa de 7 (sete) % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 1 (um) % sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20.
		Glosa de 2 (dois) % sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30.
		Glosa de 5 (cinco) % sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50.
		Glosa de 10 (dez) % sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00.
		Multa de 5 (.cinco) % sobre o valor do Contrato e Glosa de 15 (quinze) % sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de até 10 (dez) % do valor total do Contrato.

7.27. 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:

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

7.27.2 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 02 (dois) 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 15 (quinze) 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.
- 8.10. 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.
- 8.11. 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:
- 8.12. o prazo de validade;
 - 8.13. a data da emissão;
 - 8.14. os dados do contrato e do órgão Contratante;
 - 8.15. o período respectivo de execução do contrato;
 - 8.16. o valor a pagar; e
 - 8.17. eventual destaque do valor de retenções tributárias cabíveis.
- 8.18. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circuns-tância 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;
- 8.19. 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.
- 8.20. 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).
- 8.21. 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.
- 8.22. 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.
- 8.23. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contra-tual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

8.24. 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

8.25. 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.

8.26. 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

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

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

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

8.30. 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.

8.31. 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

8.32. 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.

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

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

8.35. 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.

8.36. 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)

8.37. A cessão de crédito não afetará a execução do objeto Contratado, que continuará sob a integral responsabilidade do Contratado.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

9.1. O fornecedor será selecionado por meio da realização de procedimento de Aquisição Direta, na modalidade Emergencial (Artigo 75o, Inciso VIII da Lei 14.133), sob a forma de Cotação Eletrônica, com adoção do critério de julgamento pelo menor preço.

9.2. O regime de execução do contrato será por preço unitário.

Exigências de habilitação

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

Habilitação jurídica

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

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

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

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

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

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

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

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

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

Habilitação fiscal, social e trabalhista

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

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

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

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

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

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

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

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

Qualificação Econômico-Financeira

9.21. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando;

- 9.22. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
- 9.23. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.
- 9.24. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;
- 9.25. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.
- 9.26. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação [capital mínimo] de 5 (cinco)% do valor total estimado da contratação.
- 9.27. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).
- 9.28. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

- 9.29. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.
- 9.30. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contra-tos executados com as seguintes características mínimas:
- 9.31. Firewall com IPS mínimo de 10 GBPS para o item 01;
- 9.32. Roteador de borda com Throughput mínimo de 300 GBPS para o item 02;
- 9.33. Para os demais itens está dispensada a apresentação de comprovação de fornecimento.
- 9.34. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 9.35. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 9.36. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de R\$ 900.730,09 (Novecentos mil, setecentos e trinta e nove centavos), conforme custos unitários apostos na tabela acima.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União, a serem indicados no processo, no momento oportuno.

1. Responsáveis

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

GABRIEL RODRIGUES CALDAS DE AQUINO

Diretor da Divisão de Segurança

RENATO REZENDE CALANDRINI DE AZEVEDO

Diretor da Divisão de Redes

ANA MARIA DE ALMEIDA RIBEIRO

Superintendente Geral de Tecnologia da Informação e Comunicação

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - TERMO DE COMPROMISSO DE MANUTENCAO DE SIGILO.pdf (243.01 KB)