TERMO DE REFERÊNCIA

Centro Universitário Municipal de Franca - UniFACEF

Objeto: Contratação de solução integrada de segurança de rede, composta por equipamento de alto desempenho (firewall de próxima geração - NGFW) e licenciamento de software por 12 meses.

(Processo Administrativo n° 257/2025)

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de solução integrada de segurança de rede, composta por equipamento de alto desempenho (firewall de próxima geração - NGFW) e licenciamento de software para proteção abrangente por 12 meses, nos termos abaixo, conforme condições e exigências estabelecidas neste instrumento.

1.2. Ser provido com equipamento para proteção por perímetro (Firewall), a ser instalado nas dependências da Uni-FACEF, com, no mínimo, as seguintes características:

1.1.1. Os equipamento(s) devem ser novos e sem histórico de uso anterior;

1.1.2. Os equipamento(s) devem estar em produção atual, ou seja, não podem ser obsoletos ou descontinuados;

1.1.3. É fundamental que os dispositivos não estejam próximos da data de fim de suporte oficial do fabricante, garantindo sua viabilidade e suporte a longo prazo;

1.1.4. Na proposta deverá ser fornecido a marca e o modelo do(s) equipamento(s) para fins de identificação das funcionalidades;

1.1.5. Sempre que requerido pela CONTRATANTE, a CONTRATADA deverá apresentar declaração informando que ela é parceira do fabricante da solução ofertada e que possui capacidade técnica e operacional para execução do objeto deste termo de referência, descritos no presente edital;

1.1.6. Deve ser disponibilizado na forma de Next Generation Firewall (NGFW) ou Unified Threat Management (UTM);

1.1.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

1.1.8. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.1.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

1.1.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.1.11. Ser disponibilizado na forma de appliance de hardware, com recurso de alta disponibilidade em modo ativo-ativo ou ativo-passivo;

1.1.12. A CONTRATADA deverá fornecer todos os cabos de alimentação, cabos de console e mídias, bem como todos os acessórios necessários para a instalação do(s) equipamento(s), em conformidade com as recomendações do fabricante e padrões internacionais vigentes;

1.1.13. Deve ser fornecido com fonte de alimentação para funcionamento em rede elétrica 110V e 220V. A fonte fornecida deve suportar a operação da unidade com todos os módulos de interface ativos;
1.1.14. Permitir que sejam ligados no mínimo 2 links de internet de diferentes operadoras;
1.1.15. Para garantir maior segurança, não serão aceitos computadores com instalação de sistemas operacionais tradicionais do mercado, tais como Microsoft Windows, FreeBSD, Solaris, AIX ou GNU/Linux;
1.1.16. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;
1.1.17. Deverá ser fornecido documentação técnica do(s) equipamento(s) proposto, contemplando manual de usuário de utilização do(s) equipamento(s), podendo ser em idioma português e/ou inglês;
1.1.18. Deverão ser fornecidas as licenças para todas as funcionalidades solicitadas neste termo de referência, pelo período de validade do contrato;
1.1.19. O equipamento deverá ser entregue em até 10 dias corridos após a assinatura do contrato.

1.3. A plataforma de segurança deverá possuir as funcionalidades:
1.3.1. Firewall;
1.3.2. Traffic Shapping e QoS;
1.3.3. Gateway Antivírus, Anti-Spam, Anti-Bot;
1.3.4. Controle de aplicações Web e Filtro de conteúdo Web;
1.3.5. Proxy Web Transparante/Explicíto e Proxy Reverso;
1.3.6. IPS (Sistema de Prevenção de Intrusos);
1.3.7. VPN IPSEC e VPN SSL;
1.3.8. Controle para Identificação de usuários;
1.3.9. Prevenção de Ameaças do tipo “0-Day”

1.4. Deverá atender, no mínimo, os seguintes recursos de Firewall:
1.4.1. Controle de acesso através de regras baseadas em usuário, grupo de usuários, endereços IP, FQDN, horário, protocolo e aplicação;
1.4.2. Criação de objetos e agrupamento de objetos de usuários, redes, protocolos e serviços para facilitar a criação de regras;
1.4.3. Funcionamento em modo router, proxy explícito e/ou vlan-tagged;
1.4.4. Deverá permitir o controle de acesso por sub-rede;
1.4.5. Suporte a tags de VLAN (802.1q);
1.4.6. Suportar o protocolo 802.1AX ou 802.3ad (LACP-Link Aggregation Control Protocol);
1.4.7. Dever possuir recurso de depuração de pacotes enviado/recebidos, similar ao comando tcpdump;
1.4.8. Integração com Microsoft Active Directory para autenticação de usuários;
1.4.9. Deverá suportar Single-sign-on para Microsoft Active Directory;
1.4.10. Controle de acesso à internet por períodos do dia (horários e dia da semana);
1.4.11. Controle de acesso à internet por domínio (exemplo: serpro.gov.br e gov.br);
1.4.12. Suporte PBR - Policy Based Routing;
1.4.13. Filtro de pacotes sem controle de estado “stateless” para verificação em camada 2;
1.4.14. Criação de serviços por porta ou conjunto de portas dos protocolos TCP e UDP;
1.4.15. Abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
1.4.16. Prover mecanismo contra ataques de falsificação de endereços (anti-spoofing);
1.4.17. Suporte a sFlow ou NetFlow;

1.4.18. Detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas;
1.4.19. Possibilitar criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (tablets, celulares e PCs);
1.4.20. Suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
1.4.21. Suportar SIP/H.323/SCCP NAT Traversal;
1.4.22. Recurso para Tradução de endereços IP: NAT (Network Address Translation) estático e dinâmico;
1.4.23. Deve suportar Tradução de porta (PAT);
1.4.24. Suporte a roteamento estático e dinâmico: RIP V1, RIP V2, OSPF e BGP;
1.4.25. Deve possuir suporte a Jumbo Frames;
1.4.26. Suportar otimização do tráfego entre dois equipamentos;
1.4.27. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
1.4.28. Conexão criptografada entre estação de gerenciamento e o appliance, tanto em interface gráfica, quanto em CLI (linha de comando);

1.5. Suporte a configuração de alta disponibilidade Ativo/Ativo: Em layer 2 e 3:
1.5.1. A configuração em alta disponibilidade deve sincronizar: Sessões;
1.5.2. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
1.5.3. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
1.5.4. A configuração em alta disponibilidade deve sincronizar:Tabelas FIB;
1.5.5. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
1.5.6. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
1.5.7. Deve estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
1.5.8. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo permitindo a distribuição de carga entre diferentes contextos;

1.6. Deverá atender aos seguintes requisitos de gerência:
1.6.1. A solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
1.6.2. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
1.6.3. A solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
1.6.4. O gerenciamento Web deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
1.6.5. Deve possuir um mecanismo de busca por comandos ou autocomplete no gerenciamento via SSH, de forma a facilitar a configuração pelo administrador;
1.6.6. Deve suportar a criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;
1.6.7. Deve suportar backup automático das configurações e rollback de configuração para a última configuração salva;
1.6.8. Deve permitir a visualização dos logs de uma regra especial em tempo real;
1.6.9. Deve possibilitar a integração com outras soluções de SIEM de mercado;
1.6.10. O console de administração deve suportar pelo menos inglês, espanhol e português do Brasil;

1.6.11. O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança;
1.6.12. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
1.6.13. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.7. Deverá atender, no mínimo, os seguintes recursos de Traffic Shaping e Priorização:
1.7.1. Controle e a priorização do tráfego, priorizando banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
1.7.2. Limitar individualmente a banda utilizada por aplicações (por exemplo, peer-to-peer, streaming, chat, VoIP, web, etc.);
1.7.3. Identificação transparente de usuários cadastrados no Microsoft Active Directory;
1.7.4. Definir a banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo ou aplicação;
1.7.5. Deverá suportar o controle de banda, tanto para limitar, como para expandir, baseado em critérios por grupo de usuários do Microsoft Active Directory, ou por sub-rede de origem e destino, ou endereço IP de origem e destino.

1.8. Deverá atender, no mínimo, os seguintes recursos de Antivírus, Anti-Spam e Anti-Bot:
1.8.1. Função de Antivírus em tempo real para ambiente de gateway internet para os seguintes protocolos: HTTP, SMTP, IMAP, POP3 e FTP;
1.8.2. Bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
1.8.3. Proteção contra conexões a servidores masters de controle de Botnet (Botmasters);
1.8.4. Bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
1.8.5. Permitir o bloqueio de download de arquivos por tamanho;
1.8.6. A solução de UTM deve ter a capacidade de detectar e bloquear spyware.

1.9. Deverá atender, no mínimo, os seguintes recursos de Controle de aplicações Web e Filtro de conteúdo Web:
1.9.1. O recurso de filtro de conteúdo web deverá estar integrado na solução de segurança;
1.9.2. Deverá suportar integração com Microsoft Active Directory;
1.9.3. Identificação transparente de usuários do Microsoft Active Directory;
1.9.4. Filtro de conteúdo baseado em categorias;
1.9.5. Deverá categorizar a página web, tanto pela sua URL, como pelo endereço IP;
1.9.6. Dispor de pelo menos 50 categorias para classificação de sites web;
1.9.7. Dispor de base de dados com, no mínimo, 200 milhões URLs;
1.9.8. Deverá suportar monitoramento do tráfego internet, com opção de bloqueio de acesso aos usuários;
1.9.9. Deverá possibilitar a criação de categorias personalizadas;
1.9.10. Deverá permitir a reclassificação de sites web;
1.9.11. Deverá efetuar filtragem de conteúdo de tráfego WEB de URLs conhecidas como fonte de material impróprio e/ou códigos (programas/scripts) maliciosos, sejam em applets Java, cookies, activeX. Deverá manter base de URL própria atualizável de acordo com políticas da solução de segurança;
1.9.12. Bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
1.9.13. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
1.9.14. Deverá efetuar atualizações regulares do produto sem interromper a execução dos serviços de filtragem de conteúdo web;

1.9.15. Deverá permitir a criação de regras para acesso/bloqueio por categorias, no mínimo, por grupos de usuários do Microsoft Active Directory, por endereço IP de origem/destino, e por sub-rede de origem/destino.
1.9.16. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;
1.9.17. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
1.9.18. Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;
1.9.19. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
1.9.20. 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;
1.9.21.
1.9.22. Deverá atender, no mínimo, os seguintes recursos de Proxy Web Transparante/Explicíto e Proxy Reverso:
1.9.23. Deverá funcionar em modo Proxy Explícito para HTTP e HTTPS, e em Proxy Transparente para HTTP;
1.9.24. Deverá permitir configuração da porta do Proxy Explícito;
1.9.25. Deverá suportar a funcionalidade através de Proxy Reverso para redirecionamento de URLs do tipo http ou https redirecionando para o servidor específico;

1.10. Deverá atender, no mínimo, os seguintes recursos de Detecção e Prevenção de Intrusão (IDS/IPS):
1.10.1. Deverá efetuar a inspeção de tráfego por regra baseada em IP origem/destino, por protocolo, ou por porta (TCP/UDP);
1.10.2. Deverá possuir base de assinaturas de IPS com pelo menos 10.000 ameaças conhecidas;
1.10.3. Deverá efetuar a atualização automática da base de assinaturas;
1.10.4. Deverá permitir a criação de assinaturas personalizadas;
1.10.5. Deverá permitir a funcionalidade de bloqueio com as opções: pass, drop;
1.10.6. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
1.10.7. Deverá ter a capacidade de análise de tráfego para a detecção e bloqueio de anomalias, tais como Denial of Service (DoS);
1.10.8. Deverá possuir possibilidade de habilitar o IPS, para analisar no mínimo, os protocolos padrões de rede (SMTP, IMAP, POP, DNS, FTP, SSH , Telnet e rlogin, e ICMP);
1.10.9. Deve possuir notificação de detecção de ataques através de alarmes na console de administração e alertas via correio eletrônico.
1.10.10. 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;
1.10.11. Deverá possuir alerta via correio eletrônico;
1.10.12. Deverá possuir alarmes na console de administração;
1.10.13. Deverá possuir métodos de notificação de detecção de ataques;
1.10.14. Deverá prover a terminação de sessões via TCP resets;
1.10.15. Deverá armazenar os logs de sessões;
1.10.16. Deverá mitigar os efeitos dos ataques de negação de serviços;
1.10.17. Deverá possuir filtros de ataques por anomalias;
1.10.18. Deverá permitir filtros de anomalias de protocolos;
1.10.19. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
1.10.20. Deverá suportar verificação de ataque na camada de aplicação;
1.10.21. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset;

1.11. Deverá atender, no mínimo, os seguintes recursos de VPN:

1.11.1. Suporte a VPNs IPSEC nos modos site-to-site, e client-to-site;
1.11.2. Suporte aos algoritmos de criptografia AES, DES, 3DES;
1.11.3. Possibilitar mecanismo de criação de VPNs entre máquinas Windows Server 2016, 2019, Windows 10 e 11, e o dispositivo, com chaves de criptografia simétricas com tamanho igual ou superior a 128 bits;
1.11.4. Funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs das redes internas, colocando-os, virtualmente, dentro das mesmas;
1.11.5. Prover cliente VPN para as plataformas Windows Server 2016 e 2019, Windows 11 e 10, Mac OS X que permita uso de chaves criptográficas simétricas com 128 ou mais bits. Deve estar licenciada para todos esses clientes;
1.11.6. A VPN SSL deve possibilitar o acesso a toda infraestrutura da área contratante, de acordo com a política de segurança;
1.11.7. Deve suportar Auto-Discovery Virtual Private Network (ADVPN);
1.11.8. Deve suportar agregação de túneis IPSec;
1.11.9. Deverá trabalhar, no mínimo, com os protocolos: IPSEC, SSL e L2TP;

1.12. Deverá atender, no mínimo, os seguintes recursos para Controle de aplicação:

1.12.1. Deverá permitir integração com Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
1.12.2. Reconhecer pelo menos 2000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
1.12.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
1.12.4. Deverá possuir, pelo menos, 10 categorias para classificação de aplicações;
1.12.5. Deverá efetuar a monitoração do tráfego de aplicações, com opção de bloqueio de acesso dos usuários;
1.12.6. Deverá controlar as aplicações através do comportamento de tráfego, independente do protocolo e porta utilizados;
1.12.7. Deverá permitir identificação transparente de usuários cadastrados no Microsoft Active Directory;
1.12.8. Deverá efetuar a inspeção/bloqueio de códigos maliciosos para, no mínimo, as categorias de aplicações Instant Messaging e transferência de arquivos;
1.12.9. Deverá efetuar atualizações regulares do produto, de forma que seja sem interromper a execução dos serviços da solução;
1.12.10. Permitir criação de padrões de aplicação manualmente;
1.12.11. Permitir a criação de regras para acesso/bloqueio por categorias, no mínimo, por grupos de usuários do Microsoft Active Directory, por endereço IP de origem/destino, e por sub-rede de origem/destino.

1.13. Deverá atender, no mínimo, os seguintes recursos de Controle de Identificação de usuários:

1.13.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações e URL's através da integração com serviços de diretório, Active Directory, LDAP e Radius;
1.13.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

1.13.3. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular;
1.13.4. Deverá possibilitar a integração com Aruba Clear Pass;
1.13.5. A solução deverá ser capaz de identificar nome do usuário, login, maquina/computador registrados no Microsoft Active Directory;
1.13.6. Deve suportar autenticação Kerberos transparente para single sign on;
1.13.7. Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

1.14. Deverá atender, no mínimo, os seguintes recursos de Prevenção de Ameaças do tipo "0-Day":
1.14.1. A solução deve oferecer suporte para adicionar recursos de detecção de malware avançado;
1.14.2. A solução deve oferecer suporte para emulação completa de sistema para detectar malware avançado durante o tempo da execução;
1.14.3. A solução deve incluir uma lista sumário de indicadores de ameaças que informam porque o arquivo foi bloqueado como malware.

1.15. Deve atender, no mínimo, os seguintes recursos de SD-WAN:
1.15.1. Deve implementar balanceamento de link por hash do IP de origem;
1.15.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
1.15.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
1.15.4. Deve implementar balanceamento de link por custo configurado do link;
1.15.5. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;
1.15.6. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
1.15.7. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde.
1.15.8. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;

1.16. Deverá possuir as seguintes certificações:
1.16.1. Certificação Wi-Fi Alliance;
1.16.2. Certificação ICSA para Firewall;
1.16.3. Certificação ICSA para VPN SSL;
1.16.4. Certificação ICSA para VPN IPSec;
1.16.5. Certificação ICSA para IPS;

1.17. A solução deverá contar com uma plataforma de gerenciamento e armazenamento de log baseado em nuvem, devidamente licenciada, que atenda aos seguintes requisitos mínimos:
1.17.1. A solução deverá permitir o gerenciamento centralizado do dispositivo de segurança diretamente pela nuvem, incluindo a possibilidade de visualizar logs, aplicar políticas, monitorar eventos e executar tarefas administrativas remotamente.
1.17.2. A plataforma deverá oferecer armazenamento seguro de logs dos eventos de segurança e rede, com visualização por dashboards, relatórios e consultas detalhadas, mantendo no mínimo 365 dias de retenção de dados.
1.17.3. A plataforma deverá permitir a atualização de firmware do equipamento diretamente pela interface de gerenciamento em nuvem, sem necessidade de acesso físico ao equipamento ou download local de firmware.

1.17.4. A solução deverá prover mecanismos de alertas automáticos para incidentes de segurança, falhas operacionais e eventos relevantes, com classificação de severidade e capacidade de drill-down para análise detalhada.

1.17.5. A plataforma de gestão deverá suportar autenticação multifator para os administradores e permitir a criação de diferentes perfis de acesso com controle granular de permissões.

1.18. Deverá disponibilizar, obrigatoriamente, cobertura de substituição de hardware com SLA de até 4 (quatro) horas a partir da confirmação técnica do defeito por parte do fabricante. O serviço deverá contemplar:

1.18.1. Diagnóstico técnico remoto imediato, realizado pelo suporte oficial do fabricante, para confirmação do defeito físico no equipamento;

1.18.2. Despacho do hardware de reposição em até 4 horas após a validação do problema;

1.18.3. Entrega prioritária (on-site), conforme a política vigente do fabricante;

1.18.4. Equipamento substituto idêntico ou equivalente, com mesmo modelo e funcionalidades compatíveis;

1.18.5. Cobertura ativa durante todo o período contratual, com garantia de disponibilidade do serviço em todos os dias úteis, dentro do horário comercial ou regime 24x7;

1.19. O(s) equipamento(s) deve(m) possuir, no mínimo, as seguintes características de desempenho:

1.19.1. Suportar 11 milhões de conexões simultâneas;

1.19.2. Suporte a, no mínimo, 39 Mpps;

1.19.3. Suporte a, no mínimo, 400 mil novas conexões por segundo;

1.19.4. Estar licenciado para, ou suportar sem o uso de licença, pelo menos 10.000 conexões VPN IPSEC client-to-server simultaneamente;

1.19.5. Suportar 2.000 acessos de usuários simultâneos;

1.19.6. Capacidade de inspeção SSL de 07 Gbps;

1.19.7. Capacidade de processamento de Firewall de 35 Gbps;

1.19.8. Capacidade de processamento de IPS de 9 Gbps;

1.19.9. Capacidade de processamento de VPN IPSEC de 35 Gbps;

1.19.10. Capacidade de processamento de VPN SSL de 03 Gbps;

1.19.11. Estar licenciado para, ou suportar sem o uso de licença, pelo menos 500 clientes de VPN SSL simultâneos;

1.19.12. Possuir ao menos 10 interfaces 1Gbps RJ45;

1.19.13. Possuir ao menos 04 interfaces 1Gbps SFP;

1.19.14. Possuir ao menos 08 interfaces 10Gbps SFP+;

1.19.15. Possuir ao menos 08 interfaces 5Gbps RJ45;

1.19.16. Possuir ao menos 01 interface 1Gbps RJ45 dedicada à gerenciamento;

1.19.17. Possuir ao menos 01 interface serial de console;

1.19.18. Possuir ao menos 01 portas USB;

1.19.19. Possuir ao menos 01 interfaces 1Gbps RJ45 dedicadas à HA (Alta Disponibilidade);

1.19.20. O modelo de referência utilizado: Fortinet, FortiGate modelo 200G Series.

1.19.21. Poderá vir Firewall de outros fabricantes, que atendam todas as especificações.

1.20. Deverá ser fornecido junto à proposta o catalogo técnico com todas as especificações para análise do setor técnico do UniFACEF.

1.21. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.

1.22. O prazo de vigência da contratação é de 01 (um) ano contados da assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.22.1. A classificação orçamentária poderá ser alterada nos eventuais aditivos, devido a natureza contratual. Será renovado apenas os serviços prestados.

1.23. O serviço é enquadrado como continuado tendo em vista que o Estudo Técnico Preliminar.

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

1.25. GARANTIA

1.25.1. O equipamento de hardware deverá possuir garantia mínima de 36 (trinta e seis) meses contra defeitos de fabricação, cobrindo peças e mão de obra, contados a partir da data de aceite definitivo da solução.

1.26. CONDIÇÕES DE ENTREGA

1.26.1. Os equipamentos deverão ser entregues no endereço do Centro Universitário Municipal de Franca – Uni-FACEF, em perfeitas condições de uso, no prazo máximo de 10 dias corridos a partir da assinatura do contrato.

1.27. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.

1.28. O prazo de vigência da contratação é de 01 ano contado do(a) entrega, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

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

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual de 2025, conforme consta das informações básicas deste termo de referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

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

4. REQUISITOS DA CONTRATAÇÃO

4.1. Subcontratação

4.1.1. Não é admitida a subcontratação do objeto contratual.

4.2. Garantia da contratação

4.2.1. 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.

4.3. Vistoria

4.3.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Condições de execução

5.1.1. **A execução do objeto seguirá a seguinte dinâmica:**

5.1.1.1. Início da execução do objeto: até 10 (dez) dias da assinatura do contrato;
5.1.1.2. Todos os serviços baseados em assinaturas e atualizações devem estar disponíveis por, no mínimo, 12 (doze) meses, sem qualquer ônus adicional, conforme Anexo I do Edital e nos termos da proposta apresentada.

5.2. Local e horário da prestação dos serviços

5.2.1. O serviço deverá ser prestado no Centro Universitário Municipal de Franca, Unidade II – Sala Tecnologia da Informação – A/C Alessandro/Daniel (Sala 206), localizada em Avenida Ismael Alonso y Alonso, nº 2400 – Bairro São José – Franca/SP, CEP 14.403-430.Os serviços serão prestados no seguinte horário: das 9h00 às 16h00.

6. MODELO DE GESTÃO DO CONTRATO

6.1. 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.
6.2. 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.
6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

7. FISCALIZAÇÃO

7.1. 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).

7.2. Fiscalização Técnica

7.2.1. O fiscal técnico do contrato 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);
7.2.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);
7.2.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);
7.2.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

7.2.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

7.2.6. 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 à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.3. Fiscalização Administrativa

7.3.1. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, 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).

7.3.2. 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).

7.4. Gestor do Contrato

7.4.1. O gestor do contrato 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).

7.4.2. 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).

7.4.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, 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).

7.4.4. 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).

7.4.5. 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).

7.4.6. 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).

7.4.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto será realizada aferição da qualidade da prestação dos serviços e ainda conforme abaixo:

8.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

8.1.1.1. não produzir os resultados acordados,

8.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

8.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade

8.2. Do recebimento

8.2.1. Os serviços serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133, de 2021 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

8.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.2.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

8.2.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022).

8.2.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.2.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.2.7. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

8.2.8. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.2.9. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

8.2.10. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.2.11. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.2.12. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.3. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.3.1.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

8.3.1.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

8.3.1.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.3.1.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.3.1.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.3.1.6. 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 pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.3.1.7. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.3.1.8. 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.

8.4. Liquidação

8.4.1. 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.

8.4.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos 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

8.4.3. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

- o prazo de validade;
- o prazo de validade;
- a data da emissão;
- os dados do contrato e do órgão contratante;
- o período respectivo de execução do contrato;
- o valor a pagar; e
- eventual destaque do valor de retenções tributárias cabíveis.

8.4.4. Havendo erro na apresentação da Nota Fiscal/Fatura, 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 à contratante;

8.4.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada 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 14.133/2021.

8.4.6. 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, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

8.4.7. 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.

8.4.8. 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.

8.4.9. 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.

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

8.5. Prazo de pagamento

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

8.5.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA/IBGE de correção monetária.

8.6. Forma de pagamento

8.6.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

8.6.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.6.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

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

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

9.1.2. Será necessário que a empresa arrematante envie o catalogo técnico com todas as especificações do equipamento e serviços prestados.

9.2. Regime de execução

9.2.1. O regime de execução do contrato será a empreitada por preço global.

9.3. Exigências de habilitação

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

9.3.1.1. Habilitação jurídica

- 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;
- Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
- 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;
- Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;
- Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.
- Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

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

9.3.1.2. Habilitação fiscal, social e trabalhista

- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
- Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
- Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;
- Prova de inscrição no cadastro de contribuintes Estadual/Distrital ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- Prova de regularidade com a Fazenda Estadual/Distrital ou Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
- O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.3.1.3. Qualificação Econômico-Financeira

- certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;
- certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

10. DEMONSTRAÇÃO

10.1. Não será necessário que a empresa proponente faça a demonstração para validação.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é **de R$ 189.911,40,** conforme custos unitários apostos na tabela abaixo:

11.1.1. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre contratante e contratado, conforme especificado na matriz de risco constante do processo em questão.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Uni-FACEF.

12.2. A contratação será atendida pela seguinte dotação:

- Item Despesa: 44905200 - EQUIPAMENTOS E MATERIAL PERMANENTE
- Unidade: 030101 - CENTRO UNIVERSITÁRIO DE FRANCA
- Programa de Governo: 3001 GESTÃO DAS AÇÕES DO ENSINO SUPERIOR UNI-FACEF
- Ação Governamental: 1302 MÓVEIS, MÁQUINAS, EQUIP. E OBRAS LITERÁRIAS

12.3. Para eventuais aditivos, a classificação orçamentária será na ficha de Serviços de Tecnologia da Informação e Comunicação.

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

Franca, 30 de junho de 2025.

DANIEL FACCIOLO PIRES:19631896803

Assinado de forma digital por DANIEL FACCIOLO PIRES:19631896803
Dados: 2025.07.02 16:23:44 -03'00'

Prof. Dr. Daniel Facciolo Pires