# 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. A contratação visa a aquisição de equipamento que garanta a proteção robusta e de alto desempenho da infraestrutura de rede, nos termos abaixo, conforme condições e exigências estabelecidas neste instrumento.

1.1.1 Esta abordagem de contratação de uma "solução completa" é fundamental para garantir a operacionalidade contínua e a segurança eficaz ao longo de todo o ciclo de vida do contrato. A inclusão de hardware, licenciamento de software abrangente e suporte técnico direto do fabricante para a resolução de quaisquer problemas, desde falhas de hardware até a necessidade de atualizações de segurança críticas.

1.1.2 Os bens objetos desta contratação são caracterizados como comuns, uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, conforme detalhado neste Termo de Referência. Esta caracterização está em plena conformidade com as diretrizes estabelecidas no Art. 6º, inciso XIII, da Lei nº 14.133, de 1º de abril de 2021. A definição do *NGFW* como um bem comum, cujas especificações são mensuráveis e comparáveis entre diferentes fornecedores de mercado, fundamenta a escolha da modalidade licitatória de pregão, promovendo a ampla competição e a busca pela proposta mais vantajosa para a Administração Pública, sem restringir indevidamente a participação de potenciais licitantes que atendam aos critérios técnicos aqui estabelecidos.

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:

1.2.1 O equipamento deve ser novo e sem histórico de uso anterior;

1.2.2 O equipamento deve estar em produção atual, ou seja, não pode ser obsoleto ou descontinuado;

1.2.3 É fundamental que o dispositivo não esteja próximo da data de fim de suporte oficial do fabricante, garantindo sua viabilidade e suporte a longo prazo;

1.2.4 Na proposta deverá ser fornecido a marca e o modelo do equipamento para fins de identificação das funcionalidades;

1.2.5 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;

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

1.2.7 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;

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

1.2.9 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;

1.2.10 Identificar o uso de táticas evasivas via comunicações criptografadas;

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

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

1.2.13 Deverá possuir fontes de alimentação AC duplas e redundantes (configuração 1+1), permitindo a continuidade da operação em caso de falha de uma das fontes, para funcionamento em rede elétrica 110V e 220V. A fonte fornecida deve suportar a operação da unidade com todos os módulos de interface ativos;

1.2.14 Para garantir a flexibilidade de conexão e a capacidade de atender às demandas de alta velocidade da rede atual e futura, o appliance deverá possuir, no mínimo, a seguinte configuração de interfaces físicas, sejam elas fixas no chassi ou através de módulos de expansão *(Network Modules, Flexi Ports, etc.)* já inclusos na proposta:

1.2.14.1 Mínimo de 12 (doze) portas 1 Gbps (em qualquer combinação de RJ45 ou SFP);

1.2.14.2 Mínimo de 8 (oito) portas Multi-Gigabit (com suporte nativo a, no mínimo, 2.5 Gbps e 5 Gbps);

1.2.14.3 Mínimo de 8 (oito) portas 10 Gbps SFP+;

1.2.15 Armazenamento Interno: Deverá possuir, no mínimo, 480 GB de armazenamento interno em disco de estado sólido (SSD) para funções como armazenamento de logs locais, geração de relatórios, quarentena de arquivos e otimização de WAN. O uso de SSD é mandatório para garantir o alto desempenho de operações de leitura/escrita intensivas.

1.2.16 Módulo de Segurança de Hardware: Deverá ser equipado com um módulo de *hardware* do tipo *Trusted Platform Module (TPM),* que permita a geração, o armazenamento e a autenticação segura de chaves criptográficas, garantindo a integridade do *firmware* e do sistema operacional do *appliance* contra adulterações.

1.2.17 Para garantir maior segurança, não serão aceitos computadores (PCs) com instalação de sistemas operacionais tradicionais do mercado, tais como Microsoft Windows, FreeBSD, Solaris, AIX ou GNU/Linux;

1.2.18 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;

1.2.19 Deverá, como requisito de desempenho de proteção contra ameaças *(Threat Protection Performance Requirement)*, capacidade da solução de segurança de manter um alto desempenho na rede, mesmo quando a proteção total contra ameaças está ativada.

1.2.20 Deverá ser fornecido documentação técnica do equipamento proposto, contemplando manual de usuário de utilização do equipamento, podendo ser em idioma português e/ou inglês;

1.2.21 Deverão ser fornecidas as licenças para todas as funcionalidades solicitadas neste termo de referência, pelo período de validade do contrato;

1.2.22 O equipamento deverá ser entregue em até 60 dias corridos após a assinatura do contrato.

1.3 A plataforma de segurança deverá possuir as funcionalidades:

1.3.1 Deverá suportar, no mínimo, 3 milhões de sessões simultâneas e taxa de 200.000 novas conexões por segundo;

1.3.2 Inspeção de Tráfego e Controle de Aplicações: A solução deverá ser capaz de identificar e controlar o tráfego de, no mínimo, 3.000 aplicações distintas, incluindo sub-aplicações (ex: Facebook Chat vs. Facebook Video). Essa identificação deve ocorrer independentemente da porta ou protocolo utilizado e deve ser eficaz mesmo contra técnicas de evasão, como o uso de proxies ou encapsulamento de tráfego. O sistema deverá permitir a criação de políticas de segurança granulares baseadas em múltiplos critérios, como identidade de usuário ou grupo (integrado a serviços de diretório como *Active Directory*), aplicação, categoria de aplicação e nível de risco da aplicação.

1.3.3 Prevenção de Intrusão (IPS): Deverá possuir um sistema de prevenção de intrusão (IPS) robusto, com um banco de dados de, no mínimo, 18.000 assinaturas para a detecção e bloqueio de *exploits*, *malwares* e outras atividades maliciosas. O fabricante deverá prover atualizações automáticas e contínuas para esta base de assinaturas. Adicionalmente, o sistema de IPS deverá suportar a funcionalidade de "*virtual patching*", que consiste na aplicação de regras de proteção específicas para vulnerabilidades recém-descobertas, permitindo que os administradores de sistema protejam servidores e aplicações críticas antes que um patch de correção oficial possa ser testado e implantado.

1.3.4 Proteção Avançada Contra *Malware*: A solução deverá prover uma defesa em múltiplas camadas contra *malware*, integrando diferentes tecnologias para maximizar a eficácia da detecção e bloqueio. Os seguintes componentes são obrigatórios:

1.3.4.1 Antivírus de *Gateway*: Proteção baseada em assinaturas para a detecção de vírus, *spyware*, e outros *malwares* conhecidos que transitam pela rede;

1.3.4.2 Detecção Heurística e Baseada em IA/ML: Capacidade de analisar arquivos e tráfego em tempo real utilizando técnicas de análise heurística e modelos de Inteligência Artificial/Machine Learning para identificar e bloquear ameaças desconhecidas e de dia zero (*zero-day*);

1.3.4.3 Dever possuir recurso de depuração de pacotes enviado/recebidos, similar ao comando tcpdump;

1.3.4.4 Suporte a políticas seletiva com base em parâmetros específicos, como endereço IP de origem e destino, porta de origem ou destino, tipo de tráfego, protocolos, lista de acesso, tamanho de pacotes ou outros critérios *(PBR - Policy Based Routing)*;

1.3.4.5 Integração com *Sandboxing*: A solução deverá se integrar nativamente com um serviço de *sandboxing* (em nuvem ou *on-premises*) do mesmo fabricante. Arquivos suspeitos que não sejam identificados pelas outras camadas de defesa deverão ser automaticamente enviados para este ambiente isolado para execução e análise de comportamento, permitindo a descoberta de malwares avançados e evasivos.

1.3.5 Filtragem *Web* e *DNS*: Deverá prover serviços abrangentes de filtragem de *URL*, *DNS* e conteúdo de vídeo. A solução deve utilizar uma base de dados global, categorizada e continuamente atualizada pelo fabricante, para classificar e controlar o acesso a *websites*. Deverá ser capaz de bloquear o acesso a sites conhecidos por hospedar *malware*, *phishing*, e que atuem como servidores de comando e controle (C&C) de *botnets*. Além disso, deverá permitir a aplicação de políticas de uso aceitável, restringindo o acesso a categorias de sites e a URLs específicas,

1.3.6 conforme políticas da instituição (ex: redes sociais, jogos, conteúdo adulto) conforme as políticas do órgão;

1.3.7 Prover mecanismo contra-ataques de falsificação de endereços (anti-spoofing);

1.3.8 Controle de acesso à internet por períodos do dia (horários e dia da semana);

1.3.9 Inspeção de Tráfego Criptografado: Considerando que a vasta maioria do tráfego de Internet hoje é criptografada, a solução deverá ser capaz de realizar a inspeção profunda (decriptação e re-criptografia) de tráfego SSL/TLS, incluindo o suporte obrigatório ao protocolo TLS 1.3. Esta funcionalidade é crítica para garantir que todas as outras camadas de segurança (IPS, Antivírus, Controle de Aplicações, DLP) possam inspecionar o conteúdo do tráfego que, de outra forma, passaria sem análise pela rede. A capacidade de inspecionar TLS 1.3, combinada com a exigência de um *throughput* mínimo de 7 Gbps para esta função, constitui um teste rigoroso da capacidade de processamento da arquitetura de hardware da solução ofertada.

1.4 Funcionalidades de Conectividade Segura e Acesso

1.4.1 *SD-WAN* Seguro (*Secure SD-WAN*): A funcionalidade de *SD-WAN* (*Software-Defined Wide Area Network*) deverá ser um recurso nativo do sistema operacional do *appliance*, sem a necessidade de licenciamento adicional ou de hardware externo. A solução deverá permitir a gestão inteligente e segura de múltiplas conexões de *WAN* (ex: links *MPLS*, Internet de banda larga, 4G/5G), oferecendo, no mínimo, as seguintes capacidades:

1.4.2 Suporte aos protocolos *NetFlow* ou *sFlow* para coletar metadados sobre o tráfego IP, permitindo que os administradores monitorem o desempenho da rede, identificando problemas e otimizando a largura de banda.

1.4.2.1 Gerenciamento Centralizado: Orquestração e provisionamento centralizado das políticas de rede e segurança para todas as localidades conectadas;

1.4.2.2 Seleção Dinâmica de Caminhos: Capacidade de monitorar em tempo real a qualidade dos links de *WAN* (medindo latência, *jitter* e perda de pacotes) e de rotear dinamicamente o tráfego de aplicações pelo caminho de melhor desempenho;

1.4.2.3 Segurança Integrada: Aplicação consistente de todo o conjunto de funcionalidades de segurança do *NGFW* (*IPS, AV, App Control* etc.) a todo o tráfego que atravessa a malha *SD-WAN.*

1.4.3 Acesso à Rede Zero *Trust (Universal ZTNA*): A solução deverá incorporar, de forma nativa em seu sistema operacional, a funcionalidade de *gateway* de aplicação *ZTNA (Zero-Trust Network Access)*. Este recurso deve substituir o acesso VPN tradicional por um modelo de acesso mais seguro e granular, no qual a confiança nunca é implícita. O *gateway ZTNA* deverá ser capaz de:

1.4.3.1 Verificação Contínua: Controlar o acesso a aplicações específicas, verificando a identidade do usuário e a postura de segurança do dispositivo (ex: versão do SO, antivírus ativo) a cada tentativa de conexão;

1.4.3.2 Acesso Mínimo Privilegiado: Conceder acesso apenas à aplicação solicitada, e não à rede inteira, reduzindo drasticamente a superfície de ataque e prevenindo o movimento lateral de ameaças;

1.4.3.3 Acesso sem Cliente (*Agentless*): Suportar um modo de acesso sem a necessidade de instalação de cliente de software no dispositivo do usuário, através de um portal *web* que atue como um *proxy* reverso. Esta modalidade é essencial para facilitar o acesso de usuários convidados, parceiros e funcionários utilizando dispositivos não gerenciados (*BYOD*).

1.4.4 Segmentação de Rede Dinâmica: Para conter a propagação de ameaças dentro da rede interna (movimento lateral), o *appliance* deverá suportar a criação de segmentos de rede lógicos e dinâmicos. Esta segmentação deve ir além das *VLANs* tradicionais, oferecendo a capacidade de isolar o tráfego com base em critérios de identidade, tipo de dispositivo ou função de negócio. A solução deverá suportar, no mínimo, a tecnologia de encapsulamento *VXLAN* para estender a segmentação de forma escalável através de domínios de rede físicos e virtuais, aplicando políticas de firewall de Camada 4 entre os diferentes segmentos.

1.4.5 Filtro de pacotes sem controle de estado *(stateless)*, permitindo que o servidor mantenha o contexto de transações anteriores, verificação em camada 2;

1.4.6 Possibilitar criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (tablets, celulares e PCs);

1.4.7 Detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas

1.5 Requisitos de gerência:

1.5.1 A solução deverá prover uma interface de gerenciamento web segura (HTTPS) local, que seja intuitiva e completa, além de uma interface de linha de comando (CLI) acessível via protocolo seguro (SSH).

1.5.2 Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

1.5.3 O gerenciamento Web deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

1.5.4 Deve suportar a criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.5.5 Deve suportar backup automático das configurações e rollback de configuração para a última configuração salva;

1.5.6 Permitir a visualização dos logs de uma regra especial em tempo real;

1.6 Autenticação de usuários:

1.6.1 Integração com Microsoft Active Directory para autenticação de usuários;

1.6.2 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;

1.6.3 Deverá suportar Single-sign-on para Microsoft Active Directory;

1.6.4 A solução deverá ser capaz de identificar nome do usuário, login, maquina/computador registrados no Microsoft Active Directory;

1.6.5 Deve suportar autenticação Kerberos transparente para single sign on;

1.6.6 Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

1.6.7 possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.7 Certificações de Segurança Obrigatórias

A comprovação da qualidade, eficácia de segurança e robustez do design de um produto de cibersegurança não pode se basear unicamente nas alegações do fabricante. Portanto, a solução ofertada (combinação específica de modelo de hardware e versão do sistema operacional) deverá possuir, obrigatoriamente, todas as certificações listadas abaixo. Estas certificações devem estar válidas no momento da apresentação da proposta e devem ter sido emitidas por laboratórios de teste independentes e reconhecidos internacionalmente. A comprovação será realizada mediante a apresentação dos certificados ou de links diretos e públicos para os registros nos sites das respectivas entidades certificadoras. A exigência deste conjunto de certificações estabelece um patamar mínimo de qualidade e confiabilidade, garantindo que apenas soluções de classe empresarial, submetidas a rigorosos processos de validação externa, sejam consideradas.

1.7.1 *ICSA Labs Firewall – Corporate*: O produto deverá possuir a certificação *ICSA Labs* na categoria *"Firewall"*, tendo sido testado com sucesso contra os critérios do *"Corporate Module"* (versão 4.2 ou superior). Esta certificação valida que o produto cumpre com os requisitos fundamentais de um *firewall* de nível corporativo, incluindo a correta aplicação de políticas de segurança, *logging* robusto, funcionalidades de administração segura e resistência a técnicas de ataque conhecidas. É um selo de qualidade amplamente reconhecido no mercado que atesta a funcionalidade básica e a segurança do produto.

1.7.2 *Common Criteria for Information Technology Security Evaluation - EAL4+*: O produto (hardware e sistema operacional) deverá possuir a certificação *Common Criteria* no nível de garantia *EAL4+ (Evaluation Assurance Level 4 augmented)*, em conformidade com o padrão internacional *ISO/IEC* 15408. O nível *EAL4* significa que o produto foi "Metodicamente Projetado, Testado e Revisado". A designação "+" (*augmented*) indica que o produto foi avaliado contra requisitos de garantia adicionais, que vão além do padrão EAL4, demonstrando um nível ainda maior de rigor. Esta certificação é um dos qualificadores técnicos mais importantes deste termo de referência. Diferente de testes que focam apenas na funcionalidade, a certificação EAL4+ envolve uma análise profunda e metódica de todo o ciclo de vida de desenvolvimento do produto, incluindo a documentação de design, os processos de desenvolvimento seguro do fabricante, a análise de vulnerabilidades e os

procedimentos de remediação de falhas. A obtenção desta certificação é um processo longo e oneroso, que apenas os fabricantes mais maduros e comprometidos com a segurança se submetem. Portanto, ela serve como um indicador objetivo e legalmente defensável da confiabilidade e da robustez da engenharia do produto, sendo um requisito comum para aquisições em ambientes governamentais e de alta segurança.

1.7.3 *FIPS 140-2 ou FIPS 140-3*: Os módulos criptográficos utilizados pela solução para todas as suas funções (VPN, gerenciamento HTTPS/SSH, integridade do sistema etc.) deverão possuir a certificação *FIPS 140-2* ou sua sucessora, *FIPS 140-3*, no Nível 1 ou superior. Esta certificação é emitida pelo *National Institute of Standards and Technology (NIST)* e é o padrão de fato para validar que os algoritmos de criptografia e sua implementação em um produto de segurança são corretos, seguros e não possuem falhas conhecidas. A conformidade com o padrão FIPS é um requisito não negociável para qualquer solução que lide com a proteção de informações sensíveis.

1.7.4 *USGv6 / IPv6 Ready Logo*: Com a transição global para o protocolo IPv6, é fundamental que a solução de segurança de perímetro seja totalmente compatível e otimizada para operar em redes que utilizam este protocolo. Para comprovar esta capacidade, a solução deverá possuir a certificação do programa de testes *USGv6* do *NIST* ou o selo "*IPv6 Ready Logo Phase 2*". Estas certificações garantem que o produto implementa corretamente as funcionalidades do IPv6, incluindo as de segurança, e que foi submetido a um conjunto rigoroso de testes de conformidade e interoperabilidade.

1.8 Qualificação do Fabricante

1.8.1 Para garantir a aquisição de uma solução de classe empresarial com comprovada capacidade de inovação, suporte global e eficácia na detecção de ameaças, o fabricante da solução de *Next Generation Firewall (NGFW)* ofertada deverá, obrigatoriamente, estar posicionado no quadrante "Líderes" *(Leaders)* do relatório *Gartner® Magic Quadrant™ for Network Firewalls* (ou seu sucessor) mais recente, publicado no ano corrente ou no ano anterior ao da realização desta licitação.

1.8.1.1 A comprovação deverá ser feita mediante apresentação de cópia do relatório ou link público para a documentação oficial do instituto de pesquisa."

1.9 Deverá atender, no mínimo, os seguintes recursos de Traffic Shaping e Priorização:

1.9.1 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;

1.9.2 Limitar individualmente a banda utilizada por aplicações (por exemplo, peer-to-peer, streaming, chat, VoIP, web, etc.);

1.9.3 Identificação transparente de usuários cadastrados no Microsoft Active Directory;

1.9.4 Definir a banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo ou aplicação;

1.9.5 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.

1.10 Deverá atender, no mínimo, os seguintes recursos de Controle de aplicações Web e Filtro de conteúdo Web:

1.10.1 O recurso de filtro de conteúdo web deverá estar integrado na solução de segurança;

1.10.2 Deverá suportar integração com Microsoft Active Directory;

1.10.3 Identificação transparente de usuários do Microsoft Active Directory;

1.10.4 Filtro de conteúdo baseado em categorias;

1.10.5 Deverá categorizar a página web, tanto pela sua URL, como pelo endereço IP;

1.10.6 Dispor de pelo menos 50 categorias para classificação de sites web;

1.10.7 Dispor de base de dados com, no mínimo, 200 milhões URLs;

1.10.8 Deverá suportar monitoramento do tráfego internet, com opção de bloqueio de acesso aos usuários;

1.10.9 Deverá possibilitar a criação de categorias personalizadas;

1.10.10 Deverá permitir a reclassificação de sites web;

1.10.11 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;

1.10.12 Bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

1.10.13 Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

1.10.14 Deverá efetuar atualizações regulares do produto sem interromper a execução dos serviços de filtragem de conteúdo web;

1.10.15 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.

1.10.16 Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

1.10.17 Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

1.10.18 Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

1.10.19 Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

1.10.20 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;

1.10.21 Deverá atender, no mínimo, os seguintes recursos de Proxy Web Transparante/Explicíto e Proxy Reverso:

1.10.22 Deverá funcionar em modo Proxy Explícito para HTTP e HTTPS, e em Proxy Transparente para HTTP;

1.10.23 Deverá permitir configuração da porta do Proxy Explícito;

1.10.24 Deverá suportar a funcionalidade através de Proxy Reverso para redirecionamento de URLs do tipo http ou https redirecionando para o servidor específico;

1.11 Deverá atender, no mínimo, os seguintes recursos de Detecção e Prevenção de Intrusão (IDS/IPS):

1.11.1 Deverá efetuar a inspeção de tráfego por regra baseada em IP origem/destino, por protocolo, ou por porta (TCP/UDP);

1.11.2 Deverá possuir base de assinaturas de IPS com pelo menos 10.000 ameaças conhecidas;

1.11.3 Deverá efetuar a atualização automática de segurança e da base de assinaturas direto do fabricante;

1.11.4 Deverá permitir a criação de assinaturas personalizadas;

1.11.5 Deverá permitir a funcionalidade de bloqueio com as opções: pass, drop;

1.11.6 Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

1.11.7 Deverá ter a capacidade de análise de tráfego para a detecção e bloqueio de anomalias, tais como Denial of Service (DoS);

1.11.8 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);

1.11.9 Deve possuir notificação de detecção de ataques através de alarmes na console de administração e alertas via correio eletrônico;

1.11.10 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;

1.11.11 Deverá possuir alerta via correio eletrônico;

1.11.12 Deverá possuir alarmes na console de administração;

1.11.13 Deverá possuir métodos de notificação de detecção de ataques;

1.11.14 Deverá prover a terminação de sessões via TCP resets;

1.11.15 Deverá armazenar os logs de sessões;

1.11.16 Deverá mitigar os efeitos dos ataques de negação de serviços;

1.11.17 Deverá possuir filtros de ataques por anomalias;

1.11.18 Deverá permitir filtros de anomalias de protocolos;

1.11.19 Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

1.11.20 Deverá suportar verificação de ataque na camada de aplicação;

1.11.21 Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset;

1.12 Deverá atender, no mínimo, os seguintes recursos de VPN:

1.12.1 Suporte a VPNs IPSEC nos modos site-to-site, e client-to-site;

1.12.2 Suporte aos algoritmos de criptografia AES, DES, 3DES;

1.12.3 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;

1.12.4 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;

1.12.5 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;

1.12.6 A VPN SSL deve possibilitar o acesso a toda infraestrutura da área contratante, de acordo com a política de segurança;
1.12.7 Deve suportar Auto-Discovery Virtual Private Network (ADVPN);
1.12.8 Deve suportar agregação de túneis IPSec;
1.12.9 Deverá trabalhar, no mínimo, com os protocolos: IPSEC, SSL e L2TP;
1.13 Treinamento: Deverá ser oferecido treinamento hands-on de atualização tecnológica das soluções implantadas com o mínimo de 08 (oito) horas de duração, em dias úteis, para até 05 (cinco) funcionários da Uni-FACEF, com emissão de certificado. O treinamento deverá ser ministrado por profissional Certificado pelo fabricante na categoria Especialista conforme a classificação de cada fabricante;
1.14 Garantia e Suporte Tecnico:
1.14.1 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.
1.14.2 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:
1.14.2.1 Diagnóstico técnico remoto imediato, realizado pelo suporte oficial do fabricante, para confirmação do defeito físico no equipamento;
1.14.2.2 Despacho do hardware de reposição em até 4 horas após a validação do problema;
1.14.2.3 Entrega prioritária (on-site), conforme a política vigente do fabricante;
1.14.2.4 Equipamento substituto idêntico ou equivalente, com mesmo modelo e funcionalidades compatíveis;
1.14.2.5 Cobertura ativa durante todo o período contratual, com garantia de disponibilidade do serviço em todos os dias úteis, em regime 24x7, com resposta
1.14.2.6 em até 1 hora para incidentes críticos (Severity 1).
1.15 A solução deverá atender aos princípios e diretrizes da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), assegurando confidencialidade, integridade e rastreabilidade das informações trafegadas.
1.16 Condições de Entrega:
1.16.1 Os equipamentos deverão ser entregues no endereço do Centro Universitário Municipal de Franca – Uni-FACEF, em perfeitas condições de uso, no prazo máximo de 60 dias corridos a partir da assinatura do contrato;
1.16.2 O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns), conforme justificativa constante do Estudo Técnico Preliminar.
1.16.3 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.
1.17 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 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).

8.3.2 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;

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

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

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

8.3.6 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.

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

8.3.8 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;
- 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 catálogo 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 Será necessária demonstração ou teste de aceitação para validação das funcionalidades e desempenho da solução antes do aceite definitivo.

## 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, 29 de outubro de 2025.

DANIEL FACCIOLO PIRES:19631896803

Assinado de forma digital por DANIEL FACCIOLO PIRES:19631896803
Dados: 2025.10.31 09:03:03 -03'00'

Prof. Dr. Daniel Facciolo Pires

ALESSANDRO RODRIGUES DA SILVA:15982537861

Assinado de forma digital por ALESSANDRO RODRIGUES DA SILVA:15982537861
Dados: 2025.10.31 09:08:03 -03'00'

Alessandro Rodrigues da Silva

Oficial de Tecnologia e Informática