**TERMO DE REFERÊNCIA**

|  |
| --- |
| **UNIDADE SOLICITANTE: UTIC** |
| **RESPONSÁVEL PELA ELABORAÇÃO: Alisson de Souza Lima** |

|  |
| --- |
| 1. **OBJETO DA CONTRATAÇÃO:**   Contratação de serviço especializado para fornecimento de solução de segurança de Firewall de Nova Geração (Next Generation Firewall - NGFW), com funções de SD-WAN, IPS, VPN, antivírus, controle de aplicações, filtro de URL, QoS, load balance e alta disponibilidade, com todos os recursos (licenças) habilitados para as unidades regionais do Sebrae/RO. Contemplando todos os procedimentos necessários para entrega, bem como garantia, instalação, configuração e operação conforme condições, quantidades e exigências estabelecidas neste termo de referência. |

|  |
| --- |
| 1. **JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO:**   O Sebrae Rondônia conta atualmente com sete Unidades Regionais (URs) e um Ponto de Atendimento (PA), todos interligados à Sede por meio da tecnologia MPLS, com o objetivo de integrar as redes locais de computadores de forma segura e eficiente.  Com o compromisso de aprimorar continuamente suas soluções tecnológicas e a infraestrutura de TIC, a instituição busca garantir a entrega de serviços de qualidade as micro e pequenas empresas do estado de Rondônia. Nesse sentido, a adoção de uma solução de rede baseada em SD-WAN representa um avanço significativo na interligação das unidades, promovendo maior eficiência operacional em âmbito estadual.  A nova solução permitirá ganhos de desempenho no tráfego de dados, com melhor aproveitamento dos recursos computacionais e aumento na segurança da informação. Além disso, assegurará qualidade de serviço (QoS) nos circuitos, possibilitando a priorização do tráfego das aplicações críticas, como voz sobre IP (VoIP) e videoconferência.  Com isso, será possível garantir o desempenho adequado das aplicações de negócio, aliando qualidade, disponibilidade e otimização do uso da rede para os serviços essenciais ao funcionamento institucional. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **DETALHAMENTO/ESPECIFICAÇÃO DO OBJETO:**   3.1.Contratação de serviço especializado para fornecimento de solução de segurança de firewall de próxima geração (NGFW – Next Generation Firewall) para a unidades regionais do SEBRAE/RO. Contemplando todos os procedimentos necessários para entrega, bem como garantia, instalação, configuração e operação conforme condições, quantidades e exigências estabelecidas.   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | SOLUÇÃO DE SEGURANÇA DE FIREWALL | | | | |  | | ITEM | ESPECIFICAÇÃO | UNIDADE DE  MEDIDA | QTDE  (A) | PREÇO  MENSAL  (B) | PREÇO  TOTAL  MENSAL  C=BxA | PREÇO  TOTAL  Cx36 | | 01 | Contratação de serviço especializado para fornecimento de solução de segurança de firewall (NGFW/SD-WAN) (Appliance físico) para as agências regionais do SEBRAE/RO, bem como Serviço de instalação, ativação, configuração e operação dos equipamentos. | UN | 8 (appliances) | R$ | R$ | R$ | | 02 | Contratação de serviço especializado para fornecimento de solução de gerenciamento centralizado para os firewalls (NGFW/SD-WAN) para a sede do SEBRAE/RO. | UN | 8 (appliances gerenciados) | R$ | R$ | R$ | | 03 | Contratação de serviço especializado para armazenamento de LOG para NGFW/SD-WAN. | GB | 1 GB/dia  (armazenamento) | R$ | R$ | R$ |  * 1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, conforme o detalhamento a seguir:      1. Throughput de, no mínimo, 1 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;      2. Suporte a, no mínimo, 950 mil conexões simultâneas;      3. Suporte a, no mínimo, 10.000 novas conexões por segundo;      4. Throughput de, no mínimo, 450 Mbps de VPN IPSec;      5. Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;      6. Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de clientes VPN IPSEC simultâneos;      7. Suporte a no mínimo, 100 clientes de VPN SSL simultâneos;      8. Throughput de, no mínimo, 500 Mbps para funcionalidades de Proteção contra Ameaças;      9. Possuir ao menos 6 interfaces 1Gbps;      10. Possuir ao menos 1 Slots SFP Gigabit;      11. Os appliances fornecidos devem ser novos, de primeiro uso, e com licenciamento ativo durante toda a vigência do contrato;      12. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;      13. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;      14. As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;      15. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;      16. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada equipamento;      17. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;      18. A solução deve permitir o gerenciamento tanto via interface Web ou cliente, como também via SSH;      19. Os dispositivos de proteção de rede devem possuir suporte a Vlans;      20. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM- DM);      21. Deve suportar BGP, OSPF, RIP e roteamento estático;      22. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;      23. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;      24. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;      25. Deve suportar NAT dinâmico (Many-to-Many);      26. Deve suportar NAT estático (1-to-1);      27. Deve suportar Tradução de porta (PAT);      28. Deve suportar NAT de Origem;      29. Deve suportar NAT de Destino;      30. Deve suportar NAT de Origem e NAT de Destino simultaneamente;      31. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;      32. Enviar log para sistemas de monitoração externos;      33. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;      34. Deve permitir criar regras de automação, definindo ações para eventos previamente determinados;      35. Dentre as possibilidades para iniciar regras de automação, deve suportar webhooks, IOCs, logs pré-definidos e agendamento;      36. Como ação para as regras de automação, deve suportar: execução de scripts, envio de e- mails, webhooks e execução de lambda/functions;      37. Deve possuir conectores para diversas nuvens públicas e privadas, tais como: AWS, Azure, GCP, Vmware ESXi, NSX, ACI e OpenStack;      38. A solução deve oferecer capacidade de integração com ambientes de orquestração e controle de endpoints, podendo disponibilizar conectores nativos ou mecanismos de integração via API, webhooks ou serviços externos do fabricante, para Kubernetes, NAC e MDM/endpoint;      39. Deve suportar threat feeds, tais como: listas de hashes, Ips e nomes;      40. Proteção anti-spoofing;      41. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;      42. Deve suportar Modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;      43. Deve suportar Modo Camada 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;      44. A configuração deve sincronizar: sessões, configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;      45. Deve possuir suporte a criação de múltiplas instâncias de segurança virtual no mesmo appliance;      46. 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;      47. Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);      48. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.   2. CONTROLE DE POLÍTICAS:      1. Deverá suportar controles por zonas de segurança;      2. Deverá suportar controles de políticas por porta e protocolo;      3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;      4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;      5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);      6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);      7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2;      8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;      9. Suporte a objetos e regras IPV4 e IPV6;      10. Suporte a objetos e regras multicast;      11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.   3. CONTROLE DE APLICAÇÕES:      1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;      2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;      3. Reconhecer pelo menos 4500 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;      4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, tiktok,linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, face- book chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active direc- tory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;      5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;      6. 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;      7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;      8. 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;      9. Identificar o uso de táticas evasivas via comunicações criptografadas;      10. Atualizar a base de assinaturas de aplicações automaticamente;      11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;      12. A integração de com o Microsoft Active Directory para controle de aplicação deve acontecer nativamente via o appliances de firewalls, sem a necessidade de instalação de nenhum modulo apartado do appliance;      13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;      14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo me- nos checagem de assinaturas e decodificação de protocolos;      15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;      16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;      17. Deve alertar o usuário quando uma aplicação for bloqueada;      18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;      19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;      20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;      21. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;      22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol);      23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;      24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.   4. PREVENÇÃO DE AMEAÇAS:      1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;      2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);      3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;      4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;      5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;      6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;      7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;      8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;      9. Deve permitir o bloqueio de vulnerabilidades;      10. Deve permitir o bloqueio de exploits conhecidos;      11. Deve incluir proteção contra-ataques de negação de serviços;      12. Deverá possuir os seguintes mecanismos de inspeção de IPS:      13. Análise de padrões de estado de conexões;      14. Análise de decodificação de protocolo;      15. Análise para detecção de anomalias de protocolo;      16. Análise heurística;      17. IP Defragmentation;      18. Remontagem de pacotes de TCP;      19. Bloqueio de pacotes malformados.      20. Ser capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;      21. Detectar e bloquear a origem de portscans;      22. Bloquear ataques efetuados por worms conhecidos;      23. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;      24. Possuir assinaturas para bloqueio de ataques de buffer overflow;      25. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;      26. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;      27. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;      28. Identificar e bloquear comunicação com botnets;      29. Registrar na console de monitoração as seguintes informações sobre ameaças identifica- das: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;      30. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;      31. Os eventos devem identificar o país de onde partiu a ameaça;      32. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;      33. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;      34. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.      35. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;      36. A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;      37. A solução de sandbox deve ser capaz de identificar URLs maliciosas e adicioná-las automaticamente à blacklist do firewall, bloqueando novos acessos por usuários;      38. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;      39. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;   5. FILTRO DE URLS:      1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);      2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;      3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;      4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;      5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;      6. Suportar proxy explícito;      7. Suportar a criação de limites diários de tempo e banda consumida por categoria;      8. Possuir pelo menos 60 categorias de URLs;      9. Deve possuir a função de exclusão de URLs do bloqueio;      10. Permitir a customização de página de bloqueio.   6. ANÁLISE DE MALWARES MODERNOS:      1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;      2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;      3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;      4. Deve possuir mecanismo de análise de arquivos capaz de classificá-los ao menos em três grupos distintos, como: arquivos maliciosos (com comportamento ou assinatura de ameaça conhecida), arquivos seguros (sem evidência de risco), e arquivos potencialmente indesejados ou com comportamento anômalo, como os que possam impactar negativamente a performance do sistema ou modificar parâmetros sem consentimento do usuário;      5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;      6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10 (32 bits) e (64 bits);      7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;      8. A solução deve possuir a capacidade de analisar em sandbox links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sandbox o identifique como site hospedeiro de exploits;      9. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;      10. O sistema de análise “In Cloud” ou local deve prover informações sobre ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);      11. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;      12. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;      13. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;      14. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;      15. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.      16. A solução deve oferecer funcionalidade de análise de malwares não conhecidos (sandbox), podendo ser disponibilizada em formato de appliance físico, máquina virtual ou **serviço em nuvem homologado pelo fabricante**, desde que: a) ofereça nível equivalente de proteção; b) respeite a LGPD quanto à localização, proteção e auditoria dos dados; c) seja nativamente integrada à plataforma de gerenciamento da solução de segurança (NGFW/SD-WAN); d) permita criação de políticas granulares para envio de arquivos à sandbox      17. Caso seja necessário licenças, para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;      18. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;      19. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class);      20. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox com frequência mínima de 15 minutos      21. Permitir o envio de arquivos para análise no ambiente controlado via de forma automática via API.   7. IDENTIFICAÇÃO DE USUÁRIOS:      1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-Directory e base de dados local;      2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;      3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;      4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;      5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;      6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);      7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;      8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;   8. FILTRO DE DADOS:      1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office e PDF) identificados sobre aplicações;      2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;      3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;      4. Geolocalização:         1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;         2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;   9. DEVE PERMITIR VPN:      1. Suportar VPN Site-to-Site e Cliente-To-Site;      2. Suportar IPSec VPN;      3. Suportar SSL VPN;      4. A VPN IPSEC deve suportar:         1. 3DES;         2. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;         3. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;         4. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);         5. A VPN IPSEc deve suportar AES 128 e 256 (Advanced Encryption Standard);         6. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;         7. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Fortinet, SonicWall;         8. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;         9. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;         10. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;         11. Atribuição de DNS nos clientes remotos de VPN;         12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;         13. Suportar autenticação via AD/LDAP, certificado e base de usuários local;         14. Suportar leitura e verificação de CRL (certificate revocation list);         15. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;         16. Deverá manter uma conexão segura com o portal durante a sessão;         17. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 (32 e 64 bit), Windows 11 (64 bit) e Mac OS X (v10.14 ou superior).         18. Deve suportar a autenticação e autorização de usuários para acesso VPN;   10. DEVE PERMITIR SD-WAN:       1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;       2. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping ou http;       3. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, todos ao mesmo tempo;       4. A solução deve permitir a definição do roteamento para cada aplicação;       5. Deve permitir balanceamento de pacotes de uma mesma sessão;       6. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e todos os links abaixo do threshold definido (estatísticas dos links);       7. Deve possibilitar a definição do link de saída para uma aplicação específica;       8. Deve implementar balanceamento de link por hash do IP de origem;       9. Deve implementar balanceamento de link por hash do IP de origem e destino;       10. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;       11. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;       12. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);       13. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:           1. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;           2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;           3. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;           4. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações;           5. Suportar a criação de políticas de QoS e Traffic Shaping por porta;           6. QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;           7. QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;       14. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;       15. QoS deve possibilitar a definição de fila de prioridade;       16. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;       17. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas à todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;       18. Deve possibilitar a definição de bandas distintas para download e upload;       19. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);       20. A solução de SD-WAN deve suportar IPv6;       21. Deve suportar o recurso de duplicação de pacotes, para mitigar cenários onde todos os links apresentam perda moderada;       22. Deve suportar recurso que permite correções de erro na transmissão;       23. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;       24. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego com- patível com a capacidade do equipamento de firewall;   11. DEVE PERMITIR O MONITORAMENTO:       1. Situação do dispositivo/cluster, se for o caso;       2. Principais aplicações;       3. Principais aplicações por risco;       4. Administradores autenticados na gerência da plataforma de segurança;       5. Número de sessões simultâneas;       6. Uso de CPU;       7. Os seguintes relatórios/dashboards devem ser suportados:       8. Resumo gráfico de aplicações utilizadas;       9. Principais aplicações por utilização de banda;       10. Principais aplicações por taxa de transferência de bytes;       11. Visibilidade sobre eventos de IPS e antivírus;       12. Estatísticas de acesso de um usuário específico;       13. Estatísticas sobre a utilização da rede de forma geral;       14. Deve permitir a criação de relatórios personalizados;       15. Deve enviar os relatórios automaticamente para e-mails pré-definidos;       16. Deve possibilitar relatórios nos formatos PDF e HTML;   12. SOLUÇÃO DE GERENCIAMENTO:       1. O fornecedor deve considerar recursos de gestão centralizada para as soluções NGFW e SD-WAN;       2. Pode ser ofertado em VM, desde que compatível com hipervisor Nutanix Acropolis;       3. Deve oferecer recursos avançado de controle de acesso baseado em funções (RBAC);       4. Deve oferecer suporte extendido a SSL e certificados ssl-ssh-profile;       5. Deve oferecer o backup automatizado de configuração de dispositivos;       6. Permitir configurar de maneira central todas as políticas de segurança: regras, IPS, filtragem web e aplicativos;       7. Permitir ajustes na política de SLA nas configurações SD-WAN e ajustar direcionamento do tráfego de maneira centralizada;       8. Obter gráficos de visibilidade de acesso e gerenciamento dos dispositivos.       9. A licença fornecida para atender as funcionalidades solicitadas deve ser de no mínimo 36 meses (três anos);       10. A console de gerência deverá informar o status up/down/speed das interfaces LAN e WAN;       11. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, antivírus e antispyware;       12. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;       13. Permitir localizar quais regras um objeto está sendo utilizado;       14. Permitir criação de regras que fiquem ativas em horário definido;       15. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;       16. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;   13. SOLUÇÃO DE LOGS:       1. Devem ser fornecida em **appliance físico, máquina virtual ou serviço em nuvem homologado pelo fabricante**, compatível com o firewall/SD-WAN ofertado, permitindo a administração centralizada de todos os dispositivos implantados.       2. O appliance virtual deve ser compatível com Nutanix AHV.       3. Caso fornecida como serviço em nuvem, garantir:   a) Nível de segurança equivalente à solução local;  b) Armazenamento dos dados em data centers certificados (ISO 27001 ou equivalente);  c) Conformidade com a LGPD;  d) Alta disponibilidade do serviço (SLA ≥ 99,5%)   * + 1. Deve oferecer console unificado para configuração de políticas de segurança (Firewall, IPS, Antivírus, Filtro de URL, Controle de Aplicações, VPN, SD-WAN), evitando necessidade de ferramentas externas.     2. Devem ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados;     3. Disponibilizar gerenciamento remoto e seguro, acessível via HTTPS, SSH e API aberta, garantindo autenticação robusta com suporte a:  1. Autenticação local ou remota via RADIUS, LDAP, SAML, TACACS+, PKI. 2. Segundo fator de autenticação (2FA/MFA) para administrador    * 1. A solução deverá estar devidamente licenciada para a quantidade adquirida;      2. Para máquina virtual os itens abaixo devem ser atendidos:   a) Permitir expansão de armazenamento conforme demanda;  b) Suportar alocação escalável de vCPUs;  c) Suportar expansão de memória conforme necessidade operacional.   * + 1. Suportar **multi-tenancy**, permitindo que diferentes ambientes ou unidades sejam administrados de forma independente a partir da mesma plataforma.     2. Garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;   Monitoração de logs; ferramentas de investigação de logs que permitam filtros diversos;   * + 1. Possuir mecanismo para que logs antigos sejam removidos automaticamente, após estarem consolidados na solução de armazenamento e análise de logs e relatoria;     2. Permitir a extração de relatórios;     3. Garantir a exportação dos logs;     4. Possuir relatórios pré-definidos;     5. Possibilitar a duplicação de relatórios e gráficos existentes para edição logo em seguida;     6. Possuir a capacidade de personalização de capas para os relatórios;     7. Permitir a geração de relatórios sobre logs de tráfego de dados;     8. Possuir a capacidade de personalização de gráficos como barra, linha, tabela e pizza para inserção aos relatórios;     9. Deve possuir mecanismo para exibir de forma detalhada informações complementares nos relatórios em tempo real;     10. Deve ser possível fazer download dos arquivos de logs recebidos;     11. Possibilitar o envio de maneira automática de relatórios por e-mail;     12. Permitir a criação e personalização de relatórios pela contratante com interface gráfica intuitiva, sem necessidade de conhecimento avançado em programação;     13. Ter a capacidade de definir filtros nos relatórios;     14. Ser capaz de definir o leiaute do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;     15. Garantir a capacidade de criar consultas SQL ou semelhantes para uso nos gráficos e tabelas de relatórios;     16. Deve dispor de gráfico demonstrando o resultado MOS de modo centralizado;     17. Deve ser possível analisar de modo centralizado o desempenho global das aplicações e desempenho por aplicação, podendo ainda filtrar por jitter, perda de pacote, latência e largura de banda;     18. Deve ser possível monitorar de modo centralizado o resultado do traffic shaping;     19. Deve dispor de relatório demonstrando o controle e risco das aplicações utilizadas no ambiente;     20. Deve oferecer um relatório com uma avaliação completa do ambiente de SD-WAN, envolvendo saúde do ambiente e utilização do tráfego;     21. Deve dispor de um painel que resume os principais eventos que ocorreram no ambiente por tipo, nome e nível de criticidade do log;     22. Deve ser possível ofuscar dados dos usuários ao realizar o encaminhamento dos logs para um servidor syslog, por exemplo;     23. Deve ser possível ofuscar dados dos usuários ao gerar um relatório;     24. Deve ser possível gerar um relatório no idioma português;     25. Deve ser possível definir um limite de recebimento de log por dispositivo;     26. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, SAML, TACACS+ e PKI;     27. Deve suportar segundo fator de autenticação para os administradores da solução;     28. Deve suportar integração com soluções de ITSM de terceiros;     29. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência da licença;     30. A licença fornecida para atender as funcionalidades solicitadas deve ser de no mínimo 36 meses (três anos).     31. Deve permitir a criação de eventos customizados, baseados em logs, que permitam à solução realizar automações variadas;     32. Acesso concorrente de administradores;     33. Mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.     34. Possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;     35. Definição de perfis de acesso à console, com permissões granulares como: acesso de escrita e leitura;     36. Autenticação integrada ao Microsoft Active Directory e servidor Radius;     37. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);     38. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;     39. Permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS e antivírus;     40. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;     41. Possuir mecanismo "Drill-Down" para navegação nos logs. Nas opções de "Drill-Down", deve ser possível identificar o usuário que fez determinado acesso;     42. Permitir que os logs e relatórios sejam rotacionados automaticamente baseados no tempo em que estão armazenados na solução, assim como no espaço em disco usado;     43. Permitir fazer o envio de logs para soluções externas de forma granular.     44. Visibilidade sobre eventos de IPS e antivírus;     45. Estatísticas de acesso de um usuário específico;     46. Deve enviar os relatórios automaticamente para e-mails pré-definidos, em formato PDF ou HTML;     47. A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente, contendo:         1. Principais eventos críticos identificados, situação geral da rede no período,   cumprimento dos indicadores de SLA (disponibilidade, tempo de resposta, tempo de resolução), ações corretivas/preventivas mais relevantes executadas.   * + - 1. Tentativas de intrusão bloqueadas: Total do período, classificação por severidade (alta/média/baixa), principais origens (IPs, países),       2. Ataques detectados (varredura, força bruta, exploits): descrição resumida. bloqueios de malware/spyware: quantidade e tipo detectado.       3. Volume total de tráfego: (em Mbps ou GB), top aplicações/protocolos: (por consumo de banda), top talkers (usuários ou IPs que mais consumiram banda): lista dos 5 principais. top destinos externos acessados: com observação de acessos suspeitos, se houver.       4. Uso de link ou vpns: estatísticas de conexão, quedas, falhas.   1. INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO DOS EQUIPAMENTOS      1. DA INSTALAÇÃO E CONFIGURAÇÃO:      2. A Solução deve ser fornecida com os componentes necessários para sua completa instalação e o perfeito funcionamento da solução.      3. O prazo poderá ser prorrogado por até 60 dias mediante justificativa da CONTRATADA.      4. A CONTRATADA deverá alocar um gerente de projeto para acompanhar e gerenciar toda a implementação do serviço;      5. O gerente de projeto deverá realizar as seguintes atividades:         1. Conduzir reunião inicial de planejamento;         2. Elaborar carta de projeto;         3. Elaborar planejamento das atividades, com previsão de datas;         4. Informar requisitos técnicos para ativação do serviço;         5. Realizar Status Report periódicos desde o start do projeto até o final da ativação;   2. DA OPERAÇÃO TÉCNICA      1. Os serviços de operação técnica deverão ser prestados 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do contrato e o atendimento deverá ocorrer após a abertura do chamado técnico, no qual deverá ser fornecido um número de registro de chamado técnico;      2. Consiste na operação das soluções ofertadas, a validação de configurações, aplicação de novas configurações, realização de atualizações de segurança, monitoramento proativo das soluções, atendimento das soluções, Health Check anuais;      3. Análise de disponibilidade;      4. Criação e configuração de VPN Site-to-Site em VXLAN;      5. Auxílio na reserva de IPv6 com base em DHCP/MAC Address;      6. Tratativas relacionadas a IPv6;      7. Problemas relativos a Certificado Digital;      8. Análise e resolução de problemas de comunicação com servidores LDAP;      9. Análise e resolução de problemas via CLI (VPN, SSO, RADIUS, dentre outros);      10. Configuração de VPN SSL com certificado próprio;      11. Auxílio na confecção de políticas com inspeção de pacotes;      12. Integrações com demais soluções de segurança presentes nesta contratação;      13. Configuração de alta disponibilidade;      14. Configuração do Single Sign On (SSO);      15. Restauração da solução a partir de backup;      16. Configuração de inspeção profunda de pacotes e SSL nas políticas de firewall;      17. Tratamento de incidentes junto ao fabricante da solução;      18. Tratamento de RMA junto ao fabricante da solução.      19. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.      20. O serviço de operação técnica deverá ser composto de um monitoramento (NOC) 24x7X365 de todos os appliances e modelos que compõem a oferta do serviço, monitorando no mínimo os seguintes parâmetros:          1. Disponibilidade de cada appliance;          2. Performance dos appliances;          3. Memoria;          4. CPU;          5. Uptime;          6. Data e horário dos alarmes.      21. Os logs de monitoramentos devem ser armazenados por no mínimo 12 meses;      22. O monitoramento deve enviar e-mail em regime 24x7 para ocorrência de alarmes de severidade crítica e alta;      23. Os serviços de operação técnica e monitoramento do (NGFW-SDWAN), gerenciamento e armazenamento de logs ofertados as unidades do SEBRAE/RO devem ser executados por meio de 02 (dois) Centros de Operações de Segurança redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos serviços de operação técnica e monitoramento.          1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.          2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, durante todo o período de vigência contratual.          3. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;          4. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da SEBRAE, sem que haja impacto na operação do Centro de Operações de Segurança e/ou da própria SEBRAE;          5. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.          6. Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação.          7. Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento;  |  | | --- | | **Certificações** | | ABNT NBR ISO/IEC 27001 | | ABNT NBR ISO/IEC 20000 | | ABNT NBR ISO/IEC 9001 |  * 1. OS NÍVEIS MÍNIMOS DE SERVIÇO      1. Os Serviços de Garantia/Suporte do Fabricante deverá ser prestado para a solução adquirida e deverá ser acionado em caso de qualquer indisponibilidade da solução, troca de equipamento danificado e/ou falhas na solução, conforme os índices de criticidade abaixo:      2. Severidade 1 - (Crítico): Sistema totalmente inoperante com impacto nas operações críticas de negócio;      3. Severidade 2 - (Alta): Sistema parcialmente inoperante com impacto nas operações críticas de negócio;      4. Severidade 3 - (Média): Sistema parcialmente inoperante sem impacto nas operações críticas de negócio;      5. Severidade 4 - (Baixa): Informacional, ajustes na configuração, dúvidas e/ou esclarecimentos;      6. Os tempos de início de atendimento e de solução após início do atendimento devem obedecer a tabela a seguir:  |  |  |  | | --- | --- | --- | | **Criticidade** | **Prazo Máximo de início de atendimento** | **Prazo máximo de solução após início de atendimento** | | Severidade 1 | Em até 1 horas\* | Em até 4 horas | | Severidade 2 | Em até 2 horas\* | Em até 12 horas | | Severidade 3 | Em até 8 horas\* | Em até 18 horas | | Severidade 4 | Em até 24 horas\*\* | Em até 48 horas | |
| 1. COMPETE AO SEBRAE/RO:   Sem prejuízo das disposições contidas neste instrumento, o Sebrae em Rondônia fica obrigado a:   1. Acompanhar e fiscalizar a execução deste contrato, de modo a zelar pela qualidade, transparência e agilidade na execução do objeto, sem prejuízo da responsabilidade da CONTRATADA; 2. Efetuar o pagamento à CONTRATADA, após a disponibilização do serviço e dos relatórios de consolidação, mediante apresentação de nota fiscal com o devido atesto pelo gestor responsável pela fiscalização do instrumento contratual; 3. Proporcionar todas as facilidades para que a CONTRATADA possa cumprir suas obrigações dentro das normas e condições estabelecidas neste Contrato; 4. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA; 5. Fiscalizar e Notificar a CONTRATADA, por escrito, sobre imperfeições, falhas, eventuais atrasos e irregularidades constatadas na execução dos serviços para que sejam adotadas as medidas corretivas necessárias; 6. Exigir o fiel cumprimento de todos os requisitos acordados e da proposta apresentada, avaliando, também, a qualidade dos serviços realizados podendo rejeitá-los no todo ou em parte; 7. Verificar a documentação apresentada para fins de pagamento; 8. Conferir a Nota Fiscal/Fatura/Recibo apresentada pela CONTRATADA em prazo que permita o seu pagamento no período referido no Contrato; 9. Comunicar formalmente à CONTRATADA sobre qualquer irregularidade constatada na execução do objeto contratado, fixando prazo para corrigir defeitos ou irregularidades verificadas no fornecimento do objeto do contrato; 10. Designar o Gestor e o Fiscal do contrato, o qual certificará a qualidade e aceite do objeto contratado; 11. Expedir a ordem de fornecimento e solicitar a entrega dos produtos de acordo com suas necessidades de consumo, observada o prazo de validade; 12. Receber o objeto no dia previamente agendado, no horário de funcionamento da unidade responsável pelo recebimento; 13. Rejeitar, no todo ou em parte, os produtos de consumo entregues em desacordo com as obrigações assumidas pelo fornecedor, no prazo de até 24 (vinte e quatro) horas, a contar da data de recebimento; 14. Comunicar à CONTRATADA quaisquer alterações relativas ao objeto do certame; 15. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA para a fiel execução do contrato. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. QUALIFICAÇÃO TÉCNICA DA EMPRESA:   5.1. Para fins de aferimento da qualificação técnica das empresas interessadas em participar do certame, deverá ser apresentado pelas mesmas: Atestado(s) de Capacidade Técnica (declaração ou certidão) fornecidos por pessoa jurídica de direito público ou privado, comprovando o desempenho, características, quantidades e prazos com o objeto da licitação, Considerando:  5.2. Entende-se por pertinente e compatível em quantidades: Atestado que comprove que a empresa efetivamente prestou ou presta serviço de fornecimento de firewall 24x7 nas especificações demandadas no edital desta licitação;  5.3. Entende-se por pertinente e compatível em prazos: Atestado que comprove que a empresa prestou ou presta serviços com as especificações demandadas no Edital desta licitação, pelo período mínimo de 12 (doze) meses;  5.4. Entende-se por pertinente e compatível em características: Atestado que demonstre em sua individualidade ou soma do serviço/fornecimento do objeto desta licitação, com serviço de fornecimento de firewall 24x7 de acordo com as especificações do presente Edital.  5.5. O atestado deverá indicar dados da entidade emissora (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, telefone, etc.). Além da descrição do objeto, quantidades e prazos de prestação dos serviços.  5.6. Todo o serviço deverá ser realizado por um técnico certificado do fabricante e comprovado;  5.7. A licitante deverá, antes da disputa pública, juntamente com a proposta comercial, apresentar os manuais, catálogos, folders, ou outros documentos técnicos, ou ainda, links públicos oficiais da solução exigida ou do serviço exigido, para comprovação do atendimento às características técnicas especificadas neste Termo de Referência;  5.7. Deverá ser fornecida uma planilha em formato xlsx, docx ou pdf, junto à proposta comercial com a comprovação de todos os itens das especificações técnicas indicando documento ou link público com seu devido trecho e página.  5.8. No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação pelo SEBRAE/RO deverá vir indicando corretamente, o item, especificação, link ou documento, página e trecho que comprove o atendimento de cada item/subitem das especificações técnicas descritas nos serviços a serem ofertado, conforme modelo abaixo.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Item** | **Especificação** | **Link ou Documento** | **Página** | **Trecho** | |  |  |  |  |  | |  |  |  |  |  |   5.9. Deverá apresentar com clareza a marca, o modelo, o tipo, a configuração e outras informações aplicáveis e necessárias à perfeita caracterização do dispositivo, serviço ou componente proposto, de forma a permitir a correta identificação deste na documentação técnica apresentada.  5.10. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento desses requisitos implicará na desclassificação da proposta  5.11. A CONTRATADA deverá apresentar carta do fabricante que demonstre que ela é empresa parceira de todas as soluções ofertadas neste certame.  5.12. Os documentos serão analisados, para fins de verificação do atendimento às características da solução especificados neste Edital.  5.13. A análise das características dos itens ofertados será procedida em cotejo com as especificações técnicas constantes deste instrumento, não sendo admitidos itens com especificações inferiores.  5.14. Na hipótese de a proposta da licitante ser desclassificada, por não atendimento das especificações técnicas requeridas, serão convocadas as demais licitantes, obedecendo-se rigorosamente a ordem de classificação das propostas, seguindo-se aos mesmos moldes descritos nos itens anteriores. |

|  |
| --- |
| 1. VIGÊNCIA:   6.1. O contrato terá vigência de 36 (trinta e seis) meses, contados a partir da data de assinatura, podendo ser prorrogado, não ultrapassando o limite estipulado no REGULAMENTO DE LICITAÇÕES E CONTRATOS DO SISTEMA SEBRAE:  *Art. 36. Os contratos terão prazo determinado, não podendo ultrapassar, inclusive com suas eventuais prorrogações, o limite máximo de 10 (dez) anos, ressalvadas as hipóteses previstas neste artigo, desde que haja previsão no processo de contratação, com ou sem licitação, e que as condições permaneçam vantajosas.* |

|  |
| --- |
| 1. ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO: 2. A gestão do contrato será realizada pelo Sebrae/RO que fará o acompanhamento da execução para suprir eventual necessidade de informações e ações corretivas juntamente à empresa, e deverá receber e aprovar entregas citadas neste termo, e atestar as notas fiscais quando comprovada sua fiel e correta execução para fins de pagamento. 3. Para a gestão do contrato, fica designado o analista da Unidade de Tecnologia da Informação e Comunicação, do Sebrae/RO. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. PRAZOS E CONDIÇÕES DE ENTREGA DO PRODUTO/SERVIÇO:    1. A contratada deverá entregar e instalar todos os links e acessórios no prazo de 60 (sessenta) dias corridos nas Unidades Regionais e Ponto de Atendimento, a contar da data de expedição da Ordem de Serviço pela contratante nos seguintes endereços:       1. A contratada deverá entregar e instalar todos os links e acessórios no prazo de 60 (sessenta) dias corridos nas Unidades Regionais e Ponto de Atendimento, a contar da data de expedição da Ordem de Serviço pela contratante nos seguintes endereços:  |  |  | | --- | --- | | **Unidade do Sebrae** | **Endereço** | | **Guajará Mirim** | Av. Dr. Mendonça de Lima, 311, Centro, Guajará Mirim – RO. | | **Ariquemes** | Av. Tancredo Neves, 1730, Setor Institucional, Ariquemes – RO. | | **Jaru** | Rua João Batista, 3038, Setor 1, Jaru – RO. | | **Ji-Paraná** | Av. Presidente Vargas, 742, Centro, Ji-Paraná – RO. | | **Cacoal** | Av. Castelo Branco, 17020, Incra, Cacoal – RO. | | **Rolim de Moura** | Av. 25 de Agosto, 6172, Setor Industrial, Rolim de Moura – RO. | | **Pimenta Bueno** | Av. Fagundes Varela, 361, Centro, Pimenta Bueno – RO. | | **Vilhena** | Av. Rony de Castro Pereira, 4061, Jardim América, Vilhena – RO. | |

|  |
| --- |
| 1. PENALIDADES:   A inexecução total ou parcial injustificada, a execução deficiente, irregular ou inadequada, a subcontratação total ou parcial, assim como o descumprimento dos prazos e condições estipulados no contrato implicará, conforme o caso, a aplicação das seguintes penalidades:   1. Advertência; 2. Multa, nas hipóteses abaixo elencadas:    1. De até 10% (dez por cento) sobre o valor do contrato, no caso de inexecução total;    2. De até 10% (dez por cento) sobre os valores dos objetos não executados, no caso de inexecução parcial;    3. De 1% (um por cento) do valor dos respectivos objetos por dia de atraso, limitado a 10 (dez) dias, no caso de atraso na entrega, não ultrapassando 10% (dez por cento); 3. Rescisão unilateral do contrato, sem prejuízo do pagamento das respectivas multas, na hipótese de ocorrer: 4. O previsto nas alíneas a ou b do inciso II desta Cláusula; 5. A extrapolação dos 10 (dez) dias previstos na alínea c do inciso II, desta cláusula. 6. Multa de até 10% (dez por cento) do valor total atualizado do contrato, sem prejuízo do pagamento de outras multas que lhe tenham sido aplicadas e de responder por perdas e danos que a rescisão ocasionar ao SEBRAE, no caso de rescisão do contrato por iniciativa da CONTRATADA, sem justa causa; 7. Suspensão temporária do direito de licitar e contratar com o Sistema SEBRAE, por prazo de até 2 (dois) anos, a critério do Sebrae/RO, pela aplicação das penalidades acima.   **Parágrafo** **Primeiro**: Para a aplicação das penalidades aqui previstas, a CONTRATADA será notificada para apresentar defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir da notificação. Após decurso do prazo, não apresentando a Contratada defesa prévia, ou o Gestor do Contrato julgue a justificativa improcedente, deverá este tomar as providencias necessárias a regular aplicação da penalidade.  **Parágrafo Segundo**: As multas serão descontadas dos pagamentos a que a CONTRATADA fizer jus ou recolhidas diretamente à tesouraria do Sebrae/RO, no prazo de 15 (quinze) dias corridos, contados a partir da data de sua comunicação ou, ainda, quando for o caso, cobradas administrativa ou judicialmente Parágrafo Terceiro: As penalidades previstas neste contrato são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis. |

|  |
| --- |
| 1. FORMA DE PAGAMENTO: 2. A CONTRATADA deverá encaminhar a Nota Fiscal/Fatura de produto/serviço por e-mail ou diretamente pelo sistema SE ou no Sebrae em Rondônia na Avenida Campos Sales, 3421, Bairro Olaria, Porto Velho - Rondônia e endereçada ao gestor do contrato, com entrega protocolada, a fim de que sejam adotas as medidas afetas ao pagamento; 3. O pagamento será efetuado mediante crédito em conta bancária indicada pela empresa registrada, no prazo de até 10 (dez) dias úteis contados na data da apresentação de nota fiscal ao Sebrae em Rondônia, e devidamente atestada após verificação da regularidade fiscal da CONTRATADA; 4. A Nota Fiscal deverá ser entregue ao Sebrae em Rondônia pela CONTRATADA, respeitando a data limite do dia 20 de cada mês para entrega do documento fiscal; 5. Quaisquer despesas decorrentes de transações bancárias correrão por conta da CONTRATADA; 6. O Sebrae em Rondônia poderá deduzir, do montante a pagar, as indenizações devidas pela CONTRATADA em razão de inadimplência; 7. As Notas Fiscais/Faturas não aprovadas pelo Sebrae em Rondônia com erros ou circunstância que impeça a liquidação da despesa serão devolvidas pelo Gestor à CONTRATADA para as correções, acompanhadas dos motivos de sua rejeição, e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal, sem qualquer tipo de reajuste de seu valor ou qualquer ônus para o Sebrae em Rondônia, seja ele a que título for; 8. Deverão constar obrigatoriamente no corpo das notas fiscais as seguintes informações:  * Razão social; CNPJ; Inscrição Estadual; Inscrição Municipal; * Informar o número da contrato; Valor total, com as deduções de impostos devidos; * Descrição dos produtos/serviços fornecidos, quantidade do produto, preço unitário, data de emissão.  1. É condição para o recebimento dos créditos decorrentes dos produtos fornecidos, a CONTRATADA apresentar juntamente com as notas fiscais/faturas as Certidões que comprovem sua regularidade fiscal com os seguintes documentos:    1. Certidão Conjunta de Débitos Relativos a Tributos Federais/INSS;    2. Certidão de Regularidade de Tributos Estaduais;    3. Certidão de Regularidade de Tributos Municipais;    4. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço –FGTS;    5. Certidão Negativa de Débitos Trabalhistas – TST. |

Porto Velho, 11 de agosto de 2025