



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de solução de firewall next generation, com licenças de segurança, instalação, migração e suporte técnico, com garantia do fabricante/fornecedor mínima de 60 (sessenta) meses, para modernização da infraestrutura da tecnológica da Câmara Municipal de Ribeirão Preto, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	ESPECIFICAÇÃO	CÓDIGO MAT/SER	UNIDADE DE MEDIDA	QUANTIDADE
1	1	Firewall de Próxima Geração - Next-Generation Firewall (NGFW) ou UTM - Solução em cluster de alta disponibilidade (HA) ativo/passivo incluídas as licenças de uso do software de segurança com todas as funcionalidades descritas e ativas, com garantia, suporte técnico e atualização, por 60 meses.	CATMAT 609340	UNIDADE	01
	2	Appliance ou servidores exclusivos para armazenamento de logs incluídas as licenças de uso de software, com garantia, suporte técnico e atualização, por 60 meses.	CATMAT 481646	UNIDADE	01
	3	Licenças de uso de software para servidores de rede em ambiente virtual e físico com todas as funcionalidades descritas e ativas, com suporte técnico e atualização de software, enquanto vigorar o contrato.	CATSER 27464	UNIDADE	25

- 1.2. O Fornecimento e Prestação de Suporte para Solução Corporativa de recursos para Data Center contemplando Hardware, Software, Subscrições de Segurança, Treinamento, por conseguinte, implantação, configuração, garantia, suporte com transferência de conhecimento, monitoramento 24x7 por NOC Físico e suporte técnico integral da solução.
- 1.3. A contratação será na modalidade de fornecimento e suporte para equipamentos nas instalações da CONTRATANTE e em nuvem nos casos das subscrições que forem citados neste termo de referência. Os equipamentos instalados no local da CONTRATANTE e serviços técnicos de suporte presencial ou remoto conforme com as funcionalidades mínimas descritas neste Termo de Referência e seus Anexos.
- 1.4. A solução de segurança deverá se basear em componentes de hardware do tipo Appliance para Firewall NGFW e software integrados dos respectivos fabricantes sob a forma de subscrições e/ou licenças de uso.
- 1.5. A solução de proteção deverá ser fornecida como software sob a forma de subscrições ou licença de uso.
- 1.6. A solução deverá ser fornecida sob a forma de licenciamento de uso;
- 1.7. Todos os softwares envolvidos nas soluções de segurança deverão ser integrados logicamente aos equipamentos e com as funcionalidades mínimas descritas neste Termo de Referência e seus Anexos e deverão ser obrigatoriamente da mesma marca.
- 1.8. Não será aceita nenhuma solução com equipamentos de propósito genérico (PCs ou Servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 1.9. VISTORIA OPTATIVA: a licitante deverá visitar as seguintes instalações, com anterioridade à abertura da sessão do Pregão, oportunidade em que lhe será fornecido Atestado de Vistoria:
 - 1.9.1. É recomendada para averiguação e ciência da complexidade da arquitetura técnica atual, das necessidades de serviços na instalação que a licitante deverá prover e que recairão na proposta para atender o objeto e exigências descritas nesta licitação.
 - 1.9.2. A vistoria deverá ser agendada pelo telefone Fone (16) 3607 4096 - Coordenadoria Administrativa ou e-mail: diretoria@camararibeiraopreto.sp.gov.br.
 - 1.9.3. Câmara Municipal de Ribeirão Preto - Endereço: Av. Jerônimo Gonçalves, 1200, Centro, Ribeirão Preto/SP, CEP 14010-907.
- 1.10. Em nenhum momento a LICITANTE poderá alegar a falta de informações do ambiente de instalação e das condições para tal, uma vez que será dada a oportunidade de sua verificação in-loco para a inclusão de todos os componentes de instalação e de prestação dos serviços, acessórios e outros em sua proposta.
- 1.11. A licitante fica ciente e responsável de todo e qualquer ônus de sua omissão na cotação de algum componente, acessório ou serviço não incluído em sua proposta no certame de licitação, não podendo, em nenhum momento cobrar adicionais da CONTRATANTE para a entrega do objeto deste Edital.
- 1.12. Destacamos que a solução ofertada deverá ser entregue em operação plena, integrada aos demais equipamentos dos Data centers da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO, ou seja, a arquitetura técnica atual deverá conviver com a arquitetura técnica dos novos equipamentos desta licitação.
- 1.13. A solução proposta deverá contemplar OBRIGATORIAMENTE a migração de todas as regras e políticas de segurança atualmente adotadas no ambiente que está instalado na CÂMARA MUNICIPAL DE RIBEIRÃO PRETO, para minimizar os impactos no ambiente dos usuários.
- 1.14. A prestação dos serviços e a entrega dos produtos será em um lote único e indivisível, e vem ao encontro do conceito de conglobação dos itens, que busca evitar prejuízo ao conjunto diversificado de atividades integradas que se aglutinam em um único complexo. Ou seja, o necessário agrupamento no lote foi fundamentado nas características intrínsecas da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO aos produtos que se completam e se dependem para o funcionamento integral e sem falhas.
- 1.15. Todos os serviços serão regidos com Acordo de Níveis Mínimos de Serviço, objetivando a boa prestação dos serviços de suporte contratados.
- 1.16. Para o atendimento do objeto e as prestações de serviços, a decisão sobre o número de profissionais necessários tornar-se-á de responsabilidade da CONTRATADA, porém um mínimo de profissionais será exigido, reforçando a premissa acima de que os níveis mínimos de serviço se tornam instrumento que traga garantia à qualidade na prestação dos serviços.
- 1.17. Em observância Lei n.º 14.133/2021, as especificações técnicas do objeto a ser contratado atendem aos padrões usuais do mercado e não contêm minúcias excessivas, irrelevantes ou desnecessárias que limitem a competição.
- 1.18. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as LICITANTES, desde que não comprometam o interesse público, a finalidade e a segurança da contratação.
- 1.19. O objeto desta contratação deverá incluir todos os custos e despesas diretas e indiretas, tributos e impostos incidentes, encargos sociais, previdenciários, trabalhistas e comerciais, materiais e mão de obra a empregados, seguros, frete, embalagens e quaisquer outros obrigatórios ou necessários deverão estar inclusos à composição do preço do presente objeto.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 1.20. Além dos fornecimentos descritos, a empresa contratada deverá estar apta a instalar, parametrizar, configurar e dar o suporte técnico, durante a vigência contratual, oferecendo garantias e pleno funcionamento das soluções descritas neste Termo de Referência e nos Anexos. Será também exigido o treinamento em todas as soluções implementadas de software e hardware que estiverem envolvidas no fornecimento, com capacitação técnica e logística para o atendimento de chamados técnicos, ilimitados, durante a vigência contratual.
- 1.21. A instalação de equipamentos necessários para a prestação dos serviços deverá ser de no máximo 90 (noventa) dias corridos, a contar a partir da assinatura do contrato e ser efetuada de forma planejada e aprovada previamente pelos responsáveis do Departamento de Informática da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO.
- 1.22. Os profissionais que executarão os serviços de implantação, migração e manutenção deverão ter experiência e conhecimentos em cada solução descrita e deverão ser comprovadas por meio de certificações ou declaração de fabricante, onde for indicado no Termo de Referência e seus Anexos.
- 1.23. Ao término da implantação, a CONTRATADA deverá entregar à CONTRATANTE, documentação técnica do projeto contendo informações de configurações, parâmetros, resultados de testes, procedimentos de contingência e demais informações pertinentes para a operação e manutenção das soluções implantadas.
- 1.24. A CONTRATADA deverá capacitar os técnicos da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO, indicados pelo Departamento de Informática e Telecomunicações, em todos os componentes de hardware e software implantados, descrito neste Edital.
- 1.25. A CONTRATADA, deverá seguir as recomendações de Órgãos Públicos de Saúde, Ministério do Trabalho e da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO quanto aos cuidados na execução dos serviços e proteção individual dos seus colaboradores.
- 1.26. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.
- 1.27. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme justificativa constante do Estudo Técnico Preliminar.

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.

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

- 3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

Especificação dos materiais e serviços

3.2. ESCOPO E DEFINIÇÕES DA ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SEGURANÇA

- 3.2.1. A CONTRATADA deverá fornecer os equipamentos, licenças de uso de software e demais componentes, conforme descritos neste Termo de Referência e seus Anexos. Acessórios e itens de instalação e conectorização para o bom funcionamento da solução é de responsabilidade da CONTRATADA e deverá ser verificada esta necessidade na ocasião da vistoria técnica.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.2.2. O hardware e o software (componentes das soluções) não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. A LICITANTE deverá apresentar uma carta de compromisso certificando que os componentes da solução estão de acordo com essa exigência.
- 3.2.3. A CONTRATADA deverá fornecer solução de Armazenamento de LOGs em equipamentos especialmente destinado para esse fim em Appliance ou em Servidor físico, ambos em configuração para instalação em rack 19”:
- 3.2.3.1. O armazenamento dos logs NÃO poderá ser efetuado dentro dos Appliance FIREWALL / NGFW.
- 3.2.3.2. A CONTRATADA deverá fornecer software de sistema de pesquisa e relatórios a partir do sistema de armazenamento de logs, cujas especificações estão presentes no descritivo dos FIREWALL, sem mais custos adicionais.
- 3.2.3.3. Cada FIREWALL / NGFW deverá possuir 1 (uma) Appliance de armazenamento, com no máximo 2U no padrão 19” com fonte redundantes e discos SSD embarcados na solução e descritos neste documento.
- 3.2.4. Os equipamentos Firewall Next-Generation (NGFW), deverá conter licenciamento de uso de software de segurança com especificações e requisitos mínimos contidos no ITEM específico de FIREWALL NGFW.
- 3.2.5. O licenciamento de software de segurança avançada deverá suportar a autenticação de duplo fator para Servidores de Rede e Usuários.
- 3.2.6. Deverão ser fornecida 25 (vinte e cinco) licenças do software de Segurança Avançada Anti-Exploit, Anti-Ransomware para proteção de Servidores e estas deverão ser monitorados por meio de uma central em nuvem para defesa zero-day anti-exploit baseados em comportamento a fim de realizarem o bloqueio das técnicas mais avançadas de entrega de malwares de ZERO DIA.
- 3.2.7. Deverá ser fornecida as licenças de Software sem nenhum custo adicional para a CONTRATANTE.
- 3.2.8. Todo o licenciamento fornecido para a solução proposta deverá possibilitar a renovação automática na ocorrência de renovação/prorrogação contratual (nos termos da lei de licitações), sem ônus adicional ao CONTRATANTE. Esta diretriz vale para todos os itens deste termo de referência, que apresentem a necessidade de licenciamento de uso.
- 3.2.9. Toda a solução deverá prever o fornecimento de suporte, instalação, parametrização, configuração, manutenção preventiva, corretiva e preditiva, suporte técnico local e remoto, monitoramento e gerenciamento na modalidade 24x7x365, pelo período de 60 (sessenta) meses.

3.3. ITENS DE FORNECIMENTO

- 3.3.1. Os itens de fornecimento da solução a ser ofertada deve ser o conjunto completo dos componentes, expressos na tabela a seguir:

O detalhamento dos itens desta tabela está contido neste documento e seus anexos.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

TABELA DE FORNECIMENTO DE HARDWARE E SOFTWARE				
Item	Solução	Descrição	Qtde	Métrica
1	FIREWALL NGFW	<i>Firewall de Próxima Geração - Next-Generation Firewall (NGFW) ou UTM</i> - Solução em cluster de alta disponibilidade (HA) ativo/passivo incluídas as licenças de uso do software de segurança com todas as funcionalidades descritas e ativas, com garantia, suporte técnico e atualização, enquanto vigorar o contrato por 60 meses	01	Appliance (hardware) + software
2	Solução de Armazenamento de Logs	<i>Appliance ou servidores exclusivos</i> para armazenamento de logs incluídas as licenças de uso de software, com garantia, suporte técnico e atualização, enquanto vigorar o contrato por 60 meses.	01	Appliance (hardware) + software
3	Solução de proteção avançada para proteção de servidores de rede virtual e físico	<i>Licenças de uso de software para servidores de rede</i> em ambiente virtual e físico com todas as funcionalidades descritas e ativas, com suporte técnico e atualização de software, enquanto vigorar o contrato	25	L.U. Licença de Uso

3.4. DEFINIÇÕES TÉCNICAS PARA FIREWALL – NGFW

- 3.4.1. A solução de FIREWALL NGFW deverá ser do tipo Appliance Firewall NGFW ou UTM operando em cluster de alta disponibilidade (HA) em modo ativo-passivo, constituído de 2 (dois) equipamentos idênticos e da mesma marca para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, equipamentos para proteção de informação perimetral e de rede interna, administração de largura de banda (QoS), VPN IP Sec, SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, inspeção de tráfego criptografado (SSL inspection), proteção DNS e Sandbox em Nuvem. Deverá ser fornecida console de gerenciamento dos equipamentos instalado na rede ou virtualizado, ou ambos, fornecido pelo mesmo fabricante da marca dos FIREWALL NGFW.
- 3.4.2. A solução ofertada deverá contemplar a totalidade das capacidades exigidas em cada Appliance que, individualmente deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceita a somatória de vazões, no caso de mais de um equipamento, para atingir os limites mínimos exigidos.
- 3.4.3. Os equipamentos envolvidos na prestação dos serviços deverão ser monitorados por meio de uma central única de monitoração, para todas as funcionalidades descritas, com sincronização com todos os Servidores Active Directory da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO, políticas por usuários e grupos de usuários, administração de largura de banda (QoS), VPN IP Sec, SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, inspeção de tráfego criptografado (SSL inspection), proteção DNS e Sandbox em Nuvem. Deverá ser fornecida console de gerenciamento dos equipamentos instalado na rede ou virtualizado, ou ambos, fornecido pelo mesmo fabricante da marca dos FIREWALL NGFW.
- 3.4.4. Todo o software/subscrição de segurança envolvido deverá ser processado exclusivamente nos equipamentos FIREWALL NGFW, exceto se indicado o contrário.
- 3.4.5. O fabricante da solução de FIREWALL NGFW deverá ser avaliado pela NSS Labs 2019 (Network Security Services) no desempenho do Next Generation Firewall Comparative;
- 3.4.6. Não serão aceitos equipamentos com discos rígidos internos. Analysis mais recente, estando no "Security Value Map" acima de 95% (noventa por cento) da avaliação de segurança efetiva.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.7. Fornecimento de equipamento FIREWALL NGFW em Appliance adicionadas as licenças de uso do(s) software de todos os serviços baseados em subscrição para atender ao objeto deste EDITAL;
- 3.4.8. Não serão aceitos equipamentos baseados em PC ou servidores genéricos;
- 3.4.9. Não serão aceitos equipamentos com discos rígidos internos.
- 3.4.10. Os equipamentos fornecidos deverão ser baseados na tecnologia Stateful Inspection, com funcionalidade de operação em modo de alta disponibilidade – ativo-passivo;
- 3.4.11. Os equipamentos oferecidos deverão ter suporte à proteção imediata contra ameaças (default threat protection / zero day threat protection), Filtro de Conteúdo, IPS, Anti-spam, Anti-virus, Autoridade de Reputação na Web, Controle de Aplicações e APT (Advanced Persistent Threat) e devem oferecer suporte, no mínimo, a três zonas de segurança: ZONA EXTERNA, PRIVADA e DMZ;
- 3.4.12. Deverão oferecer suporte à configuração de endereços IP estáticos e dinâmicos (por DHCP e PPPoE) em interfaces externas.
- 3.4.13. Os equipamentos aqui solicitados deverão ser aptos para montagem em rack padrão de 19", com altura máxima de 3U e ambos com as licenças de uso ativas e válidas durante a vigência do contrato sendo que cada equipamento deverá apresentar OBRIGATORIAMENTE, no mínimo, os seguintes recursos e características, em cada um dos equipamentos TIPOS fornecidos, tipo RACK 19".
- 3.4.14. Portas de comunicação:
 - 3.4.14.1. Deverá possuir no mínimo 8 (oito) portas 1Gb no padrão RJ45 (cobre) e 2 (DUAS) portas 10 GbE SPF+, podendo todas elas serem configuradas em qualquer das zonas de segurança disponíveis: zona externa, privada ou opcional DMZ bem como interfaces de gerenciamento;
 - 3.4.14.2. (uma) porta RJ45 GbE para gerenciamento e duas portas USB todas posicionadas na parte frontal dos equipamentos;
- 3.4.15. Firewall throughput (UDP 1518) de no mínimo, 16,0 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
- 3.4.16. Throughput VPN (VPN UDP 1518) mínimo de 5,0 Gbps;
- 3.4.17. IPS throughput mínimo de 3,0 Gbps (varredura completa);
- 3.4.18. Capacidade mínima de suportar 4.000.000 de sessões concorrentes, conexões simultâneas para o NGFW;
- 3.4.19. Capacidade mínima de suporte a 90.000 novas conexões por segundo;
- 3.4.20. Deverá possuir AntiVirus com throughput mínimo de 3,0 Gbps;
- 3.4.21. Deverá possuir FIREWALL NGFW throughput FULL SCAN de no mínimo 2,0 Gbps;
- 3.4.22. Deverá suportar VPNs, fixas e móveis;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.22.1. Oferecer suporte a VPNs móveis sobre protocolos IPSEC e PPTP, com licenciamento, para 250 usuários móveis no protocolo IPSEC e com licenciamento, para 250 usuários móveis no protocolo SSL.
- 3.4.22.2. Deverá suportar 250 VPNs fixas usando protocolo IPSEC e deverá suportar a configuração de VPNs fixas com qualquer outro produto que ofereça suporte ao padrão IPSEC.
- 3.4.23. Os equipamentos deverão suportar os mecanismos de autenticação DES, 3DES, AES 128, 192, 256-bit e mecanismos de cifra SHA-1, MD5, IKE Pre-Shared Key, certificados digitais;
- 3.4.24. Os equipamentos deverão suportar a Dead Peer Detection (DPD);
- 3.4.25. Os equipamentos deverão suportar a VPN failover;
- 3.4.26. Os equipamentos deverão suportar a Caching Proxy Server (Uso de Servidor de Cache):
 - 3.4.26.1. Exceptions (Exceções);
 - 3.4.26.2. Safe Search Enforcement (Suporte a Busca Segura);
 - 3.4.26.3. Filtro de Conteúdo;
 - 3.4.26.4. AntiVirus (Anti-vírus);
 - 3.4.26.5. Reputation Enabled Defense (Defesa por Autoridade de Reputação);
 - 3.4.26.6. Deny Message (Mensagem de Bloqueio);
 - 3.4.26.7. Proxy and AV Alarms (Geração de Alarmes) suporte a tráfego de broadcast e multicast sobre VPNs.
- 3.4.27. A solução deverá suportar no mínimo 250 VLANs;
- 3.4.28. Os equipamentos deverão suportar regras de firewall com autenticação de usuários (sem limites ao número de usuários) a partir de base de dados interna e servidores de autenticação RADIUS, IPSEC, LDAP e Active Directory;
- 3.4.29. Os equipamentos deverão oferecer suporte a Serviço de DNS dinâmico (Dynamic DNS) no caso de interfaces externas serem configuradas com endereços IP dinâmicos;
- 3.4.30. Os equipamentos deverão oferecer suporte a implementação de regras de firewall de tipo Proxy (em camada 7 ou camada de aplicação) para, os protocolos HTTP, HTTPS, POP3, SMTP, FTP, DNS, VoIP (H.323 e SIP) e TCP-UDP.
- 3.4.31. Os equipamentos deverão suportar solução de software SD-WAN integrada ao FIREWALL NGFW ou UTM com, no mínimo, Failover Multi-WAN, seleção dinâmica de caminho, controle de instabilidades e de perda de conexão ou de latência dos links.
- 3.4.32. As regras de proteção de DNS deverão controlar e atender, no mínimo, aos seguintes aspectos:
 - 3.4.32.1. Deverá possuir proteção de DNS incluída na própria ferramenta ou entregue em composição com outro fabricante (outra marca);



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.32.2. Deverá possuir serviço baseado em nuvem que monitora pedidos de DNS para evitar conexões com domínios mal-intencionados conhecidos;
 - 3.4.32.3. Deverá proteger contra os domínios de phishing e clickjacking maliciosos, independentemente do tipo de conexão, protocolo ou porta;
 - 3.4.32.4. Deverá resolver a requisição de DNS para um endereço IP de blackhole, caso uma ameaça seja detectada, em vez de resolver o endereço IP real;
 - 3.4.32.5. Deverá encaminhar ao usuário uma página de negação personalizável, em caso de conexão HTTP/S negada;
 - 3.4.32.6. Deverá fornecer alertas e análises via e-mail para os administradores da rede.
- 3.4.33. Definição das regras de firewall de tipo Proxy:
- 3.4.33.1. Deverá permitir o controle dos seguintes aspectos do protocolo HTTP:
 - 3.4.33.1.1. HTTP Request/Response: General Settings (Configurações Gerais)
 - 3.4.33.1.2. HTTP Request: Request Methods (Métodos HTTP)
 - 3.4.33.1.3. HTTP Request: URL Paths (URLs)
 - 3.4.33.1.4. HTTP Request/Response: Header Fields (Campos de Header)
 - 3.4.33.1.5. Request: Authorization (Autorização)
 - 3.4.33.1.6. HTTP Response: Content Types (Tipos MIME)
 - 3.4.33.1.7. HTTP Response: Cookies
 - 3.4.33.1.8. HTTP Response: Body Content Types (Tipos de Arquivos)
 - 3.4.33.1.9. Use a Caching Proxy Server (Uso de Servidor de Cache)
 - 3.4.33.1.10. Exceptions (Exceções)
 - 3.4.33.1.11. Safe Search Enforcement (Suporte a Busca Segura)
 - 3.4.33.1.12. Filtro de Conteúdo
 - 3.4.33.1.13. AntiVirus (Anti-vírus)
 - 3.4.33.1.14. Reputation Enabled Defense (Defesa por Autoridade de Reputação)
 - 3.4.33.1.15. Deny Message (Mensagem de Bloqueio)
 - 3.4.33.1.16. Proxy and AV Alarms (Geração de Alarmes)
 - 3.4.33.2. Deverá permitir o controle dos seguintes aspectos do protocolo HTTPS:
 - 3.4.33.2.1. General Settings (Configurações Gerais)
 - 3.4.33.2.2. Content Inspection (Inspeção de Conteúdo)



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.33.2.3. Bypass List (Lista de Bypass)
- 3.4.33.2.4. Filtro HTTPS (Filtro de Conteúdo)
- 3.4.33.2.5. Certificate Names (Certificados Digitais)
- 3.4.33.2.6. Proxy and AV Alarms (Geração de Alarmes)

3.4.33.3. Deverá permitir o controle dos seguintes aspectos do protocolo POP3:

- 3.4.33.3.1. General Settings (Configurações Gerais)
- 3.4.33.3.2. Authentication (Autenticação)
- 3.4.33.3.3. Content Types (Tipos MIME)
- 3.4.33.3.4. 6.33.3.4 File Names (Nomes de Arquivos)
- 3.4.33.3.5. 6.33.3.5 Headers (Headers)
- 3.4.33.3.6. 6.33.3.6 Deny Message (Mensagem de Bloqueio)
- 3.4.33.3.7. 6.33.3.7 AntiVirus (Anti-vírus)
- 3.4.33.3.8. 6.33.3.8 Filtro de Spam (Anti-spam)
- 3.4.33.3.9. 6.33.3.9 Proxy and AV Alarms (Geração de Alarmes)

3.4.33.4. Deverá permitir o controle dos seguintes aspectos do protocolo SMTP:

- 3.4.33.4.1. General Settings; Greeting Rules; ESMTP Settings; TLS Encryption; Authentication; Content Types; File Names; Mail From / Rcpt To; Headers (Headers); Antivirus; Deny Message; Anti-spam; Proxy and AV Alarms.
- 3.4.33.4.2. Deverá permitir o controle dos seguintes aspectos do protocolo FTP: General Settings; Commands; Content - Upload; Content – Download; AntiVirus; Proxy and AV Alarms.
- 3.4.33.4.3. Deverá permitir o controle dos seguintes aspectos do protocolo DNS : General Settings; OPcodes; Query Types; Query Names; Proxy and AV Alarms.
- 3.4.33.4.4. Para o proxy / application layer gateway deverá permitir o controle dos seguintes aspectos do protocolo H.323 e SIP: General Settings; Access Control; Denied Codecs.

3.4.34. Cada equipamento deverá suportar serviços de NAT, nas seguintes modalidades:

- 3.4.34.1. NAT estático e dinâmico;
- 3.4.34.2. NAT 1-to-1;
- 3.4.34.3. NAT Traversal;
- 3.4.34.4. NAT sobre VPN (1-to-1 NAT Through VPN);



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.34.5. NAT baseado em políticas (Policy-Based Dynamic NAT).
- 3.4.35. Cada equipamento deverá suportar serviços de PAT (Port Address Translation);
- 3.4.36. Os equipamentos FIREWALL NGFW deverão oferecer suporte à divisão de cargas entre servidores (server load-balance);
- 3.4.37. Os equipamentos deverão oferecer serviços de multi-wan (suporte a múltiplos links / enlaces externos), com suporte a no mínimo quatro interfaces destinadas à zona externa de segurança, com possibilidade de funcionamento em modo failover ou em modo de divisão de carga (load-balance), neste caso com possibilidade de definição pelo administrador do algoritmo a ser utilizado (round-robin, weighted round-robin, routing table ou interface overflow);
- 3.4.38. A solução deverá suportar serviços de gerência de tráfego (traffic management) e de QoS
- 3.4.39. (Quality of Services – qualidade de serviços);
- 3.4.40. Os equipamentos deverão possibilitar a implementação em modo de roteador (modo routed), em modo semitransparente (modo drop-in, com endereço IP único para todas as interfaces de rede) e em modo transparente (modo bridge ou switch);
- 3.4.41. Os equipamentos deverão oferecer suporte a IPv6 conforme o IPv6 Forum (Product Classification - Router; IPv6 Ready Phase 2 - Gold Logo);
- 3.4.42. Os equipamentos deverão possuir obrigatoriamente o certificado de homologação da ANATEL.
- 3.4.43. A instalação dos equipamentos com as licenças de segurança ativas deverá suportar a autenticação de usuário nos seguintes aspectos:
- 3.4.43.1. Banco de dados interno, Windows Active Directory, LDAP, RADIUS;
- 3.4.43.1.1. No caso do Active Directory, a solução deve fornecer uma opção Single Sign-On (SSO) para que os usuários não precisem se autenticar no firewall depois de terem autenticados no domínio AD;
- 3.4.43.1.2. Os relatórios emitidos por Usuários Autenticados, os relatórios deverão incluir o nome de usuário e endereço IP usado para fazer a conexão;
- 3.4.43.1.3. Deverá possuir mecanismo automático de redirecionamento dos usuários para o portal de autenticação quando SSO não é utilizado;
- 3.4.43.1.4. O portal de autenticação deve suportar usuários que se conectam a partir de dispositivos móveis, tais como smartphones.
- 3.4.43.1.5. Os equipamentos deverão cumprir, ou estar em processo de cumprimento, com as certificações de segurança eletrônica, no mínimo, ICSA Firewall, ICSA IPSEC, VPN, FIPS, e VPNC;
- 3.4.43.1.6. Os equipamentos deverão possuir fontes de energia as quais possam operar sobre uma voltagem de 100 a 240 VAC (auto-sensing);
- 3.4.43.1.7. Operar, no mínimo, sob condições ambientais de temperaturas entre 0 e 40 graus Celsius com percentual de umidade relativa entre 10% e 85%;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.44. Os equipamentos em operação plena deverão permitir monitorar e desconectar usuários internos, em tempo real e por espaço de tempo definido pelo administrador, sem necessidade de criação de regras ou políticas de segurança adicionais;
- 3.4.45. Deverá permitir a geração e envio de alarmes / notificações por protocolo SNMP v2 ou v3, janela de pop-up ou mensagem de e-mail;
- 3.4.46. Deverá suportar administração via interface web (browser), por interface de rede, sobre protocolo seguro HTTPS, permitindo alterar o número da porta TCP usada para conexões HTTPS;
- 3.4.47. Deverá suportar administração via interface gráfica (sistema específico de gestão), por interface de rede, sobre protocolo HTTPS;
- 3.4.48. Deverá suportar recursos de visualização de conexões simultâneas a partir de elementos de rede em quaisquer de suas interfaces de rede;
- 3.4.49. Deverá oferecer uma console única que permita acompanhar em modo gráfico o desempenho do equipamento (performance console) em termos de informações do sistema (uso de CPU e memória), informações sobre as interfaces de rede e informações sobre as políticas e regras de segurança;
- 3.4.50. Deverá possibilitar visualização on-line de usuários autenticados (authentication list) e de endereços IP bloqueados (blocked sites);
- 3.4.51. Deverá permitir a implementação e conexão com servidores de registros (logs) de maneira a centralizar o armazenamento dos registros gerados pelo equipamento, seguindo, necessariamente, as seguintes diretrizes mínimas:
 - 3.4.51.1. Compatibilidade com as plataformas Hiper-V e VMWare;
 - 3.4.51.2. O ISO e/ou Máquinas virtuais deverão estar incluídos na oferta, sem custos adicionais para a CONTRATANTE;
 - 3.4.51.3. O serviço de armazenamento de registros deve ser baseado em protocolo TCP/IP e utilizar uma base de dados SQL a qual deverá estar incluída como parte integral da proposta e sem custo adicional de licenciamento para a CONTRATANTE;
 - 3.4.51.4. Permitir ao administrador configurar o tamanho máximo da base de dados e respectivos alertas de uso do atingimento da capacidade configurada;
 - 3.4.51.5. Suportar a configuração de múltiplos servidores de logs;
 - 3.4.51.6. Os logs não poderão ser armazenados dentro dos FIREWALL NGFW ou UTM - Appliance. A transmissão dos logs para os appliance de armazenamento deverá ser de maneira cifrada (encriptada), sem que para tal se requeira a configuração de VPNs em Appliance separado e exclusivo;
 - 3.4.51.7. A CONTRATADA deverá fornecer equipamento exclusivo, servidor ou appliance, dedicado para o armazenamento de logs e geração de relatórios, cujas características estão descritas neste termo de referencia sem custo adicional para a CONTRATANTE;
 - 3.4.51.8. A CONTRATADA deverá fornecer, também armazenamento redundante de logs com retenção mínima de 365 dias em CLOUD. O acesso às informações deverá estar



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

protegidos e o seu acesso somente pela plataforma web disponível e da mesma marca da solução oferecida e sem custo adicional para a CONTRATANTE;

3.4.51.9. Deverá oferecer suporte à utilização opcional de serviços de logs de sistema (syslog) para armazenamento de logs;

3.4.51.10. Deverá ter ferramentas de software para a geração de relatórios a partir de múltiplos servidores de logs;

3.4.51.10.1. O serviço de geração de relatórios deverá permitir gerá-los em formatos PDF e CSV, além de permitir automatizá-los e com acesso por portal WEB para a visualização de relatórios.

3.4.52. A CONTRATADA deverá fornecer os serviços de instalação das licenças de uso e configuração dos equipamentos, bem como serviços de suporte constante no edital;

3.4.53. As licenças deverão ser autossuficientes para cada aquisição, isto é, devem permitir a habilitação de todos os recursos sem haver necessidade de novas aquisições;

3.4.54. A ferramenta de gerenciamento e administração de firewall deve permitir configuração, acompanhamento e implementação centralizados, capaz de possibilitar aos administradores, definir, distribuir e implementar um amplo número de serviços, atualizações e política de segurança para os equipamentos de firewall gerenciados pela solução;

3.4.55. Deverá permitir backup de configuração de sistemas (regras), aplicação de patches e novas atualizações de softwares, gerenciamento de modificações e análise de logs;

3.4.56. Deverá permitir a visão do status atual do (s) firewall, relatórios gráficos e atividades de rede por firewall;

3.4.57. Deverá possibilitar monitoramento por análise de dados ou por falhas, incluindo status do firewall e dos túneis VPN em tempo real;

3.4.58. Deverá permitir a visualização do gerenciamento e dos relatórios por meio de interfaces gráficas;

3.4.59. Deverá possibilitar o envio de alertas e notificações por e-mail;

3.4.60. Deverá possibilitar notificação e log das tentativas de ataques;

3.4.61. Deverá permitir a configuração de mais de um perfil de administrador e suas respectivas permissões.

3.4.62. O modelo de suporte oferecido pelo fabricante deverá ser Gold (24 x 7); A CONTRATADA deverá apresentar documento comprobatório deste modelo de suporte (contratado).

3.4.63. O fornecimento do software e/ou subscrições de segurança deverá ser sob a forma de LICENÇA DE USO e deverá atender integralmente a todas as funcionalidades descritas neste termo de referência, incluindo a atualização e suporte técnico, durante a vigência contratual;

3.4.63.1. O licenciamento deverá vigorar a partir da ativação das licenças e ter a capacidade de configuração dos equipamentos em alta disponibilidade no modo ativo/passivo e o suporte técnico integral na modalidade 7x24 com chamados ilimitados;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.4.63.2. Todo software/subscrição envolvido nesta contratação deverá permitir que seu licenciamento possa ser renovável ou prorrogável, a critério da CONTRATANTE, conforme o que é permitido e regido pela Lei de Licitações;
- 3.4.63.3. Os equipamentos deverão ser configurados e ter, no mínimo, as seguintes funcionalidades ativadas, simultaneamente: Controle de Aplicações, Gateway AntiVirus, IPS - Intrusion Prevention, Autoridade de Reputação na Web, AntiSpam, Filtro de conteúdo, Bloqueio de Ataque APT, Análise em Nuvem Sandbox, Proteção DNS com todos os detalhes e exigências definidas neste termo de referência.
- 3.4.63.4. Deverá apresentar a funcionalidade de proteção DNS, que poderá ser no software do FIREWALL NGFW/UTM e/ou em nuvem ou em equipamento à parte em forma de appliance, exclusivo para esse fim, do mesmo fabricante do FIREWALL NGFW/UTM ou de outro fabricante, não sendo aceita solução em equipamento genérico, PC e outros assemelhados.

3.5. FILTRO DE CONTEÚDO

- 3.5.1. Os equipamentos deverão suportar funcionalidades de filtro de conteúdo via subscrição e sem a necessidade do uso de outro equipamento adicional dedicado, respeitando, no mínimo, os seguintes aspectos:
 - 3.5.1.1. A opção de filtro deverá se categorizado com no mínimo 50 categorias pré-configuradas;
 - 3.5.1.2. Permitir que sejam configurados, os filtros, por usuário, grupo de usuários, endereço IP, grupo de endereços IP, sub-redes em horários específicos devendo também permitir estabelecer exceções quanto ao filtro de conteúdo, tanto no sentido de permissão (allow) quanto de bloqueio (deny) permitindo filtrar conteúdo em múltiplos idiomas;
 - 3.5.1.3. Deverá possibilitar a consulta a uma base de dados local (sobre interfaces privados ou opcionais - DMZ), e também consultas a uma base de dados externa
 - 3.5.1.4. Suportar, no mínimo, os protocolos HTTP e HTTPS;
 - 3.5.1.5. Possibilitar a inclusão, exclusão ou mudança de classificação de novos sites, ou sites existentes de forma on-line;
 - 3.5.1.6. A base de dados local deverá suportar atualização automática para que o filtro de conteúdo não necessite que um administrador classifique inicialmente os websites no banco de dados.

3.6. Antivírus de Gateway

- 3.6.1. Os equipamentos deverão possuir funcionalidades nativamente serviços de antivírus gateway via subscrição, sem a necessidade do uso de outro equipamento adicional dedicado, permitindo:
 - 3.6.1.1. A descompressão de arquivos nos formatos mais comuns (formatos: .rar, .tar, .tgz, .gz, .zip, .gzip, .jar, .chm, .lha, .pdf, container XML/HTML, container OLE - documentos do Microsoft Office, .cab, .arj, .ace, .bz2 - bzip e .swf) em até 5 níveis;
 - 3.6.1.2. A atualização das assinaturas da solução de antivírus deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador;
 - 3.6.1.3. Deverá suportar serviços de quarentena com remoção de arquivos infectados, bloqueio de conexão (drop) e bloqueio de endereços (block);



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.6.1.4. A solução de antivírus deverá suportar a detecção e bloqueio de código hostil, em geral, incluindo vírus, cavalos de troia (trojans), vermes (worms), spyware e rogueaware;
- 3.6.1.5. Suportar os protocolos HTTP, HTTPS, FTP, SMTP, TCP-UDP e POP3;

3.7. AntiSpam

- 3.7.1. Os equipamentos deverão suportar funcionalidades de AntiSpam via subscrição adicional, sem a necessidade de equipamento dedicado e suportar, no mínimo, o seguinte:
 - 3.7.1.1. Mecanismos de detecção de padrões recorrentes (RPD – Recurrent Pattern Detection) de modo a minimizar a necessidade de processamento no próprio equipamento;
 - 3.7.1.2. Serviços de quarentena de mensagens, bem como de modificação do campo de assunto (subject) da mensagem, bloqueio de conexão (drop) e recusa de mensagens de correio (deny);
 - 3.7.1.3. Integrar a detecção de epidemia de vírus na análise de spam (VOD – Virus Outbreak Detection);
 - 3.7.1.4. Bloquear spam em múltiplos idiomas;
 - 3.7.1.5. Bloquear tanto spam baseado em imagens quanto spam baseado em texto;
 - 3.7.1.6. Protocolos SMTP e POP3;
 - 3.7.1.7. A utilização de um serviço baseado no uso de recursos de “computação em nuvem” (cloud-based) de categorização de mensagens de correio eletrônico.

3.8. IPS

- 3.8.1. Os equipamentos deverão suportar funcionalidades de serviços de IPS via subscrição adicional, com modalidade de renovações sucessivas, sem a necessidade de equipamento dedicado, observando-se, minimamente, as seguintes características:
 - 3.8.1.1. Atualização das assinaturas de ataques utilizadas pela solução de IPS deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador;
 - 3.8.1.2. Classificação das ameaças por nível de risco / severidade dos ataques, com não menos que 5 (cinco) níveis e a possibilidade de geração de alarmes e registros de log;
 - 3.8.1.3. Bloqueio de conexão (drop) e de bloqueio de endereços fonte de ataques (block), bem como a geração de alarmes por nível de risco;
 - 3.8.1.4. Detecção de ameaças em todos os protocolos e portas, independentemente do tipo de regra de firewall utilizada;
 - 3.8.1.5. Configuração de exceções quanto à análise de tráfego de rede por assinaturas de ataques;
 - 3.8.1.6. O fabricante, para a funcionalidade IPS, deverá oferecer um portal na Internet, na forma de uma base de dados, onde possam ser obtidas informações adicionais sobre as assinaturas de ataques utilizadas na detecção de ameaças;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.8.1.7. Suportar por default (default threat protection), proteção imediata contra ataques e ameaças do tipo ataques de inundação (SYN flood attacks, IKE flood attacks, ICMP flood attacks, UDP flood attacks), ataques de falsificação (spoofing attacks), ataques de varredura de portas e endereços (port / address space probes) e ataques de negação de serviços (DoS) / negação de serviços distribuída (DDoS);
- 3.8.1.8. Possibilitar a configuração, pelo administrador, dos limites para a detecção de ataques de inundação (flood) e de ataques de negação de serviços (DoS / DDoS);

3.9. Controle de Aplicações

- 3.9.1. Os equipamentos deverão suportar a funcionalidade de serviços de controle de aplicações via subscrição adicional, sem a necessidade de equipamento dedicado, permitindo, no mínimo:
 - 3.9.1.1. A atualização das assinaturas de aplicações utilizadas pela solução de controle de aplicações deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador;
 - 3.9.1.2. Oferecer um portal, acessível via Internet, na forma de uma base de dados onde possam ser obtidas informações adicionais sobre as aplicações passíveis de serem controladas.

3.10. DEFINIÇÕES TÉCNICAS PARA ARMAZENAMENTO DE LOGs ON PREMISES

- 3.10.1. Todos os logs gerados pela solução FIREWALL NGFW/UTM em HA descrita nesse termo de referência deverão ser armazenados em equipamento exclusivo e diferente dos Appliance firewall, ou seja, em equipamento dedicado para esse fim, pois não será permitido o armazenamento dos logs dentro dos FIREWALL NGFW/UTM ou nos servidores de rede da CONTRATANTE;
- 3.10.2. A CONTRATADA deverá fornecer uma solução de armazenamento de logs em, pelo menos, 1 (um) equipamento físico, da mesma marca homologada e dedicado, possuir fonte redundante em cada equipamento para uso exclusivo de armazenamento de logs (banco de dados de logs) – configurando-se uma redundância de armazenamento.
- 3.10.3. Cada equipamento de armazenamento de logs deverá apresentar, pelo menos, 256 Gb RAM e capacidade de armazenamento mínimos de 2,8 TB líquidos em discos SSD Endurance Class acrescido de mais um disco de spare - backup para a solução oferecida, fonte redundante, no máximo 2U para rack de 19”;
- 3.10.4. Cada equipamento deverá apresentar 2 (duas) saídas de redes 10 SPF+, acompanhadas dos respectivos GBic’s que deverão ser conectadas em redundância ao switch do datacenter da CONTRATANTE;
- 3.10.5. Será de responsabilidade da CONTRATADA a configuração e a manutenção do desempenho desta solução de armazenamento de logs, Tipo e Tamanho do processador, sistema operacional e de banco de dados, placa de comunicação), desde que atenda aos volumes e prazos de retenção sem causar gargalos de processamento ao qual ele está destinado, sem CUSTOS adicionais para a CONTRATANTE;
 - 3.10.5.1. Durante a vigência contratual, a CONTRATADA deverá garantir esse serviço, mesmo que para isso tenha que substituir o equipamento em garantia, repondo peças ou software sem que isso traga nenhum ônus adicional à CONTRATANTE.
 - 3.10.5.2. O equipamento de hardware da solução, obrigatoriamente, deverá contemplar redundância de fonte de alimentação e unidades de armazenamento que aceite a configuração, de no mínimo, RAID 5;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.10.5.3. O equipamento deverá ser em Appliance ou ter a arquitetura específica construída para servidores de rede em gabinete de rack 19" e com altura máxima de 2U, cada equipamento;
- 3.10.5.4. Para ambos os casos acima descritos, (server ou appliance), somente será aceito equipamentos de marcas e fabricantes, cujo hardware esteja em produção na data da apresentação da proposta, com catálogo / datasheet / especificações técnicas, físicas e lógicas constando em site do fabricante que possam ser diligenciadas pela CONTRATANTE.
- 3.10.5.5. Os equipamentos deverão ser novos, sem uso anterior e ter suporte e garantia total do fabricante/fornecedor, para todos os seus componentes, de, no mínimo, de 60 (sessenta) meses;
- 3.10.5.6. Não serão aceitos equipamentos genéricos ou descontinuados;
- 3.10.5.7. Não serão aceitas soluções de armazenamento dos logs dentro do FIREWALL NGFW/UTM.

3.11. DEFINIÇÕES TÉCNICAS PARA A SEGURANÇA AVANÇADA PARA SERVIDORES DE REDE

- 3.11.1. A CONTRATADA deverá fornecer e instalar software para (servidores de rede) com o fornecimento de Licenças de Uso de Software para os ativos da CONTRATANTE e dos locais destinados objeto deste Edital. Para isso, a CONTRATADA deverá fornecer software destinados para tal finalidade. As especificações técnicas e funcionais estão detalhadas a seguir, e são MÍNIMAS e OBRIGATÓRIAS:
- 3.11.1.1. Todos os componentes que fazem parte da Solução de SEGURANÇA AVANÇADA PARA os SERVIDORES e deverão ser fornecidos por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes da solução do Firewall NGFW.
- 3.11.1.2. O conjunto de software que compõe esta solução para servidores deverá ser totalmente gerenciável através de um console de gerenciamento centralizado (em nuvem ou on-premise) e de forma que todos os produtos sejam monitorados através desta.

3.12. CONDIÇÕES DE FORNECIMENTO

- 3.12.1. Os equipamentos deverão ser entregues com todas as licenças necessárias para pleno funcionamento de suas funcionalidades descritas acima, incluindo segurança, roteamento avançado e SD-WAN e obrigatoriamente serem novos, sem uso anterior e estarem em linha de produção, não serão aceitos equipamentos descontinuados pelo fabricante.

3.13. TREINAMENTO

- 3.13.1. A CONTRATADA, obrigatoriamente, deverá treinar a equipe técnica da CÂMARA MUNICIPAL DE RIBEIRÃO PRETO na implantação de todas as soluções descritas no objeto deste termo de referência e seus anexos e sempre que houver atualização tecnológica da solução enquanto vigorar o contrato, cujo escopo deverá abranger toda a solução contratada:
- 3.13.1.1. O treinamento consiste na transferência de tecnologia (de, no mínimo, 24 horas de treinamento), em curso(s) ministrado(s) por profissional(ais) certificado(s) do(s) fabricante(s) das soluções entregues e implantadas.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

3.13.1.2. Deverão ser treinados, no mínimo, 5 (cinco) técnicos da CONTRATANTE;

3.13.1.3. A CONTRATADA deverá possuir Engenheiro de Sistemas certificado pelo fabricante do FIREWALL (NGFW) de instrutor oficial da solução ofertada.

3.13.2. A CONTRATADA, obrigatoriamente, deverá entregar, após o treinamento, em até 90 dias da data de assinatura do contrato, uma documentação AS-BUILT da solução, contendo todos os componentes listados, com os firmwares utilizados, parâmetros adotados, senhas de administrador, diagramas, catálogos dos produtos, regras adotadas – segurança, mecanismos de chamados técnicos e documentação técnica. Esta documentação deverá ser entregue em mídia digital em arquivos abertos e editáveis.

3.13.3. Os profissionais, da CONTRATANTE, que participarem do treinamento deverão receber um certificado oficial da marca da solução treinada.

3.13.4. O treinamento deverá ser ministrado no Centro de Treinamento nas dependências da CONTRATADA ou em outro local acordado entre as partes, desde que seja na Grande São Paulo, sendo todas as despesas de material didático, equipamentos, aplicativos e outros utilizados no treinamento de responsabilidade da CONTRATADA. O treinamento, por ser oficial, poderá ser ministrado pela CONTRATADA certificada ou pelo fabricante.

3.14. IMPLANTAÇÃO e LOCAL de INSTALAÇÃO

3.14.1. A implantação das soluções do escopo do Edital deverá ser realizada no prazo de até 90 (noventa) dias da contratação, mediante entrega de cronograma, descrevendo as fases do projeto de implantação. Esse cronograma deverá ser aprovado pela CONTRATANTE, sendo a implantação iniciada somente após à aprovação.

3.14.2. As fases do projeto, bem como os respectivos documentos mínimos necessários para cada fase, estão descritas a seguir:

3.14.2.1. Relatório de organização e planejamento com precedências e matriz de responsabilidade;

3.14.2.2. Aspectos de migração e contingência;

3.14.2.3. Implantação: Relatório de implantação;

3.14.2.4. Testes: relatório de testes, com evidências de sucesso e falhas.

3.14.3. A implantação será realizada pela CONTRATADA e o planejamento e a execução de todas as atividades envolvidas serão acompanhados, autorizados e coordenados por servidores designados pela CONTRATANTE.

3.14.4. A implantação, quando realizada no ambiente de produção, poderá envolver, a critério da CONTRATANTE, atividades fora do horário de expediente (horários noturnos ou em finais de semana e feriados).

3.14.5. A CONTRATADA será responsável por efetuar as atividades de integração da solução ofertada com o ambiente operacional da CONTRATANTE, sem provocar qualquer prejuízo aos serviços desta.

3.14.6. O prazo de garantia, manutenção e suporte técnico dos produtos e serviços de implantação deverão vigorar no mesmo prazo da vigência contratual.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.14.7. A implantação das soluções deverá ser executada tecnicamente por profissionais certificados, observando-se os requisitos de certificação técnica constante neste Termo de Referência.
- 3.14.8. Após a implantação da solução e estando tudo de acordo com este Termo de Referência e seus Anexos, a CONTRATANTE irá emitir o termo de aceite da implantação.
- 3.14.9. A CONTRATADA deverá nomear um preposto para a interlocução com a CONTRATANTE, para a apresentação de resultados da prestação dos serviços, esclarecer dúvidas sobre os serviços prestados, análise e entendimento das configurações e procedimentos implementados.
- 3.14.10. A CONTRATADA deverá apresentar um relatório mensal das atividades desempenhadas, suportes, problemas ocorridos, pendências e justificativas. Este relatório deverá ser enviado ao gestor do contrato.

3.15. Gerenciamento, Monitoramento e Serviços de Suporte Técnico

- 3.15.1. O funcionamento, suporte técnico e operação plena das soluções do escopo deverá obrigatoriamente ser provida pela CONTRATADA, sem ônus adicional à CONTRATANTE, com, no mínimo:
 - 3.15.1.1. Atualização das versões do software e firmware fornecido, se novas versões forem disponibilizadas pelos fabricantes.
 - 3.15.1.2. Atualização (inclusive na instalação ou nova instalação, se for o caso, ou atualização de versões/releases) e resolver problemas de incompatibilidade com outro componente da infraestrutura de TI.
 - 3.15.1.3. O serviço de suporte poderá ser presencial e/ou remoto. Se remoto, desde que seja possível a resolução do problema conforme o SLA dos acordos de níveis de serviço, para os prazos e severidade de atendimentos.
 - 3.15.1.4. Os firmwares só poderão ser atualizados após serem testados pela CONTRATADA, ficando esta responsável pelo sucesso da nova instalação ou a reversão da ação, caso seja necessária.
- 3.15.2. Em caso de necessidade de melhoria, nova instalação, ou nova versão ou correção, a CONTRATADA deverá prestar suporte quanto a essas operações, assim como atuar on-site, se necessário ou mediante solicitação da CONTRATANTE.
- 3.15.3. O monitoramento deverá ser em regime de operação 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, inclusive feriados, fins de semana e dias facultativos de folga (ponte entre feriados), sobre os serviços, garantindo o melhor resultado nas aplicações da CONTRATANTE e deverá abranger todas as atividades desta prestação de serviços.
- 3.15.4. A CONTRATADA deverá realizar as configurações necessárias para interligação de seu SOC (Security Operation Center - Centro de Operações de Segurança) às instalações da CONTRATANTE, por meio de uma linha de comunicação privativa de dados (LP) ou por meio de uma VPN segura com a finalidade exclusiva de realizar a prestação do serviço, durante a vigência do contrato. A contratação e instalação de uma LP, caso seja necessária, é parte integrante da solução e responsabilidade da CONTRATADA.
- 3.15.5. Todo acesso de monitoração do ambiente, e eventuais intervenções remotas, pela CONTRATADA deverão ser feitos exclusivamente por esse serviço de comunicação de dados.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.15.6. Os processos utilizados pela equipe do SOC devem seguir as melhores práticas de mercado. O ITIL (Information Technology Infrastructure Library), deve ser utilizado como modelo de referência pelo SOC para operação e gerenciamento de processos e serviços de TI e observando-se os requisitos de certificação técnica constante neste Termo de Referência.
- 3.15.7. A CONTRATADA deverá comprovar que possui profissionais certificados para a solução ofertada de no mínimo 3 (três) técnicos certificados na solução FIREWALL NGFW, sendo que com pelo menos possuírem a certificações, de 01 técnico com certificação de instrutor para a solução de FIREWALL NGFW, 02 técnicos com certificação para a solução de FIREWALL NGFW, 01 técnico deve possuir a certificação ITILv3. Podendo um técnico possuir mais de uma certificação válida das solicitadas acima.
- 3.15.8. Dentre outras, são as ações principais e exigidas do SOC da CONTRATADA, incluídas:
- 3.15.8.1. Acesso ao SOC controlado por mecanismos de autenticação forte e ambiente isolado de outros que não sejam destinados à operacionalização e controle de segurança;
 - 3.15.8.2. Política de acesso lógico: possuir autenticação forte no acesso aos equipamentos que estarão nas dependências da CONTRATANTE;
 - 3.15.8.3. Possuir políticas definidas para criação, exclusão e manutenção de chaves, senhas e perfis de acesso.
 - 3.15.8.4. Fornecer apoio técnico necessário para realizar o diagnóstico de eventos de falha em seus ativos de segurança. Através da análise dos logs do equipamento, o SOC deverá determinar se houve alguma avaria em um dos componentes de hardware da solução e identificar a necessidade ou não de sua substituição.
 - 3.15.8.5. Efetuar e gerenciar o processo de RMA (sigla em inglês de return merchandise authorization).
 - 3.15.8.6. Efetuar toda a interface com o fabricante, para o RMA e substituição do componente danificado.
 - 3.15.8.7. Efetuar a monitoração constante da capacidade e da disponibilidade da infraestrutura de segurança contratada.
 - 3.15.8.8. Ter uma arquitetura de monitoração, baseada em solução que utiliza o protocolo SNMP para realizar os healthchecks (verificações de “saúde” da infraestrutura de TI do contexto, visando identificar falhas e melhorias de curto e longo prazos).
 - 3.15.8.9. Processar e disponibilizar em relatórios mensais os dados coletados.
 - 3.15.8.10. Identificar que o componente atingiu certo nível de utilização (threshold).
 - 3.15.8.11. Alertar e encaminhar alertas para os técnicos responsáveis pela administração.
 - 3.15.8.12. Acompanhar a saúde dos dispositivos supervisionando-os 24x7.
 - 3.15.8.13. Comunicar à CONTRATANTE, anomalias quando um componente monitorado apresentar índices não usuais.
 - 3.15.8.14. Prover a monitorização da saúde dos dispositivos por meio de um número predefinido de itens, pelo menos, conforme abaixo:
 - 3.15.8.14.1. Utilização da CPU;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.15.8.14.2. Utilização de memória;
 - 3.15.8.14.3. Utilização do disco;
 - 3.15.8.14.4. Estado das interfaces de rede;
 - 3.15.8.14.5. Temperatura;
 - 3.15.8.14.6. Número de sessões de VPN;
 - 3.15.8.14.7. Número de pacotes perdidos;
 - 3.15.8.14.8. Número de pacotes negados;
 - 3.15.8.14.9. Número de conexões;
 - 3.15.8.14.10. Estado do cluster.
- 3.15.9. Estas verificações serão ativadas no momento de implantação do serviço, utilizando definições padrão de thresholds.
- 3.15.10. Estes valores poderão ser ajustados, caso necessário, a fim de identificar quais situações normalmente não correspondem à normalidade dos serviços.
- 3.15.11. A CONTRATANTE poderá acompanhar, através do console, os indicadores em tempo real.
- 3.15.12. Resolução nos incidentes de segurança que ocorrem nos elementos administrado (s), detectados pelo monitoramento ou que sejam informados pela CONTRATANTE.
- 3.15.13. Efetuar tarefas operacionais básicas, tais como executar backup/restore de configurações e gerenciamento do ambiente contratado.
- 3.15.14. Garantir o correto funcionamento dos dispositivos administrados contratados.
- 3.15.15. Manter e atualizar o ambiente contratado com o software do dispositivo na versão mais atual recomendada pelo fabricante.
- 3.15.16. Efetuar aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança.
- 3.15.17. Efetuar atualização de software e patches ao produto contratado somente se e quando autorizada pela CONTRATANTE, através do processo de gestão da mudança.
- 3.15.18. Informar à CONTRATANTE dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração.
- 3.15.19. Atender as dúvidas e solicitações de segurança da CONTRATANTE.
- 3.15.20. Acompanhar e encaminhar os chamados por meio de ferramenta Web.
- 3.15.21. Acompanhar tendências de ataques e vulnerabilidades.
- 3.15.22. No caso de detecção de algum incidente de segurança, a CONTRATADA deverá notificar a CONTRATANTE dentro do período estabelecido no Acordo de Níveis de Serviços, para serem tomadas as medidas corretivas, técnicas e legais necessárias.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 3.15.23. São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da CONTRATANTE.
- 3.15.24. A CONTRATADA comunicará imediatamente a CONTRATANTE, para poderem ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente do CONTRATANTE, em que seja evidenciada a insistência, por parte da entidade mal-intencionada.
- 3.15.25. A CONTRATADA disponibilizará todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs etc.) para serem apurados os incidentes de segurança reportados.

3.16. CONFIDENCIALIDADE DA INFORMAÇÃO

- 3.16.1. Todas as informações que trafegam nos equipamentos, bem como toda e qualquer informação originada pela CONTRATANTE e que a CONTRATADA venha a ter acesso serão consideradas “Informações Confidenciais”.
- 3.16.2. Para a prestação dos serviços do escopo deste Edital, a CONTRATADA deverá assinar o termo de confidencialidade definido em Anexo específico. a este Termo de Referência.
- 3.16.3. A CONTRATADA se obriga a devolver ou destruir imediatamente todo o material que contenha Informações Confidenciais, tão logo ocorra a rescisão ou término da vigência do contrato. firmado entre as partes.
- 3.16.4. A CONTRATANTE se compromete a tratar como confidenciais todas as informações de propriedade da CONTRATADA, que vier a ter conhecimento, durante a vigência do contrato.

3.17. ACORDO DE NÍVEIS DE SERVIÇO – SLA (SERVICE LEVEL AGREEMENT)

- 3.17.1. O nível dos serviços prestados será medido com base nas seguintes métricas:

Métrica SLA Aplica-se a:

Métrica	SLA	Aplica-se a:
Tempo de Atendimento	95%	Consultas, requisições e incidentes.
Tempo de Resposta	95%	Consultas, requisições e incidentes
Tempo de Notificação	95%	Consultas, requisições e incidentes.
Tempo de Resolução	95%	Consultas e requisições.

- 3.17.2. Os SLO's serão estabelecidos de acordo com a severidade do incidente ocorrido, conforme descrito no quadro abaixo:

Crítico	Evento que indisponibiliza os serviços de um ativo classificado como crítico
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibiliza os serviços de um ativo não crítico



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

Médio	Evento que degrada os serviços de um ativo classificado como não crítico
Baixo	Evento que não afeta os serviços

3.17.3. Abaixo os tempos de atendimento:

ITEM	SERVIÇO	DEFINIÇÃO	CRÍTICO	ALTO	MÉDIO	BAIXO
1	Todos, exceto consultas	Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	30 min	1h	2h	4h
2	Todos, exceto consultas	Tempo de resposta a partir da comunicação do cliente até que o SOC faça o primeiro diagnóstico	1,5h	2h	4h	8h
3	Todos, exceto consultas	Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do chamado	4h	6h	12h	24h
4	Consultas	Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	-	4h	6h	8h
5	Consultas	Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do problema	-	16h	20h	30h

GARANTIA

- a. A garantia em sua totalidade e da maneira como solicitada, deverá ser obrigatoriamente de responsabilidade unicamente do fabricante/fornecedor do equipamento.
- b. O fabricante/fornecedor do equipamento deverá atender, durante o período de garantia, a chamados de suporte técnico na modalidade 24x7x365, ou seja, 24 por dia, 7 dias por semana, devendo deixar o equipamento totalmente operacional após o chamado;
- c. A substituição de componentes ou peças decorrentes da garantia não poderá gerar quaisquer ônus para a CONTRATANTE. Toda e qualquer peça ou componente consertado, ou substituído, deverá ficar automaticamente garantido até o final do prazo de garantia do objeto;
- d. Todo o equipamento e acessórios fornecidos deverão possuir garantia total de funcionamento **mínima de 60 (sessenta) meses**, contados a partir da data do aceite dos equipamentos.
- e. O período de garantia citado acima compreende a garantia legal e o fornecimento de pacote(s) adicional(ais) de garantia (extensão de garantia) em número suficiente para a cobertura do prazo mencionado neste termo de referência.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- f. Durante o tempo de vigência dos serviços de garantia e suporte técnico do fabricante/fornecedor, os custos de deslocamento, troca de peças danificadas entre outros custos são de responsabilidade do FABRICANTE/FORNECEDOR, não podendo gerar qualquer ônus ao CONTRATANTE;

4. REQUISITOS DA CONTRATAÇÃO

Da exigência de catálogo ou ficha técnica

- 4.1. Será exigida a apresentação do catálogo e/ou ficha técnica do equipamento ofertado

Da exigência de carta de solidariedade

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

Subcontratação

- 4.3. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

- 4.4. 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.

5. MODELO DE EXECUÇÃO DO OBJETO

Condições de Entrega

- 5.1. O prazo máximo de entrega do bem é de 90 (noventa) dias corridos, contados da data determinada na Autorização de Fornecimento, em remessa única, podendo ser prorrogado por no máximo 30 (trinta) dias, desde que justificado e solicitado pelo fornecedor.
- 5.2. Caso não seja possível a entrega no prazo máximo estipulado, a empresa vencedora deverá comunicar as razões respectivas com pelo menos 3 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.
- 5.3. Os bens deverão ser entregues no seguinte endereço e horário indicados abaixo:
- 5.3.1. Setor de Patrimônio da Câmara Municipal de Ribeirão Preto, sito à Avenida Jerônimo Gonçalves, 1200 – 1º. Andar - Centro, CEP: 14.010-907, Ribeirão Preto – SP.
- 5.3.2. O horário para entrega dos produtos será de segunda-feira a sexta-feira, das 09h00min às 11h00min ou das 14h00min às 17h00min, com exceção de feriados e pontos facultativos apresentados em calendário oficial (disponível em <https://www.ribeiraopreto.sp.gov.br/portal/principal/feriados>).



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

Garantia do objeto

- 5.4. O prazo de garantia contratual dos bens, é de, no mínimo, 60(sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.
- 5.4.1. A garantia será prestada com vistas a manter o equipamento fornecido em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.
- 5.4.2. A garantia em sua totalidade e da maneira como solicitada, deverá ser obrigatoriamente de responsabilidade unicamente do fabricante/fornecedor do equipamento.
- 5.4.3. A garantia abrange a realização da manutenção corretiva, de acordo com as normas técnicas específicas.
- 5.4.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- 5.4.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.
- 5.4.6. O fabricante/fornecedor do equipamento deverá atender, durante o período de garantia, a chamados de suporte técnico na modalidade 24x7x365, ou seja, 24 por dia, 7 dias por semana, devendo deixar equipamento totalmente operacional após o primeiro atendimento do chamado.
- 5.4.7. A substituição de componentes ou peças decorrentes da garantia não poderá gerar quaisquer ônus para a CONTRATANTE. Toda e qualquer peça ou componente consertado, ou substituído, deverá ficar automaticamente garantido até o final do prazo de garantia do objeto.
- 5.4.8. Todo o equipamento e acessórios fornecidos deverão possuir garantia total de funcionamento mínima de 60 (sessenta) meses, contados a partir da data do aceite dos equipamentos.
- 5.4.9. O período de garantia citado acima compreende a garantia legal e o fornecimento de pacote(s) adicional(ais) de garantia (extensão de garantia) em número suficiente para a cobertura do prazo mencionado.
- 5.4.10. Durante o tempo de vigência dos serviços de garantia e suporte técnico do fabricante, os custos de deslocamento, troca de peças danificadas entre outros custos são de responsabilidade do FABRICANTE/FORNECEDOR, não podendo gerar qualquer ônus ao CONTRATANTE.

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 do Decreto Municipal nº 64, de 2023, 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.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 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.

Fiscalização

- 6.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.
 - 6.5.1. No caso de instrumento equivalente a fiscalização será acompanhada pelo setor requisitante do objeto.
 - 6.5.2. Constituem atividades a serem exercidas pelo(s) fiscal(is):
 - 6.5.2.1. Acompanhar e registrar as ocorrências relativas à execução contratual, informando à unidade responsável pela gestão de contratos do setor requisitante, aquelas que podem resultar na execução dos serviços e obras ou na entrega de material de forma diversa do objeto contratual, tomando as providências necessárias à regularização, por parte da contratada, das faltas ou defeitos observados;
 - 6.5.2.2. Recepcionar, conferir e atestar da contratada os documentos necessários ao pagamento, previstos no termo de contrato e nas exigências da Secretaria Municipal da Fazenda que disciplina os procedimentos para a liquidação e pagamento;
 - 6.5.2.3. Verificar se o prazo de entrega, as quantidades e a qualidade dos serviços, das obras ou do material encontram-se de acordo com o estabelecido no instrumento contratual;
 - 6.5.2.4. Manifestar-se formalmente, quando consultado, sobre a prorrogação, rescisão ou qualquer outra providência que deva ser tomada com relação ao contrato que fiscaliza;
 - 6.5.2.5. Consultar a unidade requisitante dos serviços, obras ou materiais sobre a necessidade de acréscimos ou supressões no objeto do contrato, se detectar algo que possa sugerir a adoção de tais providências;
 - 6.5.2.6. Propor medidas que visem à melhoria contínua da execução do contrato;
 - 6.5.2.7. Exercer qualquer outra incumbência que lhe seja atribuída por força de previsão normativa.

Gestão

- 6.6. Constituem atividades de gestão dos contratos:
 - 6.6.1. Acompanhar as contratações a partir da lavratura do ajuste até sua implantação, em se tratando de prestação de serviços ou da entrega de material, no caso de fornecimento parcelado que culmine em instrumento contratual;
 - 6.6.2. Ter conhecimento da íntegra do contrato firmado, bem como de seu cronograma físico-financeiro, bem como controlar a utilização dos recursos orçamentários destinados ao amparo das despesas dele decorrentes;



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 6.6.3. Fazer constar do processo administrativo correspondente as informações e os documentos necessários à formalização do contrato, inclusive quando o seu instrumento for substituído;
- 6.6.4. Executar as diligências e providenciar a tramitação necessária que precedem a assinatura dos contratos, termos aditivos e de apostilamento, termos de rescisão contratual, termos de recebimento contratual e afins pela autoridade competente;
- 6.6.5. Expedir a ordem serviço ou autorização de fornecimento;
- 6.6.6. Garantir acesso do contrato firmado, da proposta do contratado, do edital e dos demais documentos pertinentes ao fiscal do contrato, visando subsidiar o exercício da respectiva fiscalização;
- 6.6.7. Verificar e aprovar, com base na legislação vigente, a regularidade da documentação exigida como condição de assinatura do contrato, bem como mantê-la atualizada;
- 6.6.8. Atuar conjuntamente com o fiscal do contrato, verificando a existência de adequado acompanhamento à execução do ajuste;
- 6.6.9. Manter o controle de todos os prazos relacionados aos contratos e informar à autoridade competente, em tempo hábil, a necessidade de prorrogação contratual ou de realização de nova contratação, conforme o caso;
- 6.6.10. Dar início aos procedimentos para a prorrogação dos contratos com a antecedência necessária, levando em conta as informações prestadas pela unidade requisitante do serviço e pelo fiscal do contrato, os preços de mercado e demais elementos que auxiliem na identificação da proposta mais vantajosa para a Administração;
- 6.6.11. Verificar se a documentação necessária ao pagamento, encaminhada pelo fiscal do contrato, está de acordo com o disposto no contrato e nas exigências da Secretaria Municipal da Fazenda para liquidação e pagamento;
- 6.6.12. Verificada a existência de qualquer infração contratual, constatada pelo gestor ou unidade gestora, ou apontada pelo fiscal, relatar os fatos e iniciar o procedimento de proposta de aplicação de penalidade, nos termos previstos no instrumento contratual, bem como informar, com a devida justificativa técnica, às autoridades responsáveis, os fatos que ensejam a aplicação de sanções administrativas em face da inexecução parcial ou total do contrato, observada a legislação vigente;
- 6.6.13. Apurar situação de inadimplemento com relação às obrigações trabalhistas, ao tomar conhecimento dela por qualquer meio, independentemente de ação judicial, e adotar, garantido o contraditório e a ampla defesa, as providências previstas em lei e no contrato;
- 6.6.14. Executar as atividades inerentes à completa gestão do contrato firmado, inclusive no que se refere à manutenção das condições de regularidade fiscal, previdenciária e trabalhista da contratada;
- 6.6.15. Emitir, quando solicitado, as declarações, certidões e atestados de capacidade técnica em relação à execução dos serviços e aquisições contratados, consultado o fiscal do contrato;
- 6.6.16. Repassar as informações sobre vigência e necessidade de prorrogação do ajuste para a área responsável pelo plano de contratações anual;
- 6.6.17. Exercer qualquer outra incumbência que lhe seja atribuída por força de previsão normativa.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

- 7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega com as devidas instalações e configurações, devendo estar em pleno funcionamento, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(s) responsável(is) pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta (Art 117, inciso II, alínea "a" do Decreto Municipal nº 64, de 2023).
- 7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades e sem custos adicionais ao Município de Ribeirão Preto.
- 7.3. O recebimento definitivo ocorrerá mediante termo detalhado que comprove o atendimento das exigências editalícias e contratuais, por servidor ou comissão designada pela autoridade competente, no prazo de até 5 (cinco) dias, a contar do recebimento provisório (Art 117, inciso II, alínea "b" do Decreto Municipal nº 64, de 2023).
- 7.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências editalícias e contratuais.
- 7.5. 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.
- 7.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.
- 7.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.
- 7.8. O produto (marca, qualidade, etc) não poderá ser substituído, sem a devida autorização do contratante. Em caso de substituição, a empresa deverá, antes de efetuar a entrega, enviar o pedido ao Órgão Requisitante com as devidas justificativas.
- 7.9. O contratante reserva-se o direito de não receber o produto que estiver em desacordo com o previsto neste instrumento, podendo cancelar o pedido e aplicar as sanções cabíveis, nos termos da legislação vigente.

Liquidação

- 7.10. O(s) contratado(s) apresentará(ão) ao Órgão Requisitante a Nota Fiscal Eletrônica de Compra referente ao fornecimento efetuado.
- 7.11. Para a Nota Fiscal Eletrônica de Compras deverá ser observado o protocolo ICMS 42 de 03 de julho de 2009: ficam obrigados a emitir Nota Fiscal Eletrônica – NF-e, modelo 55, em substituição à Nota Fiscal, modelo 1 ou 1-A, a partir de 1º de dezembro de 2010, os contribuintes que, independentemente



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

da atividade econômica exercida, realizem operações destinadas à Administração Pública direta ou indireta.

7.12. Para o atendimento da Lei Municipal nº 14.303 de 21 de março de 2019, a Contratada deverá enviar a Nota Fiscal em formato PDF, acompanhada de formato XML se houver, com todas as informações, incluindo a chave de identificação da Nota Fiscal Eletrônica, para o endereço de e-mail: almoxarifado@camararibeiraopreto.sp.gov.br, patrimonio@camararibeiraopreto.sp.gov.br, contabilidade@camararibeiraopreto.sp.gov.br, como condição para aprovação da respectiva Nota Fiscal.

7.13. Para fins de liquidação, o Órgão Requisitante deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.13.1. o prazo de validade;

7.13.2. a data da emissão;

7.13.3. os dados do contrato e do órgão contratante;

7.13.4. o período respectivo de execução do contrato;

7.13.5. o valor a pagar; e

7.13.6. eventual destaque do valor de retenções tributárias cabíveis.

7.14. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

Pagamento

7.15. O pagamento será efetuado no prazo de até 5 (cinco) dias contados após a comprovação do fornecimento do objeto, nas condições exigidas, bem como, após a aprovação dos respectivos documentos fiscais pelo Órgão Fiscalizador.

7.16. 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 IPC-FIPE de correção monetária.

7.17. O pagamento será realizado exclusivamente por meio de depósito bancário, para crédito em banco, agência e conta corrente indicados pelo contratado.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de contratação, sob a forma de PREGÃO ELETRÔNICO, com adoção do critério de julgamento pelo MENOR PREÇO

Forma de fornecimento

8.2. O fornecimento do objeto será integral

Exigências de habilitação



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

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

Habilitação jurídica

- 8.4.** Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
- 8.5.** 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>;
- 8.6.** 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;
- 8.7.** 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.
- 8.8.** Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;
- 8.9.** 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.
- 8.10.** 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.
- 8.11.** Para a participação de cooperativas, será exigida a seguinte documentação complementar:
- 8.11.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;
- 8.11.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;
- 8.11.3. A comprovação do capital social proporcional ao número de cooperados necessários à execução contratual;
- 8.11.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;
- 8.11.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e
- 8.11.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.11.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

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

Habilitação fiscal, social e trabalhista

8.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

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

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

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

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

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

8.19. Caso o fornecedor seja considerado isento dos tributos Estadual/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.

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

Qualificação Econômico-Financeira

8.21. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de sociedade simples;

8.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

Qualificação Técnica

8.23. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de atestados ou certidões, por pessoas jurídicas de direito público ou privado, regularmente emitido(s) pelo conselho profissional competente, quando for o caso.



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

- 8.23.1. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 8.23.2. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 8.23.3. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.
- 8.24.** Apresentar, pelo menos, 1 (um) analista com certificado ITILv3, certificado este que deverá ser entregue pela LICITANTE, por ocasião da assinatura do contrato, conforme Súmula 25 do Tribunal de Contas do Estado de São Paulo, na assinatura de contrato.
- 8.25.** A LICITANTE deve constar no site do fabricante como canal autorizado a fornecer e instalar os produtos da marca. Deverá ser apresentado a prova no próprio website da fabricante, condição que garanta a execução da instalação dos produtos bem como a sua origem e a qualidade, na assinatura de contrato.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

- 9.1. O custo estimado total da contratação é de R\$ 427.520,20 (quatrocentos e vinte e sete mil, quinhentos e vinte reais e vinte centavos), conforme custos unitários apostos na tabela abaixo.

ITEM	ESPECIFICAÇÃO	QUANTIDADE	VALOR UNITÁRIO ESTIMADO	TOTAL ESTIMADO DO ITEM
1	Firewall de Próxima Geração - Next-Generation Firewall (NGFW) ou UTM - Solução em cluster de alta disponibilidade (HA) ativo/passivo incluídas as licenças de uso do software de segurança com todas as funcionalidades descritas e ativas, com garantia, suporte técnico e atualização, por 60 meses.	1	R\$ 261.427,00	R\$ 261.427,00
2	Appliance ou servidores exclusivos para armazenamento de logs incluídas as licenças de uso de software, com garantia, suporte técnico e atualização, por 60 meses.	1	R\$ 137.851,53	R\$ 137.851,53
3	Licenças de uso de software para servidores de rede em ambiente virtual e físico com todas as funcionalidades descritas e ativas, com suporte técnico e atualização de software, enquanto vigorar o contrato.	25	R\$ 1.129,67	R\$ 28.241,67
Total (Valor Global) estimado				R\$ 427.520,20



Câmara Municipal de Ribeirão Preto

Estado de São Paulo

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. A contratação será atendida pela seguinte dotação:

- I) Unidade Orçamentária: Câmara Municipal de Ribeirão Preto;
- II) Vínculos: Coordenadoria Administrativa;
- III) Classificações Funcionais: 4.4.90.52.00 – Equipamentos e Material Permanente e 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação PJ;
- IV) Fontes de Recursos: Tesouro;
- V) Transferência voluntária: não.

Ribeirão Preto, 11 de novembro de 2025.

Câmara Municipal de Ribeirão Preto
VAURLEI DE ALMEIDA JUNIOR
SETOR DE T.I.

Câmara Municipal de Ribeirão Preto
CHAFIK FERREIRA SCALON
COORDENADOR ADMINISTRATIVO