Whats 17/07

PREGÃO ELETRÔNICO PMI 19-2023

CONTRATO Nº 118-2023
VIGÊNCIA: 12 MESES

O MUNICÍPIO DE IBIRUBÁ-RS, Pessoa Jurídica de Direito Público, com sede à Rua Tiradentes, n.º 700, inscrito no CNPJ sob n.º 87.564.381/0001-10, neste ato representado pelo Prefeito, Sr. **ABEL GRAVE**, brasileiro, residente e domiciliado nesta cidade, com documento de identidade RG sob n.º 5064763534 e CPF sob nº 000.264.290-55, de ora em diante denominado apenas como **CONTRATANTE,** e do outro lado a Empresa **COPREL TELECOM LTDA** - CNPJ nº 12.388.471/0001-06 - Endereço Avenida Brasil, 2530 – Bairro Hermani – Ibirubá – RS – CEP 98.200-000 – contato 54 3324-5800, representada por **GABRIEL DE SOUZA**, Carteira de identidade nº 6085199096, CPF nº 013.691.920-02, na presença das testemunhas abaixo firmadas, acordam e justam firmar o presente contrato, observadas as condições do Edital que regem o Pregão e aquelas enunciadas nas cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO
1.1 - É objeto deste instrumento a contratação de Empresa destinada ao fornecimento de soluções de segurança de redes composta por dispositivo dedicado para segurança tipo (NGE_Next_Security), para prover segurança e proteção de rede de computadores de todos os setores da Prefeitura, em regime de comodato cobrindo segurança dessas unidades, com dispositivos físicos, incluindo treinamento, operação inicial, configuração, suporte técnico e monitoramento, para atender as necessidades do Departamento de Tecnologia da Informação e Comunicação, em observância com o disposto no presente Edital e nos Elementos Técnicos, que passam a fazer parte integrante do mesmo, para todos os efeitos.

CLÁUSULA SEGUNDA - DO PREÇO E DA FORMA DE PAGAMENTO
2.1 - Pelo fornecimento do objeto ora contratado, a Contratante pagará à Contratada o valor total estabelecido no Anexo I deste instrumento.
2.1.2 - O pagamento das despesas decorrentes do fornecimento a que se refere a presente licitação, será feito através de depósito bancário ou conforme determinado pela Tesouraria do Município, até o 10º(décimo) dia após a prestação dos serviços, a partir da apresentação das respectivas Notas Fiscais/Faturas, devidamente recebidas, atestadas e processadas segundo a legislação. No ato da entrega dos Serviços, a contratada deverá fornecer os dados bancários da conta jurídica (banco, agência e nº. da conta) para depósitos referentes aos pagamentos, conforme exigência da Tesouraria.
2.2 - O valor estabelecido no contrato poderá ser reajustado, devendo a empresa solicitar recomposição do preço para preservar o equilíbrio econômico-financeiro do contrato de acordo com o artigo 65 de lei 8.666/93, com as devidas justificativas e Planilhas de Preços comprovando tal recomposição.
2.3 - A liberação dos recursos será através de depósito bancário em conta da CONTRATADA, ou conforme estipulado pela Tesouraria Municipal.
2.4 - A Nota Fiscal somente será liberada quando o cumprimento do contrato estiver em total conformidade com as especificações exigidas pelo Município.
2.5 - Na eventualidade de aplicação de multas, estas deverão ser liquidadas simultaneamente com parcela vinculada ao evento cujo descumprimento der origem à aplicação da penalidade.
2.6 - As Notas Fiscais deverão ser emitidas em moeda corrente do país.
2.6.1 Juntamente com a Nota Fiscal, a contratada deverá apresentar o Certificado de regularidade do FGTS, Negativa Trabalhista e Negativa Unificada (União e INSS), porventura vencidas.
2.7 - O CNPJ da contratada constante da nota fiscal e fatura deverá ser o mesmo da documentação apresentada no procedimento licitatório.
2.8 - Nenhum pagamento será efetuado ao proponente vencedor enquanto pendente de liquidação quaisquer obrigações financeiras que lhe foram impostas, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

CLÁUSULA TERCEIRA - DO CONTRATO E DO PRAZO
3.1 - O contrato regular-se-á, no que concerne a sua alteração, inexecução ou rescisão, pelas disposições da Lei nº. 8.666, de 21 de junho de 1.993 observadas suas alterações posteriores, pelas disposições do Edital e pelos preceitos do direito público.

3.2 - O contrato poderá, com base nos preceitos de direito público, ser rescindido pelo MUNICÍPIO a todo e qualquer tempo, independentemente de interpelação judicial ou extrajudicial, mediante simples aviso, observadas as disposições legais pertinentes.
3.3 - Farão parte integrante do contrato às condições previstas no Edital e na proposta apresentada pelo adjudicatário.
3.4 – O Contrato terá vigência de 12 (doze) meses, podendo ser prorrogado se presentes os requisitos legais e se de acordo com a vontade das partes.
3.5 - Ultrapassado o período igual ou superior a um ano a contar da data limite para apresentação da proposta na licitação, poderá ser concedido reajuste do preço contratado.
3.6 – Na hipótese de concessão de reajustamento, este será calculado com base na variação do INPC, Índice Nacional de Preços ao Consumidor, abrangendo o período compreendido entre a data limite para apresentação da proposta e o mês correspondente ao do implemento da anuidade.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES
4.1 - **Do Município**:
4.1.1 - Emitir Ordem de Serviço, Fornecimento ou Empenho;
4.1.2 - Atestar nas notas fiscais na efetiva entrega do objeto desta licitação;
4.1.3 - Aplicar à empresa vencedora penalidade, quando for o caso;
4.1.4 - Prestar à Adjudicada toda e qualquer informação, por esta solicitada, necessária à perfeita execução do Objeto;
4.1.5 - Efetuar o pagamento no prazo avençado, após a entrega da Nota Fiscal no setor competente;
4.1.6 - Notificar, por escrito, à Adjudicada da aplicação de qualquer sanção.
4.1.7 - Comunicar a empresa sobre dias e horários dos eventos com antecedência mínima de 24(vinte e quatro) horas.
4.2 - **Da Contratada**:
4.2.1 - Fornecer o serviço objeto desta licitação nas especificações contidas neste edital;
4.2.1.1 - E empresa deverá ter profissional disponível para a prestação do Serviço sempre que necessário.
4.2.2 - Pagar todos os tributos que incidam ou venham a incidir, direta ou indiretamente, sobre os produtos vendidos;
4.2.3 - Manter, durante a execução do objeto, as mesmas condições de habilitação;
4.2.4 - Aceitar, nas mesmas condições do edital, os acréscimos ou supressões que se fizerem necessários no quantitativo do objeto desta licitação, até o limite de 25%(vinte e cinco por cento) do valor;
4.2.5 - Fornecer o objeto licitado, no preço, prazo e forma estipulados na proposta;
4.2.6 - Fornecer o objeto de boa qualidade, dentro dos padrões exigidos neste edital.

CLÁUSULA QUINTA - DAS PENALIDADES
5.1 - Os casos de inexecução do objeto deste Contrato, erro de execução, execução imperfeita, atraso injustificado e inadimplemento contratual, sujeitará o proponente contratado às penalidades previstas no art. 87 da Lei 8.666/93, das quais destacam-se:
a) advertência;
b) multa de 0,05%(cinco centésimos por cento) do valor do contrato, por dia de atraso injustificado na execução do mesmo, observado o prazo máximo de 05(cinco) dias úteis;
c) multa de 2%(dois por cento) sobre o valor estimado para o contrato, pela recusa injustificada do adjudicatário em executá-lo;
d) suspensão temporária de participação em licitações e impedimento de contratar com o Município, no prazo de até 02(dois) anos;
e) declaração de inidoneidade para contratar com a Administração Pública, até que seja promovida a reabilitação, facultado ao contratado o pedido de reconsideração da decisão da autoridade competente, no prazo de 10(dez) dias da abertura de vistas ao processo.
5.2 - Os valores das multas aplicadas previstas nos subitens acima poderão ser descontados dos pagamentos devidos pela Administração.
5.3 - Da aplicação das penas definidas nas alíneas "a", "d" e "e", do item 5.1, caberá recurso no prazo de 05(cinco) dias úteis, contados da intimação.
5.4 - O recurso ou o pedido de reconsideração será dirigido ao Secretário da unidade requisitante, que decidirá o recurso no prazo de 05(cinco) dias úteis e o pedido de reconsideração, no prazo de 10(dez) dias úteis.
5.5 - A inexecução total ou parcial do Contrato ensejará na sua rescisão, com as conseqüências contratuais e as previstas em Lei, cujos motivos para a referida rescisão são os previstos no art. 78 da Lei 8.666/93.
5.6 - O Município poderá rescindir o contrato, independentemente de qualquer procedimento Judicial, observada a Legislação vigente, nos seguintes casos:

a) por infração a qualquer de suas cláusulas;
b) pedido de concordata, falência ou dissolução da Contratada;
c) em caso de transferência, no todo ou em parte, das obrigações assumidas neste contrato, sem prévio e expresso aviso ao Município;
d) por comprovada deficiência no atendimento do objeto deste contrato;
e) mais de 2(duas) advertências.
5.7 - O Município poderá, ainda, sem caráter de penalidade, declarar rescindido o contrato por conveniência administrativa ou interesse público, conforme disposto no artigo 79 da lei 8.666/93 e suas alterações.

CLÁUSULA SEXTA - DA DOTAÇÃO ORÇAMENTÁRIA
6.1 - A despesa decorrente da execução do presente Contrato correrá à conta do Orçamento Programa Anual do Município, cuja classificação funcional programática e categoria econômica constante são as seguintes:
Atividade: 2017.
Rubrica: 339040.00000000

CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO
7.1. A execução do contrato será acompanhada e fiscalizada pelos servidores: Andrigo Fenner e Jeison Drum – Técnicos em Informática.

CLÁUSULA OITAVA - DA CESSÃO
8.1 - A CONTRATADA somente poderá ceder, quer total quer parcialmente, este contrato, mediante prévia e expressa autorização do Município.

CLÁUSULA NONA - DO FORO
9.1 - Para dirimir quaisquer questões decorrentes do presente contrato, elegem as partes o Foro da Comarca de Ibirubá-RS, com renúncia expressa a qualquer outro por mais privilegiado que seja.
E por estarem assim acordados, assinam este contrato os representantes das partes e as testemunhas abaixo em três vias de igual teor.

Ibirubá(RS), 14 de julho de 2023.

ABEL GRAVE
Prefeito

GABRIEL DE SOUZA
COPREL TELECOM LTDA
Fornecedor

TESTEMUNHAS:

DEMONSTRATIVO LOTE

MEMORIAL DESCRITIVO TÉCNICO

Objeto: Contratação de Empresa Especializada destinada ao fornecimento de soluções de segurança de redes compostas por dispositivo dedicado para segurança tipo (NGE_Next_Security), para prover segurança e proteção da rede de computadores de todos os setores da Secretaria Municipal do Município de Ibirubá/RS,em Regime de Comodato cobrindo segurança dessas unidades da prefeitura, com dispositivos físicos, incluindo treinamento, Operação inicial, Configuração, Suporte Técnico e Monitoramento, aos equipamentos a serem implantados.

JUSTIFICATIVA

A prestação de serviços públicos é uma das finalidades da Administração Municipal, serviços estes que possuem grande demanda, principalmente nas áreas relacionadasà saúde e educação. Para a efetivação destes meios informatizados são integralmenteutilizados, de forma a criar e manter protocolos, registros e acompanhamento da relação entre os serviços prestadose os usuários destes.

Contudo, para a operacionalização dos meios informatizados efetiva-se com o uso continuo da rede de Internet, de modo que os variados sistemas e equipamentos utilizados pelas Secretarias são interligados por esta rede ao servidor central da Prefeitura Municipal.

Atualmente, a estrutura de rede possui inúmeros equipamentos e periféricos conectados e com navegação de Internet, fato este, que interfere diretamente na questão relacionada à segurança das informações e dados digitais relativos ao uso dos sistemas informatizados.

Diante do que se refere à segurança da informação, o Departamento de Tecnologia da Informação, através desde processo, busca a contratação de serviço especializado em implantação de sistema de segurança para redes, pois o referido sistema age como primeira barreira de segurança digital, efetuando as funções de filtro, bloqueio,controle e liberação de toda a navegação dos computadores, tablets, celulares, notebooks e demais aparelhos pertencentes ao patrimônio do Município que se conectam à Internet, tendo esse controle se resume em recurso prioritário neste momento, visto as inúmeras invasões e tentativas de ataques que vão desde computadores pessoais, empresas multinacionais, estruturas críticas dogoverno e até instancias da justiça que foram vítimas recentes das ameaças digitais.

Sendo assim, existe uma elevada necessidade de controle de segurança digital dos meios informatizados citados, fica justificado a contratação dos serviços especializados mencionados, de forma a garantir a qualidade, agilidade e segurança dos registros provenientes dos sistemas de informações das Secretarias

DO APPLIANCE DE SEGURANÇA E SUAS ESPECIFICAÇÕES:

A appliance deve atender as exigências e requisitos estabelecidos neste documento.

1.1 Os equipamentos deverão ter suporte à proteção imediata contra ameaças (default threat protection), Filtro de Conteúdo por aplicação, IPS, Varredura por SandBox, controle de nivel de segurança por reputação web, Cloud Access Security Broker (CASB), controle de aplicação cloud, fornecer segurança em múltiplas camadas,fornecer segurança em zona externa, interna e ser entregue em plataforma tipo appliance físico em cluster, no qual será instalado em rack da própria instituição;

1.2 Deverá oferecer suporte a configuração de endereços de ip estáticos dinâmicos (pppoe, dhcp, estático) para conexões externas;

1.3 O fabricante do equipamento deve ter seu produto avaliado Gartner no Magic Quadrant Network Firawall 2022;

1.4 O equipamento deverá ter garantia sem custo adicional durante a vigência do contrato, em caso de defeito físico(hardware) a contratada deverá providenciar troca do equipamento, durante a vigência contratual;

1.5 O equipamento deverá suportar a comunicação entre dos os setores ecomunicações com datacenter de forma segura entre dispositivos;

1.6 Suporte a VPN sobre os protocolos IPsec tipo SSL;

1.7 Possuir controle de acesso a internet por aplicação;

1.8 Possuir controle de acesso a internet por destino;
1.9 Possuir controle de acesso a internet por sub-rede;
1.10 Possuir controle de acesso a internet por VLAN;
1.11 Possuir suporte a tags de VLANS (802.1q);
1.12 Possuir integração com Servidores de autenticação RADIUS, LDAP, AD (transparente), TACACS+ e AzureAD;
1.13 Possuir um sistema de armazenamento em nuvem para armazenamento de backups da solução;
1.14 Possuir suporte de recuperação via conexões do tipo RJ45 e SSH;
1.15 Possibilitar a visualização e controle de regras por países de origem e destino, permitindo controlar nos logs de eventos, de acessos e ameaças;
1.16 As cópias de segurança devem ser salvas compactadas e criptografadas de forma agarantirsegurança, confiabilidade e confidencialidade dos arquivos de backup;
1.17 O sistema ainda deve contemplar um recurso de cópia de segurança, que contemple a cópia completa das configurações dos serviços e recursos do sistema, facilitando migração ou restorede emergência;
1.18 Deve possibilitar a restauração das configurações através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata, por meio de importação de configurações;
1.19 Possuir métodos de autenticação de usuários que possa facilmente controlar os acessos a internet de usuários.
1.20 Possuir suporte a roteamento dinâmico OSPFv3 e BGP;
1.21 Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
1.22 Deverá ter forma de realizar controle de aplicações multimídia como: H.323, SIP e/ou outros;
1.23 Possuir tecnologia de varredura do tipo Stateful;
1.24 Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
1.25 Possuir conexão entre estação de gerência e appliance criptografada tanto eminterfaceWeb gráfica (SSL) quanto em CLI (linha de comando) via SSH;
1.26 Permitir criação de serviços por porta ou conjunto de portas dos seguintesprotocolos, TCP,UDP, ICMP e IP;
1.27 Permitir o agrupamento de serviços e/ou regras;
1.28 Permitir o filtro de pacotes sem a utilização de NAT;
1.29 Permitir a abertura de novas portas por fluxo de dados para serviços querequerem portasdinâmicas;
1.30 Possuir mecanismo de controle de ameaças por meio de filtragem de conteúdo com mecanismo dual, no qual a plataforma possa utilizar-se de duas bases de consulta de ameaças simultaneamente;
1.31 Permitir criação de regras definidas pelo usuário;
1.32 Permitir o serviço de autenticação para HTTP e FTP;
1.33 Possuir a funcionalidade de balanceamento e contingência de links;
1.34 Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Whatsapp, Tiktok,Facebook, Instagram, Hangouts, Skype, Telegram,Viber.
1.35 Deve possuir a capacidade de criação de políticas de acesso do equipamento, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC'S e Radius;
1.36 Para usuários não registrados ou não reconhecidos no domínio, a solução deveser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente instalado nas desktop;
1.37 A solução de identificação de usuário deverá se integrar com as funcionalidades,permitindo catalogar os acessos, sendo elas do mesmo fabricante;
1.38 A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais a cada unidade de cada setor adequado a solução para uso seguro das aplicações de uso do município;
1.39 Possuir controle de VPN baseada em Appliance tipo SITE-to-SITE permitindoconfiguração de pontes com duas unidades de equipamento;
1.40 Possuir algoritmos de criptografia para túneis VPN: PFS, DES, 3DES;

1.8 Possuir controle de acesso a internet por destino;
1.9 Possuir controle de acesso a internet por sub-rede;
1.10 Possuir controle de acesso a internet por VLAN;
1.11 Possuir suporte a tags de VLANS (802.1q);
1.12 Possuir integração com Servidores de autenticação RADIUS, LDAP, AD (transparente), TACACS+ e AzureAD;
1.13 Possuir um sistema de armazenamento em nuvem para armazenamento de backups da solução;
1.14 Possuir suporte de recuperação via conexões do tipo RJ45 e SSH;
1.15 Possibilitar a visualização e controle de regras por países de origem e destino, permitindo controlar nos logs de eventos, de acessos e ameaças;
1.16 As cópias de segurança devem ser salvas compactadas e criptografadas de forma agarantirsegurança, confiabilidade e confidencialidade dos arquivos de backup;
1.17 O sistema ainda deve contemplar um recurso de cópia de segurança, que contemple a cópia completa das configurações dos serviços e recursos do sistema, facilitando migração ou restorede emergência;
1.18 Deve possibilitar a restauração das configurações através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata, por meio de importação de configurações;
1.19 Possuir métodos de autenticação de usuários que possa facilmente controlar os acessos a internet de usuários.
1.20 Possuir suporte a roteamento dinâmico OSPFv3 e BGP;
1.21 Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
1.22 Deverá ter forma de realizar controle de aplicações multimídia como: H.323, SIP e/ou outros;
1.23 Possuir tecnologia de varredura do tipo Stateful;
1.24 Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
1.25 Possuir conexão entre estação de gerência e appliance criptografada tanto eminterfaceWeb gráfica (SSL) quanto em CLI (linha de comando) via SSH;
1.26 Permitir criação de serviços por porta ou conjunto de portas dos seguintesprotocolos, TCP,UDP, ICMP e IP;
1.27 Permitir o agrupamento de serviços e/ou regras;
1.28 Permitir o filtro de pacotes sem a utilização de NAT;
1.29 Permitir a abertura de novas portas por fluxo de dados para serviços querequerem portasdinâmicas;
1.30 Possuir mecanismo de controle de ameaças por meio de filtragem de conteúdo com mecanismo dual, no qual a plataforma possa utilizar-se de duas bases de consulta de ameaças simultaneamente;
1.31 Permitir criação de regras definidas pelo usuário;
1.32 Permitir o serviço de autenticação para HTTP e FTP;
1.33 Possuir a funcionalidade de balanceamento e contingência de links;
1.34 Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to- peer) e de mensagens instantâneas, suportando ao menos: Whatsapp, Tiktok,Facebook, Instagram, Hangouts, Skype, Telegram,Viber.
1.35 Deve possuir a capacidade de criação de políticas de acesso do equipamento, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
1.36 Para usuários não registrados ou não reconhecidos no domínio, a solução deveser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente instalado nas desktop;
1.37 A solução de identificação de usuário deverá se integrar com as funcionalidades,permitindo catalogar os acessos, sendo elas do mesmo fabricante;
1.38 A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais a cada unidade de cada setor adequado a solução para uso seguro das aplicações de uso do município;
1.39 Possuir controle de VPN baseada em Appliance tipo SITE-to-SITE permitindoconfiguração de pontes com duas unidades de equipamento;
1.40 Possuir algoritmos de criptografia para túneis VPN: PFS, DES, 3DES;

1.41 Suporte a certificados PKI X.509 para construção de VPNs;
1.42 Possuir suporte a VPNs IPSec site-to-site:
1.42.1Criptografia RSA;
1.42.2Integridade de conexão para verificar qual é a melhor rota de comunicação;1.42.3Algoritmo Internet Key Exchange (IKE) versões II;
1.42.4 AES 256 (Advanced Encryption Standard);
1.42.5 Suporte à proteção avançada de ameaças, capaz de controlar e monitorar DNS e AFC;
1.42 Possuir recurso de "SD-WAN", efetuado troca de rotas de forma automática com filtros pré-definidos ou customizados, utilizando como formas de identificação banda,latência, jitter, perca de pacote e outros para mudar a saída de internet;
1.43 Possuir troca de rotas estáticas com túnel datacenter de forma automática deacordo comanálise dos dados trafegados e mensuração da ferramenta SD-WAN;
1.44 O sistema de detecção e proteção que de link deverá realizar a troca de rota de links através de mensuração health-check com filtros pré-definidos ou customizados, utilizando como formas de identificação banda ou latência ou jitter ou perca de pacote ou ping;
1.45 Possuir saída personalizada de rota por aplicação, exemplo uma regra/rota para um entra ou saída especifica no qual um determinado trafego poderá ser dirigido para apenas um link;
1.46 Possuir saída personalizada de rota por VLAN;
1.47 A solução entregue deve ser composta por software e appliance (hardware) do mesmo fabricante, garantindo total integração e desempenho do ambiente;
1.48 Deve fazer uso de sistemas de sistema operacional próprio, desenvolvido e customizado para a atividade de segurança de rede, baseado em "Appliance", que se entende como um subsistema com o propósito específico para soluções de segurança em redes a nível de aplicação, não sendo permitindo uso de computadores e/ou servidores convencionais convertidos para uso de software de terceiros ou opensouce,a contratação visa a aquisição de solução totalmente desenvolvida e customizada para segurança de redes.
1.49 A plataforma deverá permitir acesso e configuração de API integrados a plataforma de terceiros tipos RMM/PSA;
1.50 Deve permitir atualização de Firmware por meio de agendamento centralizado em plataforma da própria fabricante, sendo agendamento de forma que aplique de forma autônoma em horário pré-definido.

2. DO CONTROLADOR INTEGRADO AO APPLIANCE
2.1 O appliance a for fornecido deverá ser capaz de ser utilizado como controlador centralizado capaz de controle e adição de unidade de antena (access point) futurana prefeitura, a administração dos access points deverá permitir a padronização dos equipamentos de infraestrutura do município e seus setores que possam futuramente adquirir antenas;
2.2 Os pontos de acesso devem permitir realizações de configurações centralizadas, administrando e configurando múltiplos equipamentos de forma simultânea na própriaunidade bem como na console centralizado do próprio fabricante, não sendo necessário instalar servidor de gestão ou configuração em rede local, sendo operada totalmente pela nuvem ou pela unidade local de segurança appliance;
2.3 Deve permitir no mínimo 100 equipamentos sob seu controle;
2.4 Deve possibilitar configuração através de interface gráfica (WEB) em nuvem, não sendo necessário a unidade appliance estar online para que a operação do equipamento wireless continue operando;
2.5 O Controlador deve suportar IEEE 802.1X;
2.6 O Controlador deve implementar associação de SSID com VLANS;
2.7 Deve possuir SSIDS internas que distinguem perfis de uso;

3. DEMAIS CONFIGURAÇÕES E RECURSOS DO APPLIANCE
3.1 A plataforma de segurança deve possuir appliance com capacidade e as características abaixo, por um equipamento:
3. 2 Through-put de 4000 Mbps com a funcionalidade de controle de invasão IPS habilitada;
3.3 Through-put de 1100 Mbps com as seguintes funcionalidades habilitadas simultaneamente para as assinaturas que a plataforma de segurança: controle de aplicação, IPS e Anti-vírus/Anti- spyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades,

somente o de menor valor será aceito;
3.4 Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
3.5 Suporte a, no mínimo, 2.600.000 conexões simultâneas;
3.6 Suporte a, no mínimo, 100.000 novas conexões por segundo;
3.7 Conector para fonte redundante interna ou externa;
3.8 Armazenamento interno de no mínimo 80 GB por unidade de appliance.
3.9 No mínimo, 05 (cinco) interfaces de rede 10/100/1000 base-TX;
3.10 Possuir 1 (uma) interface de rede RJ45 dedicada para gerenciamento;
3.11 Possuir 1 (uma) interface do tipo console ou similar;
3.12 Suporte a, no mínimo, 5 (cinco) zonas de segurança pré-definidas ou customizadas;
3.13 Estar licenciada para ou suportar sem o uso de licença, 2000 (dois mil) clientesde VPN SSLsimultâneos;
3.14 Estar licenciada para ou suportar sem o uso de licença, 2000 (dois mil) túneis de VPN IPsec simultâneos, ao todo a solução deverá suporta no mínimo 11.000 Mbps de trafego IPsec;
3.15 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
3.16 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as funcionalidades, bem como hardware dedicado para ofuncionamento das mesmas;
3.17 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e endof-sale. A licitante deverá indicar marca e modelo na suaproposta inicial. lançada no sistema.
3.18 A solução deve consistir de appliance de proteção de rede com funcionalidades depróximageração (N-G-F-W), e console de gerência e monitoração;
3.19 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3.20 As funcionalidades de proteção de rede que compõe a plataforma de segurança, devem funcionar em múltiplos desde que obedeçam a todos os requisitos desta especificação;
3.21 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
3.22 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3.23 A solução deverá ser fornecida e instalada em conjunto com segunda unidade para que possa operar em modo da alta disponibilidade HA, operando de forma de cluster;
3.24 O software deverá ser fornecido em sua versão mais atualizada;
3.25 Suportar sub-interfaces ethernet logicas.
3.26 A unidade deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota.
3.27 Caso haja falha na comunicação o sistema deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
3.28 Proteção contra DoS e Spoof;
3.29 Deve permitir bloquear sessões inseguras usando inteligente interna, prevenindo desta forma possíveis tráfegos maliciosos;
3.30 Deve operar com rota estática;
3.31 Deve exibir nos logs de tráfego o motivo para o término da sessão, incluindo sessões finalizadas onde houver decriptografia de SSL e SSH;
3.32 Deve suportar roteamento estático e dinâmico (RIP, BGP e OSPFv3);
3.33 Capaz de operar através de Upstream proxy;
3.34 Deve operar com SD-WAN, ser capaz de criar políticas para essas atividades;
3.35 Fabricante deve estar listada no 2021 Gartner Magic Quadrant for Network Fire-walls;
3.36 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância, mediante o uso de suas interfaces físicas nos seguintes modos de camada 2 (l2) e camada 3 (l3);
3.37 Possuir modo Sniffer(modo captura), para inspeção de dados de rede;

somente o de menor valor será aceito;
3.4 Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
3.5 Suporte a, no mínimo, 2.600.000 conexões simultâneas;
3.6 Suporte a, no mínimo, 100.000 novas conexões por segundo;
3.7 Conector para fonte redundante interna ou externa;
3.8 Armazenamento interno de no mínimo 80 GB por unidade de appliance.
3.9 No mínimo, 05 (cinco) interfaces de rede 10/100/1000 base-TX;
3.10 Possuir 1 (uma) interface de rede RJ45 dedicada para gerenciamento;
3.11 Possuir 1 (uma) interface do tipo console ou similar;
3.12 Suporte a, no mínimo, 5 (cinco) zonas de segurança pré-definidas ou customizadas;
3.13 Estar licenciada para ou suportar sem o uso de licença, 2000 (dois mil) clientesde VPN SSLsimultâneos;
3.14 Estar licenciada para ou suportar sem o uso de licença, 2000 (dois mil) túneis de VPN IPsec simultâneos, ao todo a solução deverá suporta no mínimo 11.000 Mbps de trafego IPsec;
3.15 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
3.16 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as funcionalidades, bem como hardware dedicado para ofuncionamento das mesmas;
3.17 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e endof-sale. A licitante deverá indicar marca e modelo na suaproposta inicial, lançada no sistema.
3.18 A solução deve consistir de appliance de proteção de rede com funcionalidades depróximageração (N-G-F-W), e console de gerência e monitoração;
3.19 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
3.20 As funcionalidades de proteção de rede que compõe a plataforma de segurança, devem funcionar em múltiplos desde que obedeçam a todos os requisitos desta especificação;
3.21 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
3.22 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
3.23 A solução deverá ser fornecida e instalada em conjunto com segunda unidade para que possa operar em modo da alta disponibilidade HA, operando de forma de cluster;
3.24 O software deverá ser fornecido em sua versão mais atualizada;
3.25 Suportar sub-interfaces ethernet logicas.
3.26 A unidade deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota.
3.27 Caso haja falha na comunicação o sistema deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
3.28 Proteção contra DoS e Spoof;
3.29 Deve permitir bloquear sessões inseguras usando inteligente interna, prevenindo desta forma possíveis tráfegos maliciosos;
3.30 Deve operar com rota estática;
3.31 Deve exibir nos logs de tráfego o motivo para o término da sessão, incluindo sessões finalizadas onde houver decriptografia de SSL e SSH;
3.32 Deve suportar roteamento estático e dinâmico (RIP, BGP e OSPFv3);
3.33 Capaz de operar através de Upstream proxy;
3.34 Deve operar com SD-WAN, ser capaz de criar políticas para essas atividades;
3.35 Fabricante deve estar listada no 2021 Gartner Magic Quadrant for Network Fire-walls;
3.36 Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância, mediante o uso de suas interfaces físicas nos seguintes modos de camada 2 (l2) e camada 3 (l3);
3.37 Possuir modo Sniffer(modo captura), para inspeção de dados de rede;

3.38 Deve suportar o protocolo Multicast (PIM-SM) permitindo que a unidade possa anunciar rotas multicast;
3.39 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
3.40 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
3.41 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo seradicionados nas políticas para bloqueio ou permissão do tráfego;
3.42 Deve permitir autenticação segura através de certificado nas fontes externas deendereçosIP, domínios e URLs;
3.43 Deve permitir consultar e criar exceção para objetos das listas externas a partirda interfacede gerência do próprio da unidade;
3.46 Controle de políticas por país usando GEO-IP;
3.47 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
3.48 Bloqueios dos seguintes tipos de arquivos: (exemplo bat, cab, dll, exe, pif, e reg);
3.49 Traffic shaping QoS baseado em Políticas (exemplo Prioridade, Garantia e Máximo);
3.50 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusivepor aplicações;
3.51 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
3.52 Os dispositivos de proteção devem permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
3.53 Os dispositivos de proteção capaz de reconhecer ameaças usando tecnologia de Zero-Day integrados ao próprio equipamento, a solução já deve vir licenciada comtais recursos.
3.54 Os dispositivos de proteção devem reconhecer pelo menos 3500 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;
3.55 Os dispositivos de proteção devem reconhecer aplicações de nuvem, com recurso conhecido como Cloud Access Security Broker (CASB);
3.56 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
3.57 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindogranularidade de controle/políticas para os mesmos;
3.58 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Anti-vírus e Anti-Spyware integrados no próprio appliance ou entregue através de composição com outro equipamento do mesmo fabricante.
3.59 Deve incluir assinaturas de prevenção de intrusão (IPS) capaz dedetectar/reconhecer pelomenos 2.400 ameaças.
3.60 As funcionalidades de IPS, Anti-vírus/Anti-Spyware devem operar em conjuntocom os demais recursos de segurança do equipamento.
3.61 Deve sincronizar as assinaturas de IPS, Anti-vírus, Anti-Spyware quando implementado emalta disponibilidade ativo/ativo e ativo/passivo.
3.62 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware/Anti-vírus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por umintervalo de tempo.
3.63 As assinaturas presentes no respectivo termo devem vir ativadas e continuar ativasduranteo contrato.
3.64 Exceções por IP de origem ou de destino devem ser possíveis nas regras.
3.65 Deve suportar granularidade nas políticas de IPS Anti-vírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
3.66 A solução deve ser imune e capaz de impedir ataques básicos.
3.67 A solução detectar e bloquear a origem maliciosas com possibilidade de criarexceções paraendereços IPs de ferramentas de monitoramento da organização.
3.68 A solução deve bloquear ataques efetuados por worms conhecidos, permitindo ao administrador

acrescentar novos padrões.
3.69 A solução deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
3.70 A solução deve possuir assinaturas para bloqueio de ataques oriundos da internetcom detecção por meio de assinatura.
3.71 A solução deverá possibilitar a criação/importação de assinaturas customizadas pelainterface gráfica do produto.
3.72 A solução deverá permitir configurações customizadas para controle e detecção deinvasão.
3.73 A solução deverá permitir o bloqueio de vírus/spywares, permitindo que seja escolhido qual o protocolo será feito a varredura;
3.74 A solução deverá utilizar mecanismo de varredura de ameaças dual, permitindo que seja feita a escolha do provedor de varredura.
3.75 A solução deverá suportar bloqueio de arquivos por tipo.
3.76 A solução deverá identificar e bloquear comunicação com botnets.
3.77 A solução deverá suportar várias técnicas de prevenção.
3.78 A solução deve suportar FIPS 140-2 level 1.
3.79 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
a) Permite especificar política por tempo, ou seja, a definição de regras para um determinadohorário ou período (dia, mês, ano, dia da semana e hora);
b) Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips,Redes e Zonasde segurança;
c) Deverá incluir a capacidade de criação de políticas baseadas na visibilidade econtrole dequem está utilizando quais URLs através
da integração com serviços de diretório, autenticação via ldap, Active Directory e basede dadoslocal;
d) Permite popular todos os logs de URL com as informações dos usuários conformedescrito naintegração com serviços de diretório;
e) Suporta a capacidade de criação de políticas baseadas no controle por URL eCategoria deURL;
f) Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
g) Suporta controle de URL, por meio de mecanismo do próprio fabricante comconstantes atualizações de novas URLs;
h) Possui pelo menos 80 categorias de URLs;
i) A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
3.80 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS);
3.81 Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonteexterna;
3.82 Não deve ser necessário instalação de cliente para administração da solução o mesmo deve, ser acessível por navegadores que sejam compatíveis com sistemas operacionais Windows e Linux;
3.83 Acesso de administradores via console e via HTTP;
3.84 Deve permitir que administradores escolha quais imagem o equipamento pode operar, para tanto o equipamento deverá permitir a instalação de 2 imagens(firmware) permitindo ao administrador fazer rollback em caso de falha da atualização do firmware;
3.85 Deve mostrar ao administrador do equipamento a hora e data do último login e tentativasde login com falha para acessos em seu sistema interno de logs;
3.86 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitandoa localização de comandos;
3.87 Deve permitir usar palavras chaves(descrições) para facilitar identificação de regras;
3.88 Deve suportar também o monitoramento dos seguintes recursos via SNMPv3 e Netflow;

3.89 A plataforma fornecida deverá ter console de gestão a ser disponibilizada pela contratada, capaz de concentrar todos eventos dos equipamentos de segurança instalados, essa plataforma deverá reter pelo menos 12 meses de eventos, para tantoa contratada poderá fornecer soluçãovirtualizada tipo Vmware vSphere ou HiperV das quais irá coletar esses logs, ou fornecer plataforma em nuvem da própria desenvolvedora do produto, operando como concentrador de eventos, em todo o caso caberá a contratada custear toda a instalação, configuração ou disponibilização de equipamento caso seja necessário em razão da solução proposta.

DO SUPORTE E MONITORADO DA PLATAFORMA

4.1 A contratada deverá fornecer SOC (Security Operation Center) na modalidade 8x5 com plantões eventuais de emergências em caso de incidentes;

4.2 A contratada deverá fornecer suporte durante a vigência contratual, para tanto a contratada deverá dispor de equipe técnica qualificada, capaz de interpretar e resolver problemas de forma direta ou através de intervenção em conjunto do fabricante da solução, quando necessário;

4.3 A contratada deverá fornecer plataforma com dashboard que permita visualização e monitoramento de consumo em tempo real de todos os recursosutilizados da solução, a plataforma deverá ser alocada na nuvem sem necessidade de instalação de software local;

4.4 A contratada deverá fornecer todos softwares, licenças, recursos e suporte necessários para o total cumprimento dos requisitos deste processo, a contratada deverá fornecer plataforma de gestão central da ferramenta com capacidade de retenção mínima de 12 Meses de eventos de segurança;

4.5 A contratada deverá configurar os alertas proativos inteligentes aos usuáriostécnicos da prefeitura, a configuração deverá gerar eventos e monitoramento 24 horas 7 dias de forma que seja possível detectar anomalias da rede indiferente do momento que ocorreu.

4.6 A contratada deverá auxiliar a prefeitura em caso de incidentes em tempo real de todas as soluções prestadas;

4.7 A deverá auxiliar a prefeitura no processo de instalação, orientando sobre as melhores práticas e indicando o que pode ser melhorado da rede e das conexões adjacentes aos equipamentos por ela fornecidos em razão do contrato;

4.8 A contratada deverá fornecer login/senha para acesso a plataforma de aberturade chamados, a plataforma de abertura deverá estar disponível 24x7, essa plataforma deverá catalogar os eventos e situações que possa necessitar de intervenção na rede;

4.9 A contratada deverá fornecer deverá configurar alertas proativos a equipamentos de alta severidade e que podem comprometer a segurança do município como um todo (DESKTOPS, APs, SERVIDORES, SWITCHS, IMPRESSORAS, DVRS, WIRELESS), como configurando recursos de ATP e Detecção de ameaças IPS.

4.10 A contratada deverá enviar alertas através dos meios de comunicação de fácil acesso aos servidores como aplicativos mensageiros mais utilizados;

4.11 A contratada deverá atender na modalidade help desk todas as dúvidas dos servidores emacessos a rede e gestão de filtros e segurança dos equipamentos por elaimplantado;

4.12 A contratada deverá atender na modalidade help desk todas as dúvidas dos servidores públicos em configurações da plataforma de segurança disponibilizada;

4.13 A contratada deverá fornecer um meio de comunicação com tempo de resposta máximo de 3 h para atendimento de chamados;

4.14 A contratada deverá disponibilizar contatos de telefone para atendimento das requisiçõescom severidade alta em caso de falha das outras opções disponíveis;

4.15 Todos os recursos dos ambientes de rede implantados (appliance) devem ser monitoradosatravés de gráficos de fácil acesso aos servidores públicos, na plataforma a ser disponibilizada pela contratada;

4.16 Todos os gráficos e dashboards fornecidos devem utilizar identificação para acesso;

FORNECIMENTOS DE SERVIÇOS:

Fornecimento de soluções multifuncional de gateway de segurança integrada com equipamento (appliance físico), com respectivo software dedicado tipo next gen (N- G-F-W) para proteção de informação perimetral, com segurança IPS multidirecional, filtros anti-vírus com bloqueio de ameaças na borda, filtro de aplicações para

controle de uso interno seguro e estável, gerencia completa da rede interna em camadas, vpn, com stateful para interligação de serviços e soluções utilizadas no município e em suas secretarias.
Fornecimento de solução e prestação de serviços na modalidade de infraestrutura como serviço, com fornecimento de equipamentos, serviços, software, além de plataforma em nuvem para gerência profissional da solução. A administração deverá ocorrer de forma isolada das configurações, a solução para acesso a rede de forma simplificada e segura, com resguardo de logs em gateway atendendo a Lei 13.709/2018 – LGPD (Lei Geral de Proteção de Dados), Lei Nº 12.965/14 - Marco Civil da Internet.
A contratada deverá realizar a disponibilização de suporte em NOC (Network Operation Center) e SOC (Security Operation Center) na modalidade 8x5, suporte a monitoramento de equipamentos e status da interligação de forma inteligente. A soluções deverá ter análise de dados, permitir alertas proativos com filtragem de severidade, com todos recursos necessários para efetivo do monitoramento em tempo real da situação da plataforma, fornecendo detecção, análise e correção de falhas, compreendendo a correção contínua de anomalias.

ENTREGA E INSTALAÇÃO

A entrega e instalação do equipamento deve ocorrer em dias úteis, devendo ser previamente agendada através do telefone (54) 3324-8500, o agendamento deverá ocorrer diretamente com o fiscal do contrato que será designado após o certame, quando da assinatura do contrato.
O Município reserva-se o direito de alterar o local de instalação dos equipamentos.
A entrega e instalação somente será efetuada e aceita caso os equipamentos estejam acompanhados de todos os cabos, módulos e acessórios necessários, não sendo permitidas entregas parciais e/ou fracionadas.
Os produtos deverão estar segregados por item e entregues em sua embalagemoriginal rotulada pelo fabricante. No momento da entrega será avaliado o acondicionamento dos equipamentos, sendo que embalagens violadas, com vazamentos, produtos manchados, sujos, mofados, enferrujados, danificados ou com aparência duvidosa não serão aceitos.
A instalação dos equipamentos contempla, entre outras ações que se fizerem necessárias:
A montagem, afixação e cabeamento nos racks existentes, incluindo ligações elétricas elógicas, conforme disposição física proposta pelo Município.
Atualização de firmware, software e sistema operacional dos componentes da solução, incluindo aplicação de patches, para a última versão disponível conforme matriz de compatibilidade do fabricante.
Configurações físicas e lógicas nos equipamentos como placas de rede, linksde agregação, ambientes virtuais, administradores, licenças e demaisconfigurações iniciais necessárias para o processo de migração da rede local possam ser iniciadas.
Configuração das rotinas de backup, gravação de logs e geração de relatórios.
O prazo para a entrega e instalação é de até 45 dias corridos após a habilitação e confecção do contratado com a empresa vencedora, a instalação deverá ocorrer na Sede da Prefeitura Municipal de Ibirubá/RS, não será aceito instalação remota.

TREINAMENTO TÉCNICO

Passado o período inicial de instalação, a contratada deverá providenciar treinamento da solução, junto ao setor técnico desta prefeitura que irá indicar os profissionais envolvidos no treinamento.
O treinamento deverá ser realizado de forma presencial, para até 4 profissionais,com no mínimo 16 horas, divididas em 2 dias de treinamento e demonstração da solução operando no ambiente real.
O treinamento obrigatoriamente deverá ser oficial do fabricante e/ou realizado por profissional com certificação oficial da solução. Caso a contratada não seja o próprio fabricante caberá a contratada fornecer treinamento oficial ou licença para realizadao treinamento da solução proposta na sede desta Prefeitura.

DEMAIS INFORMAÇÕES:

Considerando a natureza do objeto, para a presente contratação será pelo critério de JULGAMENTO POR LOTE UNICO, de modo que, os itens listados no Lote 01, em razão disso deverão ser fornecidos, instalados e configurados pela mesma empresa, exemplificado pelo fato de que cada Hardware funciona com o seu respectivo Software, devido a ser um prática executada por todas empresas que desenvolvem seus softwares de segurança, as mesmas produzem seus respectivos hardwares denominados appliance, onde toda tecnologia embarcada(software) é atrelada e desenvolvida para aquele hardware(físico) proprietário e especifico, gerando confiabilidade, qualidade, desempenho e segurança nas soluções, sendoassim as empresa que fornecerá software, hardware e as atividades de instalação, configuração, treinamento e suporte, deverão ser executados por apenas

uma única proponente, essa deverá ser o próprio fabricante, caso a proponente não seja o próprio fabricante, a mesma deverá
apresentar documento oficial informando que ela tem plenas condições de efetuar fornecimento, instalação e suporte dos produtos desta fabricante, o documentodeverá ser emitido pelo desenvolver da solução.
Considerando ainda, que o agrupamento dos itens num mesmo lote não comprometerá a competividade do certame, pois no mercado existem várias empresas certificadas que possuem condições e aptidão para cotar todos os itens, dada as condições de similaridade dos serviços de mesmo segmento desta atividade. Além disso, proporcionará para ao Departamento de Tecnologia da Informação maior controle e melhor acompanhamento da operacionalidade da solução de segurança a ser contratada.
No preço proposto deverá estar incluído o valor de mão-de-obra para entrega, deslocamentos, implantação, treinamento, configurações, bem como o suporte mensaldo objeto. O objeto deveser entregue pronto para o uso e em pleno funcionamento.

ACOMPANHAMENTO DE SUPORTE

O Acompanhamento técnico deve ser realizado após a habilitação da solução e deve contemplar:
Ajustes inicias nas configurações e otimizações que tenham sido consideradas necessárias após a habilitação da solução.
Esclarecimentos de dúvidas.
Construção e adequação de relatórios de monitoramento e controle baseado em dadosreais do ambiente de TI do Município.
A contratada poderá realizar atendimento sem custos adicionais, esses devem ser realizados em dias úteis, em momentos a serem definidos pelo setor de informática. Todo atendimento deverá ser previamente notificado na plataforma de suporte da contratada, não é permitido manutenção/alteração no sistema sem os devidos registros.
Via de regra todo o atendimento deverá ser realizado de forma presencial, no local de instalação da solução, caso seja autorizado pela fiscal, poderá ser realizado em outro formato, entretanto a proponente deverá considerar os custos inerentes a esses serviços.

COBERTURA DE DEFASAGEM TECNOLOGICA

A solução deverá fornecida na versão mais atual, sem notificação até o dia do pregão sobre descontinuidade, ou End-of-Sales da solução.
Caso ocorra defasagem tecnologia no decorrer do contrato que impeça atualização dos softwares e firmwares do equipamento, caberá a contratada a imediata substituição da solução em data anterior a descontinuação das atualizações sem custos adicionais.
A nova solução a ser entregue em caso de defasagem deverá ser do fabricante ofertado e instalado no início do contrato, no caso o modelo deverá ser semelhante ao inicialmente ofertado, obrigatório ter a mesma capacidade e recursos indicados neste termo.
A substituição em caso de defasagem deverá ser totalmente custeada pela contratadaenquanto durar o contrato, caso isso ocorra a prefeitura não deverá ter aumento nos valores pagos mensalmente.

COBERTURA E GARANTIA DA SOLUÇÃO

A solução deverá fornecidos com garantia de hardware durante os meses de contrato,a partir da data de ativação, com cobertura total de peças e serviços pelo fabricante/contratada, no localda instalação da solução.
A garantia deverá abranger todo e qualquer defeito de fabricação, além de firmwares, softwares, sistema operacional e acessórios envolvidos na implementação da solução.
Durante o período de vigência da garantia o Município terá direito a atualizações corretivas e evolutivas das versões de sistema operacional, software e firmware que integram a solução, semcustos adicionais.
Durante o período de vigência da garantia o Município terá direito a atualizações dos catálogosde aplicações, sites e assinaturas de ameaças, sem custos adicionais.
Em eventual falha técnica caberá a contratada efetuar a substituição física dasunidades com problemas, sem custos adicionais, inclusive se for necessário a intervenção do fabricante, todo esse processo de RMA será de responsabilidade da contratada.
Custos de reposição, frete e reinstalação em caso de falha física devem ser custeadospela contratada.
A garantia da solução durante a vigência contratual deverá ser completa e plena,salvo em condições de força maior, como desastres naturais, furto e/ou roubo, imperícia interna ou danopropositalao equipamento.

QUALIFICAÇÃO TÉCNICA

Atestado(s) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que o Licitante forneceu ou fornece produtos damesma natureza ou similares ao da presente

Licitação. O(s) documento(s) deverá(ão) conter o nome, o endereço e o telefone de contato do(s) atestador(es), ou qualquer outro meio que permita ao órgão promotor da licitação manter contato com a(s) empresa(s) atestante(s). Podendo ser exigido em diligência da proposta melhor classificada, que apresente cópia autenticada do contrato de fornecimento de materiais ou de prestação de serviço ou da(s) respectiva(s) nota(s) fiscal(is), que deram origem ao Atestado. Se o atestado for emitido por pessoa jurídica de direito privado, deverá constar o reconhecimento de firma passada em cartório do titular da empresa que firmou a declaração.
Declaração da LICITANTE informando que terá plenas condições de atender aosexigências do processo, meios de comunicação, estrutura adequada, pessoal qualificado, ferramentas e softwares necessários, conforme disposto no projeto.
A LICITANTE deverá possuir na sua equipe profissionais com as seguintes certificações obrigatórias e indispensáveis em face da complexidade da prestação dos serviços requeridos da rede computacional: 02 (dois) profissionais certificados com nível expert, ou engenheiro, ou Nível 2 ou superior, ou outra equivalente na solução ofertada; 01 (um) profissional com pelo menos umas das certificações de segurança da informação listadas: CISSP, OSCE, EXINIEC 27001ou CEH.
As comprovações de vínculos profissionais deverão ser feitas da seguinte forma: Mediante apresentação de cópia autenticada da CTPS – Carteira de Trabalho e Previdência Social acompanhada de cópia do Registro de Empregados, no caso de empregado da licitante; ou Contrato de prestação de serviço celebrado de acordo com a legislação civil; ou; No caso de dirigente ou sócio, do Contrato Social, ou; Declaração de contratação futura do profissional detentor do atestado apresentado, desde que acompanhada de declaração de anuência do profissional.

SUPORTE TÉCNICO

Durante o período de vigência da garantia o Município terá direito a suporte técnico preventivonos equipamentos que compõem a solução.
O suporte técnico preventivo deverá ser executado por técnicos devidamente qualificados e certificados pelo fabricante, de forma remota por meio de telefone e, quando necessário ou solicitado pelo Município, no local onde se encontrar instaladaa solução.
A contratada deve possuir mecanismo que permita a abertura de chamados de suporte técnico preventivo pelo Município através de uma Central de Atendimento, com serviço de atendimento por meio de telefone único, gratuito e não tarifado, ou através de portal web, devendo fornecer, quando da abertura, número identificador do respectivo chamado.
O registro dos atendimentos de suporte técnico preventivo deve ser feito por meio deportal web da contratada, onde será possível efetuar o registro e o acompanhamento de todos os chamados requisitados.
Não deve haver limitação quanto à quantidade de requisições de chamados de suporte técnicono período do contrato com o Município.
O suporte técnico preventivo abrange o esclarecimento de dúvidas, orientações quanto à correta utilização, configuração ou execução de operações na solução, atualização de firmware, software e sistema operacional que compõe a solução, bem como otimizações sugeridas pelo fabricante da solução.
A proponente deverá ter sede no RS, caso a mesma não tenha sede com RS a mesma deverá providenciar até a assinatura do contrato unidade capaz de atender esta prefeitura, de forma plena, dentro de prazo razoável de atendimento, uma vez quese trata de equipamento que sustenta toda a infraestrutura tecnológica da prefeitura.
A licitante proponente deverá obrigatoriamente possuir número de telefone de discagem local fixo, cod (54) a licitante poderá optar por apresentar telefone 0800 para que seja possível o atendimento de suporte da solução sem custos adicionaiscom ligações internacionais ou interurbano.
Suporte deverá cobrir ações técnicas corretiva durante o período de vigência da garantia o Município terá direito a suporte técnico corretivo nos equipamentos que compõem a solução.
O suporte técnico corretivo deverá ser executado pelo fabricante do equipamento ou seu representante legalmente constituído no Brasil e devidamente autorizado, de forma remota por meio de telefone e, quando necessário, no local onde se encontrar instalada a solução.

AMOSTRA E COMPROVAÇÕES DE ESPECIFICAÇÕES TÉCNICAS

Referente a validação da solução, a comissão de licitações deste processo poderá solicitar imediatamente após a apresentação da proposta, para a proponente primeiro colocada, a apresentação de amostra física (appliance) da solução da soluçãopor ela ofertada.
A apresentação deverá ocorrer em até 3 dias uteis após convocação, na sede desta prefeitura, junto ao setor de tecnologia da informação deste Município.

A proponente deverá disponibilizar amostra de equipamento com características idênticas ou superiores ao modelo por ela ofertado em sua proposta inicial.
A unidade poderá ficar em teste por até 20 dias uteis, na sede desta prefeitura para comprovar todas os recursos necessários e informados neste projeto.
A proponente deverá atender as solicitações técnicas e esclarecimentos que possam ocorrer durante esta etapa.
Na eventual validação técnica por amostra, o setor demandante irá emitir parecer sobre a solução ofertada, voltando a etapa de homologação.
Caso o equipamento será considerado inapto caberá a comissão de licitações dar andamento ao certamente convocando a próxima proponente.
Todos os custos de entrega, retirada, deslocamento inerentes aos eventos de apresentação de amostra devem ser custeados pela proponente.
Ao final dos testes os equipamentos ficarão a disposição para retirada na sede desta prefeitura, caso a proponente não recolha seus produtos em até 60 dias, o material poderá ser descartada ou doado.

TERMO DE RECEBIMENTO DA SOLUÇÃO

Após a instalação dos itens de forma satisfatória será emitido o Termo de Recebimento Definitivo da solução.
Após a emissão do Termo de Recebimento Definitivo da solução deverá ser efetuado Acompanhamento Presencial com posterior treinamento.
Após a conclusão do Acompanhamento Presencial o Município poderá utilizar-se da requisição Suporte Técnico Preventivo e/ou Corretivo.
Após a emissão do Termo de Recebimento Definitivo da solução a contratada poderá iniciar a cobrança financeira da prestação de serviços. A primeira fatura poderá ser emitida 30 dias após a entrega definitiva, caberá a contratada emitir ao todo 12 parcelas mensais neste primeiro contrato. Eventualmente o contrato poderá ser renovado com a contratada, em razão disso poderá continuar a realizar as emissões mensais até o limite estabelecido pela lei para prestaçãode serviços continuados.

Lote	Descritivo	Valor Mensal R$	Valor por anual R$
1	Disponibilização de 01(uma) solução de segurança em appliance e suaslicenças, com treinamentos, instalação e suporte tipo NOC (Network Operation Center) e/ou SOC (Security Operation Center) durante vigência contratual **Informar (Marca/Modelo/Licenças)**	4.100,00	49.200,00