TERMO DE REFERÊNCIA

Município de Ivoti

Secretaria Municipal de Administração

Necessidade da Administração: Contratação de empresa especializada na prestação de serviços de instalação, configuração, manutenção, locação de equipamentos firewall (Appliance) e gerenciamento dos sistemas de segurança, para Prefeitura Municipal de Ivoti.

1. DEFINIÇÃO DO OBJETO

Locação de equipamentos firewall (Appliance) baseada em gerenciamento unificado de ameaças (UTM) com serviço de instalação, para proteção de todos os computadores, sistemas e redes instalados no Centro Administrativo, Secretarias e Órgãos Municipais. Além de possibilitar o gerenciamento centralizado de acessos à internet, proteção AntiSpam e antivírus, conforme itens abaixo e descritivo detalhado dos itens constante no Termo de referência do edital e serviços técnicos especializados, com o objetivo de garantir a plena utilização da solução contratada, bem como sua instalação e adequação ao ambiente tecnológico da Prefeitura Municipal de Ivoti.

LOTE	ITEM	DESCRIÇÃO	UN	QTDE	VALOR UNIT
1	1.1	Contrato de Firewall de Próxima Geração - Solução composta de 2 (dois) appliance conforme termo de referência. Pacote de licenças da Console de Gerência Administrativa e Centralização de Logs e Relatórios. Pacote de licenças de Firewall, IPS, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas de firewall de próxima geração e suporte especializado durante o contrato.	Mês	36	R$ 11.666,66
	1.2	Instalação, configuração e treinamento profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado, reestruturação, instalação e integração do AD (Active Directory).	UN	1	R$ 46.333,33

TOTAL R$ 466.333,09

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Prefeitura Municipal de Ivoti possui um parque computacional de processamento de porte significativo, disponibilizando serviços de TI, na área administrativa, em servidores com médio grau de complexidade de manutenção.

O serviço a ser contratado requer profissionais habilitados e, até o momento, a Prefeitura Municipal de Ivoti não possui quantitativo suficiente em seu quadro pessoal de técnicos especializados e certificados para a realização de alguns serviços críticos de suporte e manutenção do ambiente em questão.

3. REQUISITOS DA CONTRATAÇÃO

Os serviços têm natureza comum, tendo em vista que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, nos termos do art. 6º, inciso XIII, da Lei Federal nº 14.133/2021.

A contratação será realizada preferencialmente por meio de licitação, na modalidade Pregão, na sua forma eletrônica, com critério de julgamento por menor preço, nos termos dos artigos 6º, inciso XLI, 17, § 2º, e 34, todos da Lei Federal nº 14.133/2021.

3.1. DOCUMENTAÇÃO RELATIVA À QUALIFICAÇÃO TÉCNICA

3.1.1 A empresa deverá apresentar declaração assinada pelo responsável legal indicando nomínimo um de cada técnico abaixo listados, com a devida comprovação da formação:

A. Técnico Nível Engineer Next Generation Firewall;

B. TécnicoNível Architect Next Generation Firewall;

C. Técnicocom Certificação MCSA Windows Server 2012 ou superior;

D. Técnicocom certificação LPI-2.

3.1.2 A empresa deverá indicar o DPO Data ProtectionOfficer ou Encarregado de Dados da empresa;

3.1.3 Apresentação de no mínimo, 1 (um) atestado de capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior;

3.1.4 Apresentar comprovante de que a empresa é revendedora autorizada do objeto da licitação.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. CARACTERISTICAS GERAIS DA APPLIANCE

A. Solução de segurança (APPLIANCE) baseada em gerenciamento unificado de ameaças (UTM):
B. O fabricante do software da appliance deverá estar enquadrado no quadrante mágico do Gartner na categoria Leader, Challengers, NichePlayes ou Visionaries.
C. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.
D. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.
E. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
F. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
G. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
H. O hardware e o software fornecidos 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.

4.2 CARACTERISTICAS DE HARDWARE

A. Suportar no mínimo 140.000 (cento e quarenta mil) novas conexões porsegundo;
B. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;
C. Performance mínima de 6.000 (seis mil) Mbps de performance de NGFW.
D. Possuir no mínimo 36.000 (trinta e seis mil) de rendimento (throughput) do Firewall;
E. No mínimo 6.200 (seis mil e duzentos) Mbps de rendimento (throughput) do IPS;
F. Possuir no mínimo 15000 (quinze mil) Mbps de throughput de VPN IPsec;
G. Suporte a, no mínimo, 2000 (dois mil) túneis SSL VPN;

4.3 A SOLUÇÃO PROPOSTA DEVE CORRESPONDER AOS SEGUINTES CRITÉRIOS DE THROUGHPUTEM MUNDO REAL

A. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo.
B. Entende-se como mundo real, testes realizados utilizando ambientes e protocolos usados no mundo corporativo.
C. A solução proposta deve possuir licenças baseadas nos recursos de hardware.
D. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
E. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP.
F. A solução proposta deve possuir no mínimo 120 GB de espaço em disco SSD para o armazenamento de eventos e relatórios.
G. Possuir slot de FleXiPort
H. Possuir ao menos uma porta COM (RJ45).
I. Possuir painel de LCD ou tecnologia equivalente ou superior, na parte frontal do appliance com funcionalidades básicas para ajudar na gerência do equipamento.
J. Número irrestrito de usuários/IP conectados.
K. Appliance com 1 U para montagem em rack.
L. Possuir no mínimo 8GB de memória RAM.
M. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.
N. Possuir 1 (uma) interface do tipo console ou similar.
O. Possuir 1 (uma) fonte 100-240VAC.

4.4 PROTEÇÃO WEB

A. Filtragem e Segurança Web
B. Proporcionar transparência total de autenticação no proxy, provendo segurança anti-malware e filtragem web.
C. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 80 categorias oferecidas pela solução.
D. Realizar autenticação dos usuários nos modos transparente e padrão.
E. As autenticações devem ser feitas via NTLM.
F. Possuir sistema de quotas aplicado por usuários e grupos.
G. Permitir criar políticas por horário aplicado a usuários e grupos
H. Possuir sistema de malwarescanning que realize as seguintes ações;
I. Bloquear toda forma de vírus
J. Bloquear malwares web
K. Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).
L. Proporcionar proteção de web malware avançado com emulação de Java script.
M. Prover proteção em tempo real de todos os acessos web.

N. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá se manter atualizada prevenindo novas ameaças.
O. Prover pelo menos duas engines diferentes de anti-malware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.
P. Fornecer PharmingProtection.
Q. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.
R. Permitir criação de regras customizadas baseadas em usuário e host.
S. Permitir criar exceções de URLs, usuários e host para que não sejam verificados pelo proxy.
T. Validação de certificado.
U. Prover cache de navegação, contribuindo na agilidade dos acessos à internet.
V. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)
W. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.
X. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.
Y. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.
Z. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.
AA. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.
BB. Range aceitável de 1 a 25600KB.
CC. Bloquear trafego que não segue os padrões do protocolo HTTP.
DD. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.
EE. Nas exceções, permitir definir operadores “AND” e “OR”.
FF. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.
GG. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.
HH. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.
II. Permitir criar regras de exceções por endereços IPs de origem.
JJ. Permitir criar regras de exceções por endereços IPs de destino
KK. Permitir criar exceções por grupo de usuários.
LL. Permitir criar exceções por categorias de sites.
MM. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.

NN. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance&Investing, Games andGambling”, entre outras.

OO. Permitir editar grupos de categorias preestabelecidos pela solução.

4.5 DEVE TER SISTEMA QUE PERMITA A CRIAÇÃO DE NOVAS CATEGORIAS COM AS SEGUINTES ESPECIFICAÇÕES

A. Nome da regra;

B. Permitir criar uma descrição para identificação da regra.

4.6 TER A POSSIBILIDADE DE CLASSIFICAÇÃO DE PELO MENOS

A. Produtivo;

B. Não produtivo;

C. Permitir aplicar Trafficshaping diretamente na categoria;

D. Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave;

E. Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões;

F. Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

G. Ter função para criar grupos de URLs.

H. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.

I. Permitir o administrador possa especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.

J. Deve permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado.

K. Nas configurações das políticas, deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.

L. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.

4.7 PERMITIR CRIAR COTAS DE NAVEGAÇÃO COM OS SEGUINTES REQUISITOS

A. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

4.8 CONTROLE E SEGURANÇA DE APLICAÇÕES

A. Reconhecer pelo menos 2.700 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer- to-peer, redes sociais, acesso remoto, serviços de rede, VoIP, streaming de mídia, proxy e

tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

B. Reconhecerpelomenos as seguintesaplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Vídeo, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
C. Controlar aplicações baseadas emcategorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
D. Permitir criar regras de controle por usuário e host.
E. Permitir realizar trafficshaping por aplicação e grupo de aplicações.
F. Possibilitar que as regras criadas baseadas em aplicação permitam;
G. Bloquear o trafego para as aplicações;
H. Liberar o trafego para as aplicações;

4.9 CRIAR CATEGORIZAÇÃO DAS APLICAÇÕES POR RISCO EM NO MÍNIMO 5 NÍVEIS.

A. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.
B. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
C. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.
D. Deverealizar o escaneamento e controle de micro app incluindo, mas nãolimitado a Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, Linkedin (Company Search, Compose Webmail,Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Vídeo Search, Vídeo Streaming, Upload, Website).
E. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

F. Permitir agendar um horário e data especifico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.
G. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, Porthopping e túnel através de tráfego SSL encriptado.
H. Atualizar a base de assinaturas de aplicações automaticamente.
I. Reconhecer aplicações em IPv6.
J. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory.
K. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

4.10 PROTEÇÃO PARA E-MAILS

A. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.

B. Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.

C. Bloquear SPAM e MALWARES durante a transação SMTP.

D. Possuir duas engines de antivírus para duplo escaneamento.

E. Ter proteção em tempo real, a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança caso necessário.

F. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.

G. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.

H. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customizá-los de acordo com o desejado.

I. Ter suporte a criptografia TLS para SMTP, POP e IMAP.

J. Ter a possibilidade de agregar RBLs do fabricante e terceiras para ajudar composição de segurança da ferramenta.

4.11 AS AÇÕES DOS E-MAILS CONSIDERADOD SPAM DEVEM SER

A. Drop
B. Warn
C. Quarantine

D. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: [SPAM] Marketing etc.
E. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.
F. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.
G. Possuir funcionalidade de allowlist e blocklist.
H. Possuir funcionalidade que rejeite e-mails com HELO invalido e/ou que nãopossuam RDNS.
I. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.

4.12 QUARENTENA DE E-MAIL

A. Possuir quarentena para os e-mails e opções de notificações para o administrador.
B. E-mails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.
C. O usuário deve poder gerenciar sua quarentena de e-mails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.
D. As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.
E. Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.
F. Possuir funcionalidade de criptografia de e-mails e DLP para os dados
G. Possuir funcionalidade de encriptação de e-mails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.
H. Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF.
I. Ter como funcionalidade a possibilidade de o usuário pode registrar sua própria senha de segurança para que seja possível abrir os e-mails criptografados.
J. Possuir também funcionalidade para geração de senhas aleatória para desencriptação do conteúdo.
K. Permitir enviar anexos junto aos e-mails criptografados.
L. Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não se deve utilizar qualquer software adicional, plugin, ou client instalado no equipamento.
M. Possuir funcionalidade de DLP nos E-mails
N. A engine de DLP deve ser automática na hora de escanear os e-mails e anexos, assim identificando todos os dados sensíveis encontrados no e-mail sem qualquer intervenção.
O. Possuir templates de dados considerados sensíveis preestabelecidos pelo fabricante (CCLs) com os padrões PII, PCI, HIPAA, com a intenção de ajudar o administrador na

criação das regras desejadas e seguir as principais normas do mercado, elas deverão ser mantidas pelo fabricante.

P. Ter a opção de criar exceções individuais para cada tipo de situação.
Q. As regras devem corresponder para as redes de origem e alvos específicos como a especificados por URLs.
R. Suporte a operadores lógicos.
S. Poder definir tamanho máximo para escaneamento.
T. Permitir bloquear e liberar ranges IP.
U. Suporte para utilização de Wildcards
V. Anexar automaticamente um prefixo/sufixo para autenticação.

4.13 ESPECIFICAÇÕES DA ADMINISTRAÇÃO, AUTENTICAÇÃO E CONFIGURAÇÕES EM GERAL

A. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.
B. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup)das configurações, incluindo os objetos de usuário.
C. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos e via FTP, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.
D. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.
E. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, e Directory, TACACS+ e Banco de Dados Local para autenticação do usuário.
F. A solução proposta deve suportar em modo automático e transparente “Single SignOn” na autenticação dos usuários do activedirectory e eDirectory.
G. Os tipos de autenticação devem ser, modo transparente, por autenticação Kerberus/NTLM e cliente de autenticação nas máquinas.
H. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
I. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.
J. Certificados de autenticação para iOS e Android.
K. A solução proposta deve suportar integração com Dynamic DNS de terceiros
L. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.
M. solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
N. solução proposta deve suportar NTP.

O. solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
P. solução proposta deve ter suporte multilíngue para console de administração web.
Q. solução proposta deverá suportar fazer um rollback de versão.
R. solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.
S. A solução proposta deve suportar instalação de LAN by-pass no caso do appliance
T. Estar configurado no modo transparente.
U. Solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar.
V. A solução proposta deve suportar SNMP v1, v2c.
W. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.
X. A solução proposta deve possuir serviço de “Host Dynamic DNS” sem custo e com segurança reforçada.
Y. A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno “rollback” da cópia de segurança.
Z. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.
AA. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação)
BB. A solução proposta deve ter suporte a ambientes de terminais (Microsoft e Citrix);
CC. Suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.
DD. solução deverá ser fornecida com licença capaz de gerar relatórios dinâmicos e avançados por meio de gestão cloud na própria plataforma do fabricante, com espaço mínimo de cem gigas para armazenamento de logs em ambiente computacional diretamente no fabricante, dashboard capaz de prover a visualização ampla da rede, saúde dos equipamentos, políticas e controle de eventos e segurança.

4.14 A SOLUÇÃO PROPOSTA DEVE SUPORTAR:

A. Serviço de DHCP/DHCPv6;
B. Serviço de DHCP/DHCPv6 Relay Agent;
C. Suporte a DHCP sobre VPN IPSec;
D. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.
E. Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.

F. Permitir exportar informações de troubleshooting para arquivo PCAP.

G. Permitir o factory reset e troca do idioma via interface gráfica.

H. Atualização de firmware de forma automatizada;

I. Reutilização de definições de objetos de rede, host, serviços, período de tempo, usuários, grupos, clientes e servers.

J. Portal de acesso exclusivo para usuários administradores.

K. Controle de acesso e dispositivos por zoneamento.

L. Integrar com ferramenta de gerenciamento centralizado disponibilizada pela própria fabricante.

M. Opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada dentro do próprio appliance ofertado.

N. Traps SNMP ou e-mail para notificações do sistema.

O. Suportar envio de informações via Netflow e possuir informações via SNMP.

P. Suporte a TAP mode para POCs e trials.

Q. Ter funcionalidade que permita que o administrador manualmente atribua e/ou distribua cores do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.

R. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

4.15 ESPECIFICAÇÕES DE BALANCEAMENTO DE CARGA E REDUNDÂNCIA PARA MÚLTIPLOS PROVEDORES DE INTERNET

A. A solução proposta deve suportar o balanceamento de carga e redundância para mais de 2 (dois) links de Internet.

B. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.

C. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.

D. A solução proposta deve fornecer opções de condições em caso de falha “Failover” do link de Internet através dos protocolos ICMP, TCP e UDP.

E. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

F. A solução proposta deve ter ativo/ativo utilizando algoritmo de “Round Robin” e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).

G. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

4.16 ESPECIFICAÇÕES DE ALTA DISPONIBILIDADE

A. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo.
B. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.
C. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.
D. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.
E. A solução proposta deve suportar sincronização automática e manual entre os appliances em “cluster”.
F. A solução deve suportar Alta Disponibilidade (HA) em “Bridge Mode” e MixedMode" (Gateway + Bridge).

4.17 PROTEÇÃO BÁSICA DE FIREWALL

A. Especificações do Firewall e roteamento;
B. A solução deve ser Standalone Appliance e com Sistema Operacional fortalecido “Hardening” para aumentar a segurança.
C. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.
D. Suporte a objetos e regras IPV6.
E. Suporte a objetos e regras multicast.
F. A solução proposta deve suportar “StatefulInspection” baseado no usuário “one-to-one”, NAT Dinâmico e PAT.
G. A solução proposta deve usar a “Identidade do Usuário” como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.
H. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso.
I. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.
J. Deve permitir o bloqueio de vulnerabilidades.
K. Deve permitir o bloqueio de exploits conhecidos.
L. A solução proposta deve suportar arquitetura de segurança baseado em Zonas
M. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.
N. A solução proposta deve ter predefinido aplicações baseadas na “porta/assinatura” e também suporte à criação de aplicativo personalizado baseado na “porta/número de protocolo”.
O. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como FirstAlive, Round Robin, Random,

Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.

P. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).
Q. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.
R. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.
S. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como: a senha padrão não foi alterada, acesso não seguro está permitindo ou a licença expirará em breve.
T. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.
U. A solução proposta deve suportar IPv6.
V. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.
W. A solução proposta deve suportar implementações de IPv6 Dual Stack.
X. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.
Y. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.
Z. A solução proposta deve suportar DNSv6;
AA. A solução proposta deve oferecer proteção DoS contra ataques IPv6;
BB. A solução proposta deve oferecer prevenção contra Spoof em IPv6;
CC. A solução proposta deve suportar 802.3 ad para Link Aggregation;
DD. A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação;
EE. Floodprotection, DoS, DDoS e Portscan;
FF. Bloqueio de Países baseados em GeoIP;
GG. Suporte a Upstream proxy;
HH. Suporte a VLAN DHCP e tagging;
II. Suporte a Multiple bridge.
JJ. Funcionalidades do portal do usuário
KK. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).
LL. Download dos clientes de autenticação disponibilizados pela ferramenta.
MM. Download do cliente VPN SSL em plataformas Windows.
NN. Download das configurações SSL em outras plataformas.
OO. Informações de hotspot.
PP. Autonomia de troca de senha do usuário.
QQ. Visualização do uso de internet do usuário conectado.
RR. Acesso a mensagens quarentenadas.

SS. Opções base de VPN

TT. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;DiffieHellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128,192 e 256 (AdvancedEncryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-sharedkey (PSK).

UU. L2TP e PPTP.

VV. VPN SSL, IPSEC.

WW. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

XX. Suportar autenticação via AD/LDAP, Token e base de usuários local.

YY. Funcionalidades base de QoS e Quotas

ZZ. QoS aplicado a redes e usuários de download/Upload em tráfegos baseados em serviços.

AAA. Otimização em tempo real do protocolo Voip.

BBB. Suporte a marcação DSCP.

CCC. Regras associadas por usuário.

DDD. Criar regras que limitem e garantam upload e download.

EEE. Permitir criar regra de QoS individualmente e compartilhada.

4.18 PROTEÇÃO DE REDES

A. Prover funcionalidade de IntrusionPrevention System (IPS) Proporcionar alta performance na inspeção dos pacotes

B. Possuir no mínimo 7000 assinaturas conhecidas.

C. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.

D. Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.

E. Possuir funcionalidade Anti-DoS.

F. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP, Flood, etc.

4.19 DEVE-SE PERMITIR CUSTOMIZAROS VALORES DAS SEGUINTES FUNCIONALIDADES DE DOS

A. SYN Flood;

B. UDP Flood;

C. TCP Flood;

D. ICMP Flood;

E. IP Flood;

F. Possuir templatespré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ, e etc.
G. Possuir proteção contra spoofing.
H. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.
I. Possuir funcionalidade para o administrador poder criar by-pass de DoS.
J. Permitir o administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.
K. Possuir proteção avançada contra ameaças persistentes (APT)
L. Deve detectar e bloquear trafego de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.
M. Possuir logs e relatórios que informem todos eventos de APT.
N. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.
O. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.

4.20 PROTEÇÃO PARA SERVIDORES WEB (WAF)

A. Possuir funcionalidade de proxy reverso
B. Possuir engine de URL hardening e prevenção a directorytraversal.
C. Possuir engine Form hardening.
D. Proteção contra SQL injection
E. Proteção contra Cross-site scripting
F. Possuir duas engines de antivírus disponíveis para análise de malware.
G. Permitir definir o fluxo que o antivírus atuará, se será no upload ou download.
H. Permitir limitar o tamanho máximo em que o antivírus atuará.
I. Permitir bloquear conteúdo considerado unscannable.
J. Possuir HTTPS (SSL) encryption offloading.
K. Proteção para cookie signing com assinaturas digitais.
L. Possuir Path-basedrouting.
M. Suporte ao protocolo do Outlook anywhere.
N. Possuir autenticação reversa para acesso aos servidores web.
O. Permitir criar templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.
P. Ter abstração de servidores virtuais e físicos.
Q. Proporcionar função de loadbalancer para que os visitantes possam ser jogados para diversos servidores de forma transparente.
R. Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.
S. Bloquear clients com má reputação.

T. Bloquear protocolos com anomalias.
U. Limitar número de requisições.

4.21 FERRAMENTAS DE RELATÓRIOS CENTRALIZADO

A. Permitir que todos os appliances do fabricante possam centralizar seus relatórios em um único appliance especializado para esta função ou plataforma de gestão cloud da mesma fabricante.
B. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.
C. Permitir a customização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.
D. Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails cadastrados.
E. Ter relatórios customizados e em conformidade com, pelo menos, estes órgãos; HIPAA, SOX, PCI.
F. Ter fácil identificação das atividades de rede e ataques em potencial.
G. Armazenar histórico dos relatórios em disco local.
H. Possuir relatórios únicos para cada um dos módulos ofertados pela solução.
I. Possuir multiformato de relatórios, pelo menos tabular e gráfico.
J. Permitir exportar relatórios para: PDF, Excel.
K. Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia, Google.
L. Possuir relatórios que informem principais atividades em cada módulo.
M. Ter logs em tempo real.
N. Ter logs arquivados para consulta posterior.
O. Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.
P. Possuir logs de auditoria.
Q. Ter sua gerência totalmente baseada em acesso web.
R. Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades específicas na ferramenta.
S. Deve-se detectar automaticamente um equipamento do mesmo fabricante quando este se reportar ao centralizador de relatórios, onde o administrador do sistema poderá dar um aceite ou não neste appliance que está realizando a tentativa de integração.
T. Permitir agrupamento dos equipamentos por tipo do dispositivo e modelo do equipamento.
U. O administrador deve poder acessar estes relatórios de qualquer lugar através de um navegador.
V. Ter total gerência sobre a retenção dos dados armazenados neste equipamento.
W. Ter disponibilidade em appliance virtual e software caso necessário instalar o appliance em um hardware baseado em Intel.

4.22 POSSUIR SUPORTE NO MINIMO AOS VIRTUALIZADORES

A. VMware

B. Hyper-V

C. Citrix

D. KVM

E. Proxmox

F. Possuir capacidade de armazenamento ilimitado, tendo apenas o disco como limitador.

G. Devem ser fornecidas soluções virtuais ou via appliance desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados.

H. Deve possuir mecanismo de procura de logs arquivados.

I. Deve ter acesso baseado em Web com controles administrativos distintos.

4.23 SERVIÇOS DE INSTALAÇÃO FIREWALL

A. Instalação do equipamento no rack no modo HA – ativo passivo.
B. Ativação do sistema operacional, com instalação da licença e demais particularidades do equipamento.
C. Criação de usuários para administração e gerência do equipamento.
D. Configuração de no mínimo 2 (dois) links de internet, configurações de endereços IPv4 e IPV6 públicos dos respectivos links.
E. Redirecionamento de no mínimo 15 portas da rede externa para rede DMZ, mais o redirecionamento de um range de portas para o serviço de telefonia VOIP.
F. Criação de no mínimo 4 (quatro) perfis de navegação, bloqueando conteúdo específicos por determinado perfil.
G. Integração com Microsoft Active Directory, autenticando o usuário automaticamente com as credenciais de acesso ao computador. Ativar a funcionalidade de Proxy SSL.
H. Ativar proteção AntiSpam, IPS e anti-DDOS.
I. Ativar proteção de servidores WEB.
J. Bloquear aplicações como TOR e Torrents.
K. Criar uma regra de QOS.
L. Configuração do sistema AntiSpam, se necessário
M. Reconfiguração e estruturação do AD
N. Instalação de uma nova VM
O. Instalação do AD nessa VM
P. Reconfiguração do AD com as políticas de acesso
Q. Permissão e configurações de usuários
R. Permissão e configurações de grupo
S. Política de GPO´s para acesso interno e externo

T. Política de GPO´s para maquinas internas e alterações da mesma (bloqueio de pendrive, papel de parede, instalação de novos aplicativos entre outros)
U. Permissão do uso de arquivos com histórico de alteração e resgate do original
V. Integração LDAP entre AD e Firewall
W. Integração LDAP dos Linux com AD
X. Integração e autenticador da rede no AD centralizado
Y. Integração do Firewall com AD autenticador;

4.24 INSTALAÇÃO DO AD

A. A presente deve considerar a construção e instalação do serviço de AD (Active Diretory) da Microsoft, voltada para o controle e gestão de usuários internos desta prefeitura.
B. Deverá ser criado e configurado todos ajustes necessários para o total e plena operação do serviço DNS, DHCP e AD.
C. Caso solicitado a contratada deverá instalar o AD principal e o primário, sendo esses devidamente configurados para a total e efetiva replicação.
D. O fornecimento de servidores e licenças de Windows server 2022 e suas respectivas calls ficarão a cargo da CONTRATANTE.
E. A contratada deverá criar os grupos de internet, controle de arquivos e demais grupos necessários para a efetiva operação do AD, de forma mais segura possível.
F. A contratada deverá considerar quando necessário a criação de políticas do tipo Policy ou GPO para a gestão dos computadores que possam ser conectados na rede, sendo necessária a configuração inicial para que seja padronizada a configuração das máquinas da rede.
G. A inserção de máquinas clientes no domínio ficará a cargo da CONTRATANTE, entretanto caberá a contratada passar todas as orientações e forma de gestão eficiência do ambiente do AD.
H. Caberá a contratada criar junto do setor demandante um perfil, com formato padrão, de usuário, o qual poderá permitir a posterior inclusão de novos usuários.
I. A contratada deverá criar usuários de Admin no AD para os profissionais do setor de TI, os quais serão instruídos e habilitados a executar tarefas de inclusão de usuários, grupos e dispositivos de forma simples.
J. Ao final da implementação do serviço do AD, a solução deverá ser configurada para que se realize a integração entre os usuários do AD e a navegação de internet, permitindo, desta forma, a vinculação do acesso aos usuários de forma especifica.

4.25 A CONTRATADA deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de segurança, visando garantir a transferência de conhecimento para no mínimo4 (quatro) pessoas indicadas pela CONTRATANTE.

A. O treinamento deverá ser presencial, possuir carga horária mínima de 8 (oito) horas e abranger todo o conteúdo sobre a solução.

B. As datas e horários para realização dos treinamentos serão definidos pela CONTRATANTE em comum acordo com a CONTRATADA.

C. O instrutor deverá possuir experiência em treinamentos desta natureza e pleno conhecimento da solução de segurança.

D. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%.

E. Treinamento deve ser ministrado por um técnico Nível Architect Next Generation Firewall.

4.26 ATENDIMENTO DE SUPORTE TÉCNICO

A. A licitante contratada deverá prestar suporte especializado para a infraestrutura da Prefeitura de Ivoti relacionadas a hardware ou software.

B. A contratada deverá prestar assistência técnica por via telefônica no período 24x7, em português, sem custo adicional para a Prefeitura Municipal de Ivoti

C. A contratada deverá efetuar atendimentos presenciais quando da necessidade de correções ou manutenções que possam exigir intervenção física, no local da instalação da solução, sem custos adicionais durante o contrato.

D. A contratada deverá disponibilizar ferramenta para abertura de Ticket para ordem de serviço (OS) de forma online no site da Licitante.

E. Quando necessário, mediante permissão da contratante, o atendimento ocorrerá via acesso remoto (VPN) pela Licitante nos servidores da Empresa, sem a necessidade de aquisição de licenças de software pela Prefeitura Municipal de Ivoti para realização do acesso independentemente do canal de comunicação utilizado para acionar um pedido de suporte.

F. Os acessos às estatísticas e números de atendimentos devem estar disponíveis para Prefeitura Municipal de Ivoti.

G. Independente da forma como for aberto o chamado, a contratada deverá registrar o chamado no Help Desk, mesmo que este se resolva por telefone, com o registro da hora de abertura e fechamento.

H. Os eventos devem ser acompanhados pela contratada e enviados para a equipe de suporte de TI da Prefeitura Municipal de Ivoti via e-mail.

I. O atendimento poderá ser realizado para correção de problemas, bem como para criação de regras diretamente na solução.

4.27 INFORMAÇÕES

A. Licitante vencedora se obriga a fornecer soluções em Appliance de Firewall com Gerenciamento Unificado de Ameaças (UTM – UnifiedThreatMangement), entendendo-se como tais, o conjunto de hardware e software dedicados, necessários e suficientes para o funcionamento da solução, atualização e treinamento para capacitação técnica da equipe da Prefeitura Municipal de Ivoti, de acordo com as especificações descritas no

ANEXO I – Termo de Referência. A licitante deverá indicar em sua proposta marca modelo, tipo, versão dos produtos por ela ofertado em sua proposta inicial.

B. Os equipamentos deverão ser entregues e instalados em até 45 (quarenta e cinco) dias após a ordem de início.

C. A instalação e entrega deverá ocorrer junto ao Setor de Informática, no centro administrativo da Prefeitura Municipal de Ivoti.

D. O fabricante deverá fornecer garantia dos equipamentos pelo período de vigência das licenças.

E. A vigência contratual será de 36 (trinta e seis) meses, contados da ordem de início.

F. Todas as despesas (de qualquer natureza) sejam elas tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), fornecimento de mão-de-obra especializada, leis sociais, administração, lucros, equipamentos e ferramentas, transporte de material e de pessoal, acomodações e despesas com os funcionários da contratada que executarão os serviços (alojamento, transporte, refeição, encargos sociais, trabalhistas, etc.) e demais despesas referentes à execução do objeto da presente licitação, ficarão a cargo da licitante vencedora.

5. MODELO DE GESTÃO DO CONTRATO

A gestão e a fiscalização do objeto contratado serão realizadas conforme o disposto no Decreto Municipal 23/2023, que “Regulamenta as funções do agente de contratação, da equipe de apoio e da comissão de contratação, suas atribuições e funcionamento, a fiscalização e a gestão dos contratos, e a atuação da assessoria jurídica e do controle interno no âmbito do Município de Ivoti, nos termos da Lei Federal nº 14.133/2021”.

Fica designado como fiscal o Sr Luiz Fernando Rios Cuty.

Fica designado como gestor o Secretário de Administração.

6. CRITÉRIOS DE PAGAMENTO

O pagamento da instalação será em até 30 dias após a completa instalação, cuja será atestada pelo fiscal do contrato.

O pagamento da mensalidade será efetuadoaté o 10º dia útil após a prestação do serviço.

Os pagamentos serão condicionados à adequada prestação do serviço, o que será observado pelo fiscal do contrato. Os valores somente serão liberados mediante a apresentação das notas fiscais, devidamente assinadas pelo gestor do contrato, na pessoa do (a) Secretário (a) de Administração. O pagamento será efetuado através de depósito em conta de titularidade do contratado.

7. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR/PRESTADOR DE SERVIÇO

Conforme disposto no item 3, o futuro contratado será selecionado mediante processo licitatório na modalidade Pregão Eletrônico com critério de julgamento, menor preço.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Estima-se para a contratação almejada o valor total de R$ 466.333,09.

Vislumbra-se que tal valor é compatível com o praticado pelo mercado.

9. ADEQUAÇÃO ORÇAMENTÁRIA

O dispêndio financeiro decorrente da contratação ora pretendida decorrerá da dotação orçamentária

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

3.3.3.90.40.13.00.00.00.

Ivoti, 04 de junho de 2024.

Paulo Roberto Pohren