EDITAL DE PREGÃO ELETRÔNICO N.º 82/2022
PROCESSO N.º 160/2022

1. PREÂMBULO

1.1 O Município de Pato Branco, Estado do Paraná, **UASG Nº 450996**, através do servidor ***Eduardo José Grezele,*** designado pela Administração Municipal através da Portaria n.º 1218/2021, para atuar como ***Pregoeiro***, torna público aos interessados, que realizará licitação na modalidade de Pregão Eletrônico, ***contendo lotes de participação exclusiva para microempresas e empresas de pequeno porte e lote de ampla participação,*** objetivando a locação abaixo especificada, conforme solicitação feita por todas as Secretarias e Departamentos Municipais, por meio do protocolo n.º 451136/2022, nas condições fixadas, sendo a licitação do tipo **"*menor preço*",** com critério de julgamento "***menor preço por lote"***, em conformidade com as disposições contidas na Lei nº 10.520/2002, Decreto Municipal nº 8.441, de 08 de janeiro de 2019, Decreto Municipal nº 8.574 de 01 de novembro de 2019, Lei Complementar nº 123/2006 e alterações, e subsidiariamente a Lei nº 8.666/1993 suas alterações e demais legislações pertinentes à matéria.

1.2 - Na data, horário e endereço eletrônico abaixo indicado far-se-á a abertura da Sessão Pública de Pregão Eletrônico, acessado exclusivamente por meio eletrônico **- *www.gov.br/compras***, horário oficial de Brasília - DF, conforme segue:

1.2.1 - **A SESSÃO PÚBLICA SE INICIARÁ ÀS 09 (NOVE) HORAS DO DIA 10 DE JUNHO DE 2022.**

1.3 - *Referências de Tempo:* Para todas as referências de tempo será observado o horário oficial de Brasília - DF.

1.4 - O pregão eletrônico será realizado em sessão pública, por meio da INTERNET, mediante a inserção e monitoramento de dados gerados ou transferidos para o Portal COMPRASNET através do site www.gov.br/compras.

1.5 - Os trabalhos serão conduzidos por servidor do Município de Pato Branco, denominado Pregoeiro, designado pela Administração Municipal, mediante a inserção e monitoramento de dados gerados ou transferidos para o Portal COMPRASNET.

1.6 - O inteiro teor do Edital e seus anexos poderão ser retirados gratuitamente (em mídia digital) junto a Divisão de Licitações, na Prefeitura Municipal de Pato Branco, no horário de expediente, das 08h00min às 12h00min e 13h30min às 17h30min, na Rua Caramuru, nº 271, Centro, em Pato Branco - PR, ou pelos sites: www.patobranco.pr.gov.br / www.gov.br/compras. Demais informações, fones: (46) 3220-1566, e-mail: lc@patobranco.pr.gov.br.

2. OBJETO

2.1 - A presente licitação tem por objeto a Contratação de pessoa jurídica para fornecimento de licença de uso, locação de softwares de Firewall – Next Generation, E-mail, Acesso Remoto, Automação e Antivírus, treinamento básico, atualização corretiva, adaptativa e evolutiva, diagnósticos, atendimento e suporte técnico, por tempo determinado, com fornecimento de equipamentos mediante o comodato (*hardware*), em atendimento as necessidades de todas as Secretarias e Departamentos Municipais, conforme condições e demais especificações estabelecidas no **Anexo I - Termo de Referência,** que é parte integrante deste edital, para todos os fins e efeitos.

3. DESCRIÇÃO DOS EQUIPAMENTOS E DOS SERVIÇOS:

3.1. LOTE 01: A locação da solução integrada de **Firewall *Next Generation*** é composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de:

3.1.1 - Filtro de pacotes com controle de estado.

3.1.2 - Filtro de conteúdo web.

3.1.3 - Interceptação SSL.

3.1.4 - Filtro de aplicações.

3.1.5 - Controle da web 2.0.
3.1.6 - Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos.
3.1.7 - Integrar soluções do tipo (IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, SD-WAN, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.
3.1.8 - Aquisição de solução para gerenciamento centralizado de Firewall.
3.1.9 - Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 48 meses, onde deverá ser instalado localmente e permitir a atualização do software e do sistema operacional, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.
3.1.10 - Treinamento para a equipe do Departamento de Tecnologia de Informação da Prefeitura Municipal de Pato Branco.
3.1.11 - Suporte técnico remoto (24x7).

3.2. LOTE 02: Serviços de E-mail (1):
3.2.1 - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.
3.2.2 - Possuir 600 contas de e-mail de 5 GB, totalizando 3TB, contendo antispam e antivírus.
3.2.2.1 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

3.2.3. Serviços de E-mail (2):
3.2.3.1 - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.
3.2.3.2 - Possuir 100 contas de e-mail de 30 GB, totalizando 3TB, contendo antispam, antivírus e backup ilimitado.
3.2.3.3 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

3.3. LOTE 03: Instalação e Prestação de Serviços do Módulo de Acesso Remoto e de Controle:
3.3.1 - Módulo de Acesso Remoto e de Controle para 750 máquinas
3.3.2 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior
3.3.3 - A solução deverá prover acesso diretamente por painel *web* ou via aplicação instalável
3.3.4 - A ferramenta deverá permitir e gravar opcionalmente todo e qualquer acesso remoto e manter a gravação em extensões de vídeo como: .avi,mp4 por um período configurável.
3.3.5 - A solução deverá permitir acesso remoto em primeiro e segundo plano, entende-se como acesso em segundo plano o acesso ao computador sem assumir o controle da área de trabalho do usuário.
3.3.6 - O acesso em segundo plano deverá permitir acessar ao prompt de comando e executar comandos remotamente, deverá mostrar de forma intuitiva ao usuário informações sobre aplicações, serviços, programas e *drivers* instalados, bem como possibilitar pausar, iniciar ou reiniciar um serviço do *Windows.*
3.3.7 - A solução de acesso remoto ao computador em primeiro plano deverá ao acessar a área do usuário, possibilitar o acesso a esta área, assim como permitir controlar, bloquear monitor e teclado, mouse.

3.3.8. AQUISIÇÃO E PRESTAÇÃO DE SERVIÇOS DO MÓDULO DE AUTOMAÇÃO
3.3.8.1 - Módulo de automação para 750 máquinas
3.3.8.2 - A ferramenta deverá ser integrada junto com a solução de acesso remoto.
3.3.8.3 - A ferramenta deverá conter funcionalidades para execuções de ações remotamente e agendáveis por dia, hora, semana, mês, execução imediata ou executar conforme certos critérios de configurações.

3.3.8.4 - Executar comando remoto via Prompt de Comando ou Powershell.
3.3.8.5 - Executar um arquivo em lote ou executável.
3.3.8.6 - Distribuir arquivos em todas as máquinas de forma automática.
3.3.8.7 - Atualizar registros do *Windows.*
3.3.8.8 - Instalar ou atualizar um software por .msi ou.exe.

3.4. LOTE 04: Prestação de Serviços do Módulo Antivírus:
3.4.1 - Modulo de Antivírus para 750 maquinas.
3.4.2 - A Ferramenta deverá possuir dentro da mesma solução uma central para gestão dos antivírus onde seja possível executar remotamente para um ou vários computadores.
3.4.3 - Executar varredura completa e atualizar definições de vírus.
3.4.4 - Recuperar informações mais recentes do antivírus.
3.4.5 - Ativar ou desativar proteção em tempo real.
3.4.6 - Bloquear portas *usb* dos computadores ou ainda exigir varredura imediata quando o usuário conectar em alguma porta *usb* dos computadores.
3.4.7 - A Contratada deverá entregar juntamente, o licenciamento de antivírus para 750 computadores compatíveis com os mais conhecidos no mercado, como por exemplo: Kaspersky, Bitdefender, avirá ou similares.

3.4.8. DA IMPLANTAÇÃO DOS SISTEMAS:
3.4.8.1 - Deverá contemplar a entrega técnica e o treinamento de uso da ferramenta em todos os módulos.
3.4.8.2 - A Contratada deverá orientar a equipe técnica da Contratante, de como proceder à instalação do agente e do antivírus.
3.4.8.3 - A Contratada deverá orientar a equipe técnica da Contratante, de como realizar o acesso remoto e o agendamento de tarefas.
3.4.8.4 - A Contratada deverá apresentar o escopo detalhado dos serviços contratados para equipe técnica da Contratante.

3.5. DAS ESPECIFICAÇÕES, CARACTERÍSTICAS E FUNCIONALIDADES TÉCNICAS PARA A SOLUÇÃO DE SEGURANÇA "FIREWALL UTM":
3.5.1. APPLIANCE UTM FIREWALL - Característica do Hardware:
3.5.1.1 Deverá ser entregue 02 (dois) equipamentos idênticos, para atender a necessidade de equipamento Spare (BACKUP).
3.5.1.2 O equipamento deverá ser instalado em rack, com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack.
3.5.1.3 Dispor de fonte de alimentação redundante interna, com tensão de entrada de 110V / 220V AC, automática e frequência de 50-60 Hz, Hot swapping.
3.5.1.4 Possuir painel/led indicador on/off, disco e devices de rede.
3.5.1.5 Suportar no mínimo 30.000.000 (trinta milhões) de conexões simultâneas.
3.5.1.6 Suportar no mínimo 250.000 (duzentos e cinquenta mil) novas conexões por segundo.
3.5.1.7 Possuir throughput mínimo de 12 Gbps, para tráfego IPS/IDS.
3.5.1.8 Possuir throughput mínimo de 13 Gbps, para tráfego VPN IPSEC, com criptografia (AES-128).
3.5.1.9 Possuir throughput mínimo de 07 Gbps, para tráfego VPN SSL, com criptografia (AES-128).
3.5.1.10 Possuir throughput mínimo de 12 Gbps/5.5 Gbps, para tráfego Proxy Web filter/SSL Inspection.
3.5.1.11 Possuir throughput mínimo de 6.8 Gbps, para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo).
3.5.1.12 Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000, com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch.
3.5.1.13 Possuir dispositivo de armazenamento interno de no mínimo 240GB padrão SSD.
3.5.1.14 Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento.

3.6. ESPECIFICAÇÕES GERAIS DE SOFTWARE FIREWALL NEXT GENERATION – NGFW:

3.6.1. Funções Básicas:

3.6.1.1 Hardware (Appliances) que atuam na segurança e performance do ambiente de rede.
3.6.1.2 VPN SSL, VPN IPSec (Client-to-site e Site-to-site).
3.6.1.3 Controle de Aplicações.
3.6.1.4 Proxy Web e Filtro de Conteúdo Web (URL Filtering).
3.6.1.5 Detecção e prevenção de intrusos – IPS.
3.6.1.6 Qualidade de serviço – QOS.
3.6.1.7 Anti-Malware.
3.6.1.8 SD-WAN (*Software-Defined Wide Artea Network*).
3.6.1.9 Cluster.

3.7. DAS CARACTERÍSTICAS GERAIS:

3.7.1 O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade.
3.7.2 A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 07.
3.7.3 Interface em português ou inglês.
3.7.4 Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento.
3.7.5 O sistema deverá permitir o acesso à interface de gerenciamento WEB, por qualquer interface de rede configurada.
3.7.6 O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
3.7.7 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
3.7.8 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
3.7.9 Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas.
3.7.10 A Solução deverá prover inspeção SSL:
3.7.10.1 A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho.
3.7.10.2 Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo.
3.7.10.3 Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.
3.7.10.4 Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:
3.7.10.4.1 Endereço do servidor.
3.7.10.4.2 Porta do servidor.
3.7.10.4.3 Usuário.
3.7.10.4.4 Senha.
3.7.11 Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:
3.7.11.1 Desempenho total (throughput).
3.7.11.2 Conexões simultâneas.
3.7.11.3 Usuários autenticados.
3.7.11.4 Serviços habilitados ou desabilitados.
3.7.11.5 Quantidade de endereços distribuídos pelo DHCP.
3.7.12 Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos.

3.7.13 A Solução deverá permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com o sistema central e receba a configuração.
3.7.14 Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar o sistema central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento.
3.7.15 A solução ofertada deverá permitir a criação de perfis de proteção como: a não limitação a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e deverá ser possível utilizá-los nas políticas de segurança.
3.7.16 Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV.
3.7.17 Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX).
3.7.18 A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança.
3.7.19 Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy.
3.7.20 Deverá implementar o protocolo ECMP.
3.7.21 O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.
3.7.22 Deverá possuir suporte ao protocolo de encapsulamento de redes MPLS.
3.7.23 Esta condição deverá permitir conectar links MPLS, diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

3.8. Das Funcionalidades do Firewall:
3.8.1 Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas.
3.8.2 Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH.
3.8.3 Possibilitar a visualização dos países de origem e destino nos *logs* de eventos, de acessos e de ameaças.
3.8.4 Possuir mecanismo que permita a realização de cópias de segurança (*backups*) do sistema e restauração remota, através da interface gráfica, a solução deverá permitir o agendamento diário ou semanal.
3.8.5 O sistema deverá permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
3.8.6 As cópias de segurança deverão ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup.
3.8.7 O sistema ainda deverá contemplar um recurso de cópia de segurança do tipo *snapshot* (cópia instantânea), que contemple a cópia completa das configurações dos serviços e dos recursos do sistema.
3.8.8 Deverá possibilitar a restauração do *snapshot* através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema.
3.8.9 Deverá permitir habilitar ou desabilitar o registro de *log* por política de *firewall.*
3.8.10 Possuir controle de acesso à internet por endereço IP de origem e de destino.
3.8.11 Possuir controle de acesso à internet por sub-rede.
3.8.12 Possuir suporte a tags de VLAN (802.1q).
3.8.13 Suportar agregação de links, segundo padrão IEEE 802.3ad.
3.8.14 Possuir ferramenta de diagnóstico do tipo *tcpdump*.
3.8.15 Possuir integração com Servidores de Autenticação RADIUS (Remote Authentication Dial In User Service), TACACS+, LDAP e Microsoft Active Directory.

3.8.16 Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e SSH).
3.8.17 Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
3.8.18 Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana.
3.8.19 Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br.
3.8.20 Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
3.8.21 Possuir funcionalidades de DHCP Cliente, Servidor e Relay.
3.8.22 Deverá suportar aplicações multimídia como: H.323, SIP.
3.8.23 Possuir tecnologia de firewall do tipo Stateful.
3.8.24 Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo.
3.8.25 Permitir o funcionamento em modo transparente tipo “bridge”.
3.8.26 Permitir a criação de pelo menos 20 VLANS (rede local virtual) no padrão IEEE 802.1q.
3.8.27 Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando).
3.8.28 Deverá suportar *forwarding* (encaminhamento) de multicast..2.3.29 Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP.
3.8.29 Permitir o agrupamento de serviços.
3.8.30 Permitir o filtro de pacotes sem a utilização de NAT.
3.8.31 Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
3.8.32 Possuir mecanismo de anti-spoofing.
3.8.33 Permitir criação de regras definidas pelo usuário.
3.8.34 Permitir o serviço de autenticação para HTTP e FTP.
3.8.35 Possuir a funcionalidade de balanceamento e contingência de links.

3.9 DA IDENTIFICAÇÃO DO USUÁRIO:
3.9.1 Deverá possuir a capacidade de criação de políticas de acesso de *firewall,* VPN, IPS e ao controle de aplicação integrada ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius.
3.9.2 Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
3.9.3 A solução deverá ser capaz de identificar nome do usuário, *login*, máquina/computador registrados no Microsoft Active Directory.
3.9.4 Na integração com o AD (Active Directory), todos os domain controllers em operação na rede do cliente deverão ser cadastrados de maneira simples e sem utilização de *scritps* de comando.
3.9.5 A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante.
3.9.6 A solução deverá suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o gateway (porta de entrada) tenha que fazer “queries” (consulta) no AD.
3.9.7 O UTM deverá permitir gerenciar múltiplas políticas de controles no serviço de autenticação. As políticas deverão permitir criar controles para autenticação e deverão permitir ou bloquear o acesso ao serviço de autenticação, baseado em condições e de sessão, ou seja, uma vez que o usuário esteja permitido se autenticar no serviço, a política deverá definir os parâmetros de sessão do usuário.
3.9.8 Para o sistema de controle no serviço de autenticação o produto deverá possuir no mínimo, as seguintes condições para o Controle de Autenticação:
3.9.8.1 Usuários e Grupos de Usuários.
3.9.8.2 Datas (Objetos de Datas).
3.9.8.3 Horários (Objetos de Horário).
3.9.8.4 Plataformas (Objetos de Dicionários).
3.9.8.5 Endereços Remotos (Objetos de IPv4 e IPv6).

3.9.8.6 Zona de Rede (Múltiplas Zonas).

3.10 DAS FUNCIONALIDADES DA REDE PRIVADA VIRTUAL VPN (VIRTUAL PRIVATE NETWORK):
3.10.1 Rede Privada Virtual - VPN baseada em appliance.
3.10.2 Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES.
3.10.3 Possuir suporte a VPNs IPSec site-to-site.
3.10.4 Criptografia, 3DES, AES128, AES256, AES-GCM-128, Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC.
3.10.5 Algoritmo Internet Key Exchange (IKE) versões I e II.
3.10.6 AES 128 e 256 (Advanced Encryption Standard).
3.10.7 Suporte a Diffie-Hellman (troca de chaves de maneira segura) Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30.
3.10.8 Possuir suporte a VPN SSL.
3.10.9 Possuir capacidade de realizar SSL VPNs utilizando certificados digitais.
3.10.10 Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:
3.10.10.1 Remote Desktop Protocol.
3.10.10.2 Virtual Network Computing.
3.10.10.3 SSH - Secure Shell.
3.10.10.4 WEB - World Wide Web.
3.10.10.5 SMB - Server Message Block.
3.10.10.6 Deverá permitir a arquitetura de vpn hub and spoke.
3.10.10.7 Suporte a VPNs IPSec client-to-site.
3.10.10.8 Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
3.10.10.9 Suporte à inclusão em autoridades certificadoras (enrollment = inscrição) mediante SCEP (Simple Certificate Enrollment Protocol).
3.10.10.10 Possuir funcionalidades de Auto-Dicovery VPN, capaz de permitir criar túneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).
3.10.10.11 A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de túneis:
3.10.10.11.1 Site-to-Site.
3.10.10.11.2 Full-Mesh.
3.10.10.11.3 Star.

3.11 DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO: A DETECÇÃO DE INTRUSÃO DEVERÁ SER BASEADA EM *APPLIANCE*:
3.11.1 Possuir no mínimo 25.000 (vinte e cinco mil) assinaturas ou regras de IPS/IDS.
3.11.2 O sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes.
3.11.3 Possuir tecnologia de detecção baseada em assinatura.
3.11.4 Deverá suportar a implantação em modo Gateway, *online* e em modo sniffer (farejador).
3.11.5 Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass.
3.11.6 O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança.
3.11.7 Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.
3.11.8 Possuir capacidade de remontagem de pacotes para identificação de ataques.
3.11.9 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de servidores web.
3.11.10 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
3.11.11 Mecanismos de detecção/proteção de ataques.

3.11.12 Reconhecimento de padrões.
3.11.13 Análise de protocolos.
3.11.14 Detecção de anomalias.
3.11.15 Detecção de ataques de RPC (Remote Procedure Call).
3.11.16 Proteção contra ataques de Windows ou NetBios.
3.11.17 Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol).
3.11.18 Proteção contra ataques DNS (Domain Name System).
3.11.19 Proteção contra ataques a FTP, SSH, Telnet e rlogin (logins remotos).
3.11.20 Proteção contra ataques de ICMP (Internet Control Message Protocol).
3.11.21 Alarmes na console de administração.
3.11.22 Alertas via correio eletrônico.
3.11.23 Monitoração do comportamento do appliance através de SNMP - Simple Network Management Protocol, o dispositivo deverá ser capaz de enviar traps (armadilhas) de SNMP, quando ocorrer um evento relevante para a correta operação da rede.
3.11.24 Capacidade de resposta/logs ativa a ataques.
3.11.25 Terminação de sessões via TCP resets.
3.11.26 Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos.
3.11.27 O sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços.
3.11.28 Possuir filtros de ataques por anomalias.
3.11.29 Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit.
3.11.30 Permitir filtros de anomalias de protocolos.
3.11.31 Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.
3.11.32 Suportar verificação de ataque nas camadas de aplicação.

3.12. DAS FUNCIONALIDADES DO QOS - QUALITY OF SERVICE OU QUALIDADE DE SERVIÇO:
3.12.**1** Adotar solução de Qualidade de Serviço baseada em appliance.
3.12.**2** Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
3.12.**3** Permitir modificação de valores DSCP.
3.12.**4** Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
3.12.**5** Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
3.12.**6** Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
3.12.**7** Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino.
3.12.8 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

3.13 DAS FUNCIONALIDADES DO ATP - ADVANCED THREAT PREVENTION (PREVENÇÃO AVANÇADA CONTRA AMEAÇAS):
3.13.**1** Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP.
3.13.**2** Permitir o bloqueio de malwares (adware (tipo anúncios, propagandas), spyware (tipo espião), hijackers (tipo cavalo de tróia), keyloggers, etc.).
3.13.**3** Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo.
3.13.**4** Permitir o bloqueio de download de arquivos por tamanho.

3.14. Das Funcionalidades do Proxy e do Filtro de Conteúdo Web:

3.14.1 Possuir solução de filtro de conteúdo web integrado a solução de segurança.

3.14.2 Possuir pelo menos 80 categorias para classificação de sites web.

3.14.3 Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

3.14.3.1 Webmail.

3.14.3.2 Instituições de Saúde.

3.14.3.3 Notícias.

3.14.3.4 Pornografia.

3.14.3.5 Restaurante.

3.14.3.6 Mídias Sociais.

3.14.3.7 Esporte.

3.14.3.8 Educação.

3.14.3.9 Games.

3.14.3.10 Compras.

3.14.4 Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

3.14.5 Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória.

3.14.6 Deverá permitir a definição do tamanho mínimo dos objetos salvos em cache no disco.

3.14.7 Deverá permitir a definição do tamanho máximo dos objetos salvos em cache em memória.

3.14.8 Deverá atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação.

3.14.9 Possibilitar a integração com servidores de cache WEB externos.

3.14.10 Deverá possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares.

3.14.11 Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

3.14.12 Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

3.14.13 Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante.

3.14.14 Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX, através de: base de URL própria atualizável.

3.14.15 Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual.

3.14.16 Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra.

3.14.17 Deverá permitir o bloqueio de URLs inválidas, cujo campo CN, do certificado SSL, não contém um domínio válido.

3.14.18 Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web.

3.14.19 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

3.14.20 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.

3.14.21 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem.

3.14.22 Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP.

3.14.23 Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Áudio, Vídeo e URLs originadas de Spam.

3.14.24 Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueada – lista negra.

3.14.25 Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente.

3.14.26 Deverá permitir configurar a porta do Proxy Explícito.

3.15. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES: AS FUNCIONALIDADES ABAIXO DEVEM SER BASEADAS EM *APPLIANCE*:

3.15.1 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

3.15.1.1 P2P.

3.15.1.2 Web.

3.15.1.3 Transferência de arquivos.

3.15.1.4 Chat.

3.15.1.5 Social.

3.15.2 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.

3.15.3 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

3.15.4 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

3.15.5 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.

3.15.6 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.

3.15.7 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.

3.15.8 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino.

3.15.9 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

3.16. DAS FUNCIONALIDADES DO SD-WAN - (SOFTWARE-DEFINED WAN):

3.16.1 Entende-se como tecnologia SD-WAN (Software-Defined WAN), a rede de área ampla definida por software que centraliza a gerência da rede WAN, em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN, para comunicação entre os sites remotos.

3.16.2 Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas.

3.16.3 Permitir utilizar VPN IPsec para interligar unidades remotas.

3.16.4 Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link.

3.16.5 O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes e latência.

3.16.6 Deverá possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN.

3.16.7 O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação.

3.16.8 O appliance SD-WAN deverá permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado veja avaliado. Deverá suportar especificar um valor variando de 01 a 100.

3.16.9 O recurso de SD-WAN deverá permitir o monitoramento de no mínimo 03 (três) endereços alvos, para verificar a disponibilidade e desempenho do link.

3.16.10 A solução de SD-WAN UTM, deverá permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN, de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras.

3.16.11 Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

3.16.11.1 Consumo de banda.

3.16.11.2 Perda de pacotes.

3.16.11.3 Jitter.

3.16.11.4 Latência.

3.17. **DA ALTA DISPONIBILIDADE:**

3.17.**1** Possuir mecanismo de alta disponibilidade operando em modo Ativo/Standby, com as implementações de Failover (tolerância as falhas).

3.17.**2** Não serão permitidas soluções de cluster (HA), que façam com que o equipamento reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

3.17.**3** O sincronismo dos servidores deverá ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

3.18. DAS SOLUÇÕES DE GERENCIAMENTO CENTRALIZADO DE FIREWALL:

3.18.**1** Funcionalidades de Gerenciamento:

3.18.**1.1** Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto.

3.18.1.2 A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewalls contratados.

3.18.**1.3** O gerenciamento centralizado poderá ser entregue como *appliance* físico ou virtual. Caso seja entregue em *appliance* fisíco deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em *appliance* virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o *appliance* virtual é responsabilidade da Contratante.

3.18.**1.4** Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento.

3.18.**1.5** A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica.

3.18.**1.6** Deverá manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de *logs* e emissão de relatórios.

3.18.**1.7** A solução deverá incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador.

3.18.**1.8** A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

3.18.1.9 Deverá possibilitar a realização de “backup” e restauração de dados.

3.18.**1.10** Deverá possibilitar o envio dos *“logs”* gerados a outro concentrador de *“logs”* externo a solução.

3.18.1.11 Deverá possibilitar a gerência de *“logs”,* realizando as configurações de relatórios de todos os “firewalls” integrados.

3.18.**1.12** Deverá permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

3.18.**1.13** O gerenciamento deverá permitir/possuir:

3.18.**1.13.1** Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas.

3.18.**1.13.2** Monitoração de *logs*.

3.18.**1.13.3** Debugging (depuração).

3.18.**1.13.4** Acesso concorrente de administradores.

3.18.**1.13.5** Deverá permitir usar palavras chaves para facilitar identificação de regras.

3.18.**1.13.6** Definição de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

3.18.**1.13.7** Autenticação integrada à base de dados local.

3.18.**1.13.8** Deverá possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, sub rede) na base de regras.

3.18.**1.13.9** Criação de regras que fiquem ativas em horário definido.

3.18.**1.13.10** Backup das configurações e rollback de configuração para a última configuração salva.

3.18.1.13.11 Habilidade de upgrade via interface de gerenciamento.
3.18.1.13.12 Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado.
3.18.1.13.13 Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções.
3.18.1.13.14 Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção.
3.18.1.13.15 Deverá permitir a criação de objetos e políticas compartilhadas.
3.18.1.13.16 Capacidade de definir administradores com diferentes perfis de acesso com no mínimo, as permissões de Leitura/Escrita e somente Leitura.
3.18.1.13.17 Solução deverá ser capaz de detectar ataques de tentativa de *login* e senha utilizando tipos diferentes de credencias.
3.18.1.13.18 O sistema deverá ser capaz de gerenciar de modo central as políticas de backup dos equipamentos remotos.
3.18.1.13.19 O sistema deverá permitir habilitar uma mensagem de disclaimer (isenção de responsabilidade) na página de *login* da Interface de Administração. Ou seja, a página de *login* deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.
3.18.1.13.20 Deverá suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada.
3.18.1.13.21 Deverá suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider).

3.19 DAS FUNCIONALIDADES DE ANÁLISE DE LOG:
3.19.1 Deverá prover análise de tráfego de rede de modo centralizado.
3.19.2 Deverá possuir análise de tráfego de rede e ameaças por geolocalização.
3.19.3 Deverá ser capaz de receber os *logs* e eventos com o objetivo de prover os seguintes tipos de análises:
3.19.3.1 Análise de ameaças e incidentes de segurança.
3.19.3.2 Análise de tráfego e uso de categorias Web.
3.19.3.3 Análise de tráfego e uso de aplicativos.
3.19.3.4 Análise de tráfego e ameaças por usuário.
3.19.3.5 Análise de desempenho de políticas de segurança.
3.19.3.6 A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de *logs*, consolidação de *logs*, arquivamento de *logs*, busca avançada de *logs.*
3.19.3.7 Deverá possuir ferramenta para salvar consultas avançadas.
3.19.3.8 Deverá possuir relatórios personalizados.
3.19.3.9 Deverá ser capaz de efetuar o arquivamento de relatórios.
3.19.3.10 Deverá possuir agendamento de relatórios.
3.19.3.11 Os relatórios deverão no mínimo, serem exportados em formatos flexíveis (PDF, CSV).

4. JUSTIFICATIVA
4.1 - **O *firewall*** é um ativo de segurança da informação, fundamental numa rede de dados, uma vez que ele regula e monitora todo o tráfego de entrada e saída na rede de computadores.
4.2 - Por meio da introspecção dos dados de rede, *o firewall* é capaz de bloquear acessos não autorizados ou nocivos, mediar o uso de internet, criar conexões de rede seguras, bem como oferecer atualizações para ameaças.
4.3 - As soluções de *firewall* da próxima geração (*Next Generation Firewall*) são tecnologias modernas que representam um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes confiáveis (rede interna) e não confiáveis (*Internet*) e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Isso é possível, através de um

sistema de detecção de intrusões, *anti-malware* na camada de rede, filtragem de tráfego *web* malicioso e a inspeção de tráfego SSL, na busca de ameaças camufladas sobre acamada de criptografia.
4.4 - Tendo em vista a pandemia que se iniciou no ano de 2020 de COVID-19, junto com as medidas adotadas para tentar frear a contaminação da população, houve uma mudança no paradigma da interação das pessoas com a procura de serviços públicos, demandando da gestão, disponibilizar mais serviços no âmbito da internet, impactando na atual estrutura de Tecnologia de Informação do município.
4.5 - Essa estrutura, principalmente a de *firewall e e-mail,* está muito defasada, ocasionando problemas frequentes como: longas interrupções na internet, lentidão para navegação, lentidão de sistemas hospedados em nuvens e falta de espaço local para mais contas de *e-mail* que o município necessite.
4.6 - Com essa defasagem de equipamento, pode ocorrer uma parada crítica onde o mesmo não volte mais a funcionar, tendo forte impacto nos serviços disponibilizados e incapacidade de alguns setores de atender ao público, entre outros serviços internos.
4.7 - Hoje, *e-mail* e *firewall* se encontram em um mesmo equipamento, próprio do município e nele estão os softwares, os quais não possuem mais suporte caso ocorra algum problema, pois o fabricante descontinuou a versão desde o ano de 2018. Sendo assim, além dos problemas citados acima, ainda ocorre que esse tipo de estrutura fica muito vulnerável a *cyber*-ataques, colocando em risco a segurança das informações.
4.8 - Além dessas constatações, ainda está em processo de migração para *cloud computing* (computação em nuvem) o *software* utilizado na Secretaria Municipal de Saúde, o qual será utilizado em nuvem onde terá uma grande necessidade de controle de tráfego de internet, na qual a estrutura atual mesmo sem esse acréscimo, já apresenta falhas freqüentes.
4.9 - Com todos esses avanços necessários, aumentará ainda mais o tráfego de dados na rede, e ainda considerando que atualmente o município possui um equipamento não apropriado e *software* de *firewall* e *e-mail* defasados, será imprescindível proteger o que entra ou sai da rede interna da prefeitura. Para realizar essa proteção, é necessário equipamento com especificações superiores – *Next Generation Firewall*, uma vez que o tráfego a ser analisado será substancialmente maior.
4.10 - Os **gerenciadores de e-mails** são programas para computadores que gerenciam contas de e-mail, para que possam ser operadas sem o uso de navegadores.
4.11 - O **acesso remoto** permite tanto que seus colaboradores acessem dados, e-mails e outros tipos de documentos por meio de qualquer dispositivo, como também possibilita que o suporte técnico de uma empresa manipule uma máquina e solucione o problema sem estar presente no mesmo local.
4.12 - Através da instalação e configuração de **módulos de automação (I/O - Input/Output)** e suas respectivas licenças no software de gerenciamento do CFTV é possível integrar, por exemplo, um sistema de controle de acesso, permitindo monitorar status de equipamentos e, também, controlar os mesmos.
4.13 - Os sistemas I/O (Input/Output) são módulos que têm a função de organizar e controlar o fluxo de dados produzidos pelas máquinas da empresa (entrada/input e saída/output).
4.14 - Os módulos de I/O geralmente executam algumas das seguintes funções: controle e temporização, comunicação com o processador, comunicação com periférico, armazenamento temporário de dados e detecção de erros.
4.15 - O **módulo de antivírus** serve para scanear ativamente os dados transferidos ao navegar na internet para evitar que malware seja baixado e executado no computador.
4.16 - Podemos citar alguns benefícios deste módulo como: segurança, automação, locais de trabalho mais seguros e aeroportos mais rápidos.

5. CONDIÇÕES PARA PARTICIPAÇÃO
5.1 - Poderá participar desta licitação qualquer empresa legalmente constituída, com ramo de atividade compatível com o objeto da presente licitação, desde que satisfaça as exigências deste edital e esteja devidamente cadastrada no Portal COMPRASNET, através do site www.gov.br/compras.
5.2 - Para acesso ao sistema eletrônico, os interessados em participar do Pregão Eletrônico deverão dispor de chave de identificação e senha pessoal (intransferíveis), obtidas através do portal de compras governamentais.
5.3 - O licitante responsabiliza-se exclusiva e formalmente pelas suas transações efetuadas, assumindo como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por

seu representante, excluída a responsabilidade do provedor do sistema ou do órgão promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

5.4 - NÃO PODERÃO PARTICIPAR DA PRESENTE LICITAÇÃO, além dos elencados no art. 9º da Lei 8.666/93:

5.4.1 - Empresas cujo objeto social não seja pertinente e compatível com o objeto deste pregão.
5.4.2 - Os interessados que se encontrem, mesmo que indiretamente, sob falência, concordata, recuperação judicial, (exceto empresas com plano de recuperação acolhido judicialmente, e empresas em recuperação extrajudicial, com plano de recuperação homologado judicialmente), dissolução, liquidação ou em regime de consórcio, qualquer que seja sua forma de constituição.
5.4.3 - Empresas estrangeiras que não funcionem no país.
5.4.4 - Aqueles incursos nas sanções previstas no inciso III, Artigo 87 da Lei 8.666/93, quando aplicada pelo Município de Pato Branco.
5.4.5 - Aqueles que tenham sido declarados impedidos e/ou inidôneos para licitar ou contratar com a administração pública.
5.5 - A participação na licitação e apresentação da proposta implica na integral e incondicional aceitação de todos os termos, cláusulas e condições deste Edital e de seus anexos, ressalvado o disposto no parágrafo terceiro do art. 41 da Lei 8.666/93 e suas alterações posteriores.
5.6 - O licitante deve arcar com todos os custos associados à preparação e envio de sua proposta e em hipótese alguma a Contratante será responsável ou estará sujeita a esses custos.
5.7 - Para formulação da sua proposta de preços, a licitante deverá observar o descritivo contido neste edital, bem como as demais especificações e exigidas em editas e seus anexos.
5.8 - Como condição para participação no Pregão, a licitante deverá informar, em campo próprio do sistema eletrônico, quanto ao atendimento de:
5.8.1 - Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123/2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, se for o caso da licitante;
a) Caso a licitante assinale o campo "*não*" nos itens de participação exclusiva para microempresas e empresas de pequeno porte, ficará impedida de registrar sua proposta para esses itens;
b) Caso a licitante assinale o campo *"não"* nos itens de ampla participação de empresas, produzirá o efeito de o licitante não ter direito ao tratamento favorecido na Lei Complementar 123/2006 e alterações, mesmo ser enquadrada como microempresa e empresa de pequeno porte.
5.8.2 - Que está ciente e concorda com as condições contidas em Edital e seus anexos;
5.8.3 - Que cumpre os requisitos para habilitação definidas em Edital e que a proposta a ser apresentada está em conformidade com as exigências dispostas em edital e seus anexos;
5.8.4 - Que inexistem fatos impeditivos para a sua habilitação ao certame, e que está ciente da obrigatoriedade de informar ocorrências posteriores;
5.8.5 - Que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;
5.8.6 - Que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009;
5.8.7 - Que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
5.8.8 - Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.
5.8.9 - A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

6. ESCLARECIMENTOS E IMPUGNAÇÃO DO ATO CONVOCATÓRIO

6.1 - Qualquer cidadão poderá solicitar esclarecimentos, providências ou impugnar os termos do presente Edital por irregularidade, protocolizando o pedido até **três dias úteis** antes da data fixada para a realização do Pregão.

6.2 - Decairá do direito de impugnar os termos do presente Edital a licitante ou cidadão que não apontar as falhas ou irregularidades supostamente existentes no Edital até o terceiro dia útil que anteceder à data de realização do Pregão.

6.3 - A impugnação feita tempestivamente pela licitante não a impedirá de participar do processo licitatório, ao menos até o trânsito em julgado da decisão a ela pertinente.

6.4 - O termo de impugnação ou o esclarecimento poderá ser protocolado junto a Prefeitura Municipal de Pato Branco na Rua Caramuru, nº 271, Centro, em Pato Branco-PR, ao Pregoeiro responsável ***ou*** encaminhado por meio eletrônico, via e-mail: lc@patobranco.pr.gov.br

6.4.1 - Após o envio do e-mail, o responsável pelo envio deverá entrar em contato com o pregoeiro para confirmar o recebimento do e-mail e do seu conteúdo.

6.4.2 - O pregoeiro não se responsabilizará por *e-mails* que, por qualquer motivo, não forem recebidos em virtude de problemas no servidor ou navegador, tanto do Município de Pato Branco quanto do emissor.

6.5 - Incumbe ao Pregoeiro, auxiliado pelo setor requisitante do processo, decidir sobre os pedidos de esclarecimentos e impugnações no prazo de até dois dias úteis contados da data de recebimento do pedido.

6.6 - A impugnação não possui efeito suspensivo

6.6.1 - A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação

6.7 - As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

6.8 - Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame.

7. CREDENCIAMENTO

7.1 - O licitante deverá estar previamente cadastrado junto ao Sistema de Cadastramento Unificado de Fornecedores - SICAF, que deverá ser feito junto ao Portal de Compras do Governo Federal, no sítio www.gov.br/compras, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira - ICP Brasil.

7.1.1 - O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

7.1.2 - O Licitante interessado deverá realizar o seu **cadastramento** e proceder ao seu **credenciamento** de acordo com os procedimentos do Sistema.

7.1.3 - O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para a realização das transações inerentes a este pregão.

7.2 - É de responsabilidade do licitante conferir a exatidão de seus dados cadastrais junto ao SICAF, devendo mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, a sua correção ou a alteração dos registros tão logo identifique incorreções ou aqueles que se tornem desatualizados.

8. APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO NO SISTEMA

8.1 - Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

8.2 - Serão consideradas inválidas as propostas e documentos de habilitação apresentadas por quaisquer outros meios.

8.3 - O envio da proposta e dos documentos de habilitação exigidos em edital ocorrerá por meio de chave de acesso e senha da licitante.

8.4 - Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.
8.5 - As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da Lei Complementar n.º 123/2006 e alterações.
8.6 - Os preços e os produtos/serviços propostos são de exclusiva responsabilidade da licitante, assumindo como firmes e verdadeiras suas propostas e lances, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
8.7 - EM CASO DE DIVERGÊNCIA, EM RELAÇÃO AO DESCRITIVO CONSTANTE NO EDITAL E NO PORTAL COMPRASNET, PREVALECERÁ O DESCRITIVO DO EDITAL.
8.8 - Ao oferecer sua proposta no sistema eletrônico, o licitante deverá observar rigorosamente a descrição dos itens e considerar as condições estabelecidas no Edital e seus anexos, descrevendo detalhadamente as ***características do objeto ofertado, informando em campo próprio do sistema, marca (se for o caso), preço unitário por item, com até duas casas decimais após a vírgula***.
8.9 - A validade da proposta será de no mínimo 90 (noventa) dias, contados a partir da data da sessão pública do Pregão.
8.10 - Nos valores propostos deverão estar inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais, tributos, fretes e carretos, inclusive ICMS e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens ou da prestação de serviços, de forma que o objeto do certame não tenha ônus para o Município de Pato Branco.
8.11 - Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.
8.12 - Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

8.13 - A HABILITAÇÃO DO LICITANTE SERÁ AFERIDA POR INTERMÉDIO DOS SEGUINTES DOCUMENTOS:
8.13.1 - A documentação relativa à HABILITAÇÃO JURÍDICA, conforme o caso consistirá em:
a) Registro comercial, no caso de empresa individual.
b) Ato constitutivo, estatuto ou contrato social em vigor (e a última alteração contratual), devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.
c) Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.
d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.
e) Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

8.13.2 - A documentação relativa à REGULARIDADE FISCAL E TRABALHISTA consistirá em:
a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF).
b) Prova de inscrição no Cadastro de Contribuinte Estadual ou Municipal, relativa ao domicílio ou sede da proponente, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
c) Prova de regularidade para com a Fazenda Federal mediante apresentação de **Certidão Conjunta de Débitos relativos a Tributos Federais e a Dívida Ativa da União**, expedida pela Receita Federal do Ministério da Fazenda.
d) Prova de regularidade para com a **Fazenda Estadual** do domicílio ou sede do licitante, ou outra equivalente, na forma da Lei.
e) Prova de regularidade para com a **Fazenda Municipal** do domicílio ou sede do licitante, ou outra equivalente, na forma da Lei.

f) Certificado de Regularidade para com o **Fundo de Garantia por Tempo de Serviço (FGTS)**, demonstrando situação regular no cumprimento dos encargos sociais instituídos por Lei.
g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **Certidão Negativa de Débitos Trabalhistas (CNDT)**, emitida eletronicamente através do site http://www.tst.jus.br.

8.13.2.1 - As microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.
8.13.2.2 - Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, desde que atendidos os demais requisitos do Edital, as empresas nesta condição serão declaradas habilitadas sob condição de regularização da documentação no prazo de 05 (cinco) dias úteis, prorrogáveis por igual período, a critério da Administração Pública.
8.13.2.3 - A não regularização da documentação, no prazo previsto no item supra, implicará na decadência do direito à contratação, sem prejuízo das sanções previstas no Artigo 81 da Lei nº 8.666/93, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura da Ata de Registro de Preços, ou revogar a licitação.
8.13.2.4 - Na falta da regularização da documentação, no mesmo prazo previsto, a Administração poderá aplicar a multa de 10% (dez por cento) do valor total do objeto licitado pela proponente vencedora da licitação.

8.13.2.5 - Será considerada microempresa aquela que tiver auferido receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais), e empresa de pequeno porte aquela que tenha auferido receita bruta superior à R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais), nos termos da Lei Complementar nº 123, de 14 de dezembro de 2006 e suas posteriores alterações. Sendo comprovada através do balanço patrimonial exigido como comprovação de qualificação econômica no item 8.13.3, a.

8.13.3 - A documentação relativa à QUALIFICAÇÃO ECONÔMICO-FINANCEIRA consistirá em:
a) Balanço patrimonial e demonstrações contábeis referentes ao último exercício social, já exigíveis e apresentados na forma da lei, vedada sua substituição por balancetes ou balanços provisórios. O balanço das sociedades anônimas ou por ações deverá ser apresentado em publicação no Diário Oficial.
I - No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.
II - Os microempreendedores individuais deverão apresentar o balanço patrimonial e as demonstrações contábeis como condição de qualificação econômico-financeira, nos termos do subitem 8.13.3, a.

b) Certidão Negativa de Falência e Concordata expedida pelo Cartório Judicial Distribuidor da Comarca da sede da pessoa jurídica, em data não anterior a 90 dias da abertura da sessão pública deste PREGÃO, se outro prazo não constar no documento.
c) Certidão Negativa de Recuperação Judicial, expedida pelo Cartório Judicial Distribuidor da Comarca da sede da pessoa jurídica, em data não anterior a 90 dias da abertura da sessão pública deste PREGÃO, se outro prazo não constar no documento.
8.13.3.1 - As proponentes que se encontram, mesmo que indiretamente, sob recuperação judicial ou extrajudicial deverão apresentar plano de recuperação que já tenha sido acolhido e/ou homologado (quando for o caso) pelo juízo competente.

8.13.4 – A documentação relativa à QUALIFICAÇÃO TÉCNICA consistirá em:
a) Para o Lote 01: Apresentar certificado de capacidade técnica, comprovando que a Contratada possui 01(um) ou mais técnicos habilitados para execução do serviço. O atestado, ou diploma, ou certificado, ou qualquer outro documento de comprovação só será aceito, se for emitido pelo fabricante.

8.13.4.1. COMISSÃO AVALIADORA
8.13.4.1.1 - Será composta pelos seguintes servidores:
a) Eduardo Mello Amorim, matrícula nº 10.145-1/1;

b) Carlos Henrique Bazzi, matrícula nº 7.228-1/1;
c) Douglas Luiz Mondstock, matrícula nº 7.212-5-/1.

8.13.5 - DECLARAÇÕES
a) Declaração da Licitante Unificada de idoneidade, cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, declaração de comprometimento e cumprimento ao art. 9º, inciso III da Lei 8.666/93.

8.14 - O CADASTRO no SICAF, ou Certificado de Registro Cadastral (CRC) emitido pela Divisão de Licitações do Município de Pato Branco **(DESDE QUE VÁLIDO)** poderá substituir os documentos indicados nos subitens **8.13.1, 8.13.2, 8.13.3, "a"**, sendo que é obrigatória a apresentação dos demais documentos.
8.14.1 - Na hipótese dos documentos se encontrarem vencidos no referido sistema (SICAF) ou no CRC, o licitante deverá encaminhar, juntamente com os demais, o documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvando o disposto quanto à comprovação da regularidade fiscal das microempresas ou empresas de pequeno porte, conforme disposto na Lei Complementar nº 123/2006, alterada pela Lei Complementar nº 147/2014.
8.14.2 - Também poderão ser consultados os sítios oficiais emissores de Certidão de Regularidade Fiscal e Trabalhista, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

9. ABERTURA, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DOS LANCES
9.1 - A abertura da presente licitação dar-se-á em sessão pública, por meio do sistema eletrônico, na data, horário e local indicado neste edital, momento no qual o pregoeiro passará a avaliar a aceitabilidade das propostas.
9.2 - Aberta a etapa competitiva (lances), os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.
9.3 - Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
9.4 - Durante o transcurso da sessão pública os participantes serão informados, em tempo real, do valor do menor lance registrado, sendo vedada a identificação das licitantes antes do término da fase de lances.
9.5 - Será desclassificada a proposta que identifique o licitante.

9.6 - Para o envio de lances do presente processo, o modo de disputa será o modo "***ABERTO E FECHADO".*** Neste modo os licitantes deverão apresentar lances públicos e sucessivos, com lance final e fechado.
9.6.1 - A etapa de lances terá duração inicial de 15 (quinze) minutos. Depois desse prazo, o sistema encaminhará o aviso de fechamento iminente de lances, após o qual transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.
9.6.2 - Encerrado o prazo previsto no item 9.6.1, o sistema abrirá a oportunidade para que os licitantes detentores da oferta de menor preço e das ofertas superiores em até 10% (dez por cento) ao de menor preço possam ofertar um lance final e fechado em até 5 (cinco) minutos.
9.6.2.1 - A etapa a que se refere o item 9.6.2 ocorrerá de forma sigilosa até transcorrer o tempo indicado.
9.6.2.2 - Na ausência de no mínimo três ofertas nas condições que trata o item 9.6.2, serão convocados, na ordem de classificação, os detentores dos melhores lances, até o máximo de três, para que ofereçam um lance final e fechado no prazo de 5 (cinco) minutos que ocorrera da mesma forma do disposto no item 9.6.2.1.
9.6.3 - Encerrados os prazos previstos nos itens 9.6.2, o sistema ordenará os lances em ordem crescente de valores.
9.6.4 - Na ausência de lance final e fechado na forma estabelecida no item 9.6.2, haverá o reinício da etapa fechada, oportunizando para os demais licitantes, na ordem de classificação até o máximo de três,

possam ofertar lance final e fechado no prazo de 05 (cinco) minutos, que ocorrerá da mesma forma do disposto no item 9.6.2., sendo que após esta etapa será observado o disposto no item 9.6.3.
9.6.5 - Caso não haja licitante classificado na etapa de lance e que atenda as exigências de habilitação, poderá o pregoeiro e sua equipe de apoio admitir o reinício da etapa fechada, desde que devidamente justificado.
9.7 - Encerrada a etapa de lances, o pregoeiro examinará a proposta de preços classificada em primeiro lugar quanto ao cumprimento dos requisitos exigidos no Edital, momento em que encaminhará pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.
9.7.1 - A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
9.8 - Se a proposta ou o lance de menor valor não for aceitável ou se o fornecedor desatender às exigências habilitatórias, o Pregoeiro examinará a proposta ou o lance subseqüente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital.
9.9 - Caso não sejam apresentados lances, será verificada a conformidade dos valores obtidos na etapa de "Abertura das Propostas" ou resultado de possível negociação.
9.10 - Constatando o atendimento das exigências fixadas no Edital, o objeto será adjudicado ao autor da proposta ou lance de menor preço.
9.11 - NÃO SERÃO ADJUDICADOS VALORES ACIMA DOS VALORES DE REFERÊNCIA ESTABELECIDOS NO ITEM 2.1 DO TERMO DE REFERÊNCIA CONSTANTE NO ANEXO I DESTE EDITAL.

10. JULGAMENTO DAS PROPOSTAS DE PREÇOS
10.1 - Para julgamento será adotado o critério de "***MENOR PREÇO POR LOTE"***, observado o prazo para execução, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste Edital e seus Anexos.
10.2 - O valor apresentado deverá incluir todas as despesas necessárias para fornecimento e execução do objeto da presente licitação, inclusive quanto ao frete, com cotação em moeda corrente nacional, em até duas casas decimais, expresso em algarismos.
10.3 - A presente licitação contém lotes de participação exclusiva para Microempresa e Empresa de Pequeno Porte e lote de ampla participação de empresas.
10.3.1 – Para o Lote 01: Ampla participação.
10.3.2 – Para os Lotes 02, 03 e 04: Exclusivo para microempresas e empresas de pequeno porte.
10.4 - Após a etapa de envio de lances, haverá a aplicação dos critérios de desempate previstos nos art. 44 e art. 45 da Lei Complementar nº 123, de 14 de dezembro de 2006.
10.4.1 - Na hipótese de persistir o empate, será realizado sorteio pelo sistema eletrônico dentre as propostas empatadas.
10.5 - Nos casos de não haver lances, após a etapa competitiva, os critérios de desempate serão aplicados nos termos do subitem 10.4.
10.5.1 - Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

11. ENVIO DOS DOCUMENTOS COMPLEMENTARES DE HABILITAÇÃO, APRESENTAÇÃO DA PROPOSTA DE PREÇOS AJUSTADA
11.1 - Encerrada a etapa de lances, o pregoeiro convocará o licitante detentor da melhor oferta, **item a item,** para que este anexe a PROPOSTA DE PREÇOS no prazo de até 02h (duas horas úteis), em conformidade com o último lance ofertado.
11.2 - Caso seja necessário, o pregoeiro convocará o licitante detentor da melhor oferta para que este anexe documentação complementar, no prazo de até 02h (duas horas úteis).
11.2.1 - Poderão ser solicitados também, documentos de habilitação complementares, desde que necessários a confirmação daqueles exigidos em edital e já apresentados, nos termos do item 8.1 deste Edital, dentro do prazo estabelecido no item 12.2.

11.2.2 - Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhadas por meio eletrônico, ou se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

11.2.3 - O licitante deverá anexar a documentação convocada em arquivo único (Compactado ex.: zip ou pdf), no sistema COMPRASNET.

11.3 - Os prazos estabelecidos poderão ser prorrogados pelo Pregoeiro por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.
11.4 - Em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail: lc@patobranco.pr.gov.br. Após o envio do e-mail, o responsável pelo envio deverá entrar em contato com o pregoeiro para confirmar o recebimento do e-mail e do seu conteúdo. O pregoeiro não se responsabilizará por *e-mails* que, por qualquer motivo, não forem recebidos em virtude de problemas no servidor ou navegador, tanto do Município de Pato Branco quanto do emissor.
11.5 - Encerrado o prazo determinado, sem que os documentos tenham sido anexados ou a documentação esteja incompleta, o licitante terá sua proposta recusada.

11.6 - A PROPOSTA DE PREÇOS AJUSTADA DEVERÁ SER APRESENTADA CONTENDO:
11.6.1 - Razão social ou denominação social, número do CNPJ, endereço completo, com CEP e os números de veículos de comunicação à distância (telefone, e-mail) da empresa, redigida com clareza, sem emendas, rasuras ou borrões, acréscimos ou entrelinhas, devidamente datada e assinada pelo representante legal da empresa (se Procurador acompanhado da respectiva Procuração) e conter a descrição **completa dos itens vencidos, quantidade estimada, marca (se for o caso) preço unitário final proposto e preço total estimado por item, considerando até dois algarismos após a vírgula, prazo de validade da proposta mínimo 90 (noventa) dias, conforme modelo de proposta, ANEXO IV deste Edital.**

11.7 - Os Documentos remetidos por meio do Sistema Comprasnet, ou que eventualmente tenham sido enviados através do e-mail, **poderão** ser solicitados em original ou cópia autenticada em prazo a ser estabelecido pelo Pregoeiro.
11.7.1 - Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais ou cópia autenticada quando houver dúvida em relação à integridade do documento digital.
11.7.2 - Neste caso, os documentos, caso sejam solicitados, deverão ser encaminhados à Divisão de Licitações da Prefeitura Municipal de Pato Branco - PR, situada no endereço: Rua Caramuru, 271 - CEP: 85.501-064 - Pato Branco - PR, aos cuidados do Pregoeiro.

12. DISPOSIÇÕES GERAIS DE HABILITAÇÃO

12.1 - A confirmação de regularidade perante os órgãos oficiais será realizada junto aos “sites” na INTERNET.
12.2 - Todos os documentos exigidos para habilitação deverão estar dentro dos respectivos prazos de validade.
12.3 - Para que a licitante seja considerada vencedora, além de ter sua proposta aceita, deverá enviar todos os documentos previstos no edital dentro do prazo estipulado.
12.4 - Não serão aceitos documentos em forma de ‘FAX ou equivalente’ e nem a apresentação de protocolo ou comprovantes de pagamento em substituição a documento solicitado como definitivo.
12.5 - Sob pena de inabilitação, todos os documentos apresentados deverão estar:
a) em nome do licitante, com número do CNPJ e endereço respectivo.
b) em nome da sede (matriz), se o licitante for à sede (matriz).
c) em nome da filial, se o licitante for à filial, salvo aqueles documentos que, pela própria natureza, comprovadamente forem emitidos somente em nome da sede (matriz).

12.6 - A falta de quaisquer documentos ou o descumprimento das exigências previstas nos subitens anteriores implicará a INABILITAÇÃO do licitante e sua consequente exclusão do processo.
12.7 - Havendo superveniência de fato impeditivo, fica o licitante obrigado a declará-lo, sob as penalidades legais cabíveis.
12.8 - A apresentação da proposta por parte do licitante significa o pleno conhecimento e sua integral concordância e adesão para com as cláusulas deste edital e seus respectivos anexos.
12.9 - Como condição para celebração do Contrato, o licitante vencedor deverá manter as mesmas condições de habilitação.

13. RECURSOS ADMINISTRATIVOS
13.1 - **Declarado o vencedor**, qualquer Licitante poderá, em campo próprio do sistema, manifestar sua intenção de interpor recurso, quando lhe será concedido o prazo de três dias úteis para apresentar as razões do recurso, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.
13.2 - A falta de manifestação imediata e motivada do Licitante quanto à intenção de recorrer importará na decadência desse direito, ficando o Pregoeiro autorizada a adjudicar o objeto ao Licitante declarado vencedor.
13.2.1 - O prazo para manifestação da intenção de recorrer da decisão do pregoeiro iniciará logo após a habilitação das licitantes e será informado via chat, ficando sob responsabilidade das licitantes o acompanhamento das operações no Sistema Eletrônico.
13.3 - O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.
13.4 - O recurso contra a decisão do Pregoeiro terá efeito suspensivo.
13.5 - Os procedimentos para interposição de recurso, compreendida a manifestação prévia do licitante, durante a sessão pública, o encaminhamento de memorial de eventuais razões e contrarrazões pelos demais licitantes, serão realizados **EXCLUSIVAMENTE** no âmbito no sistema eletrônico em formulários próprios.
13.6 - Os autos do processo administrativo permanecerão com vista franqueada aos interessados na Rua Caramuru, nº 271, Centro, em Pato Branco - PR, nos dias úteis, no horário de expediente das 8 às 12 horas e das 13h30min às 17h30min.
13.7 - Decididos os recursos, o Prefeito Municipal fará a homologação da adjudicatária.

14. ASSINATURA DO CONTRATO
14.1 - Adjudicado o objeto da presente licitação, o Município convocará o adjudicatário, que deverá comparecer **em até 05 (cinco) dias** após a convocação, para assinar o contrato**.** Nos casos em que o contrato for encaminhado via correio, a contratada terá o mesmo prazo para devolução, até 05 (cinco) dias contados do recebimento**, sob pena de decair ao direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº 8.666/93**, que terá efeito de compromisso de fornecimento nas condições estabelecidas.
14.2 - O Município poderá, quando o convocado não assinar o contrato no prazo e condições estabelecidos neste Edital, convocar os proponentes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto ao preço, ou revogar a licitação, independentemente da cominação prevista no artigo 81 da Lei nº 8.666/93.

15. CONDIÇÕES DE PRAZOS, LOCAL, ENTREGA E VIGÊNCIA CONTRATUAL
15.1. Os serviços deverão ser executados mediante solicitação formal da contratante, por meio de Nota de Empenho, na sede da Prefeitura Municipal, localizada na Rua Caramuru, 271, Centro, Pato Branco - PR.
15.2. O recebimento do objeto se dará conforme o disposto no artigo 73, inciso I alíneas “a” e “b” e art. 76 da Lei n.º 8.666/93, e compreenderá duas etapas distintas, a seguir discriminadas:

a) Recebimento Provisório: Deverá começar no início da prestação de serviços (instalação) e consistirá na mera verificação da conformidade com as especificações técnicas. Deverá ser finalizado em **até 24 (vinte e quatro) horas** após a conclusão do serviço.
b) Recebimento Definitivo: Ocorrerá em até **48 (quarenta e oito) horas**, após o Recebimento Provisório, pela Comissão de Avaliação Técnica e constará de:
I - Verificação da conformidade com as especificações técnicas exigidas em cada etapa e se estas atendem plenamente aos requisitos de forma aderente aos termos contratuais.
II - O recebimento definitivo dar-se-á mediante termo circunstanciado de Recebimento Definitivo e posterior certificação na Nota Fiscal, autorizando assim o pagamento.
III - Constatada(s) irregularidade(s) nos serviços contratados, a Administração Municipal poderá rejeitá-los no todo ou em parte, determinando o seu ajuste, às suas expensas, em um prazo que **deverá se iniciar no máximo em até 02 (dois) dias**, contados da assinatura do recebimento da notificação formal, pela Contratada, observando o disposto no art. 69, da Lei 8.666/93 e deverá ser concluído **em até 05(cinco) dias.**
15.3. Os serviços serão considerados aceitos somente após emissão do termo circunstanciado de Recebimento Definitivo devidamente documentado e assinado pelo gestor e/ou fiscal do Contrato de Prestação de Serviços.
15.4. Na hipótese de verificação a que se refere o recebimento definitivo, não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.
15.5. A fiscalização por parte do município e o recebimento provisório ou definitivo não excluem a responsabilidade civil da Contratada pela correção e/ou substituição do objeto contratual, bem como pelos danos e prejuízos ao município ou a terceiros, decorrentes da má execução/desconformidades com as normas técnicas exigíveis, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

15.6. Prazo de Execução: O prazo de execução será de até 15 (quinze) dias, contados a partir do Recebimento da Nota de Empenho.

15.7. Prazo de Vigência: O prazo de vigência será de 12 (doze) meses, contados a partir da assinatura do Contrato de Prestação de Serviços, podendo ser prorrogado conforme legislação vigente e de acordo entre as partes, conforme contempla o Artigo 57, da Lei nº 8.666/93, mediante Termo de Aditamento.

15.8. PRESTAÇÃO DE SERVIÇO DE INSTALAÇÃO
15.8.1 - Para as soluções ofertadas, a Contratada deverá cotar um valor total para a instalação, configuração e treinamento para os dispositivos adquiridos.
15.8.2 - Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, funcionalidades e políticas.
15.8.3 - A instalação deverá ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante.
15.8.4 - Deverá ser realizada a configuração das regras de entrada, saída.
15.8.5 - Configuração do Active Directory.

15.8.6. TREINAMENTO PARA O SISTEMA FIREWALL UTM:
15.8.6.1 - Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware e software) para a equipe do setor de tecnologia da informação (T.I) da Contratante.
15.8.6.2 - Este treinamento deverá possuir carga horária mínima de 08 horas.
15.8.6.3 - O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação.
15.8.6.4 - O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas.
15.8.6.5 - O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta.

15.8.6.6 - Deverá ser incluso, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada.
15.8.6.7 - Os cursos deverão ser realizados em horários e data a serem acordados pela Contratada e pela Contratante.

15.9. PRESTAÇÃO DE SERVIÇOS DE SUPORTE TÉCNICO E REMOTO:
15.9.1 - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis 24 x 07 x 365 (vinte e quatro horas por dia sete dias por semana e trezentos e sessenta e cinco dias no ano), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR), com as seguintes características:
15.9.1.1 - A Contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede, relativos aos equipamentos e/ou produtos fornecidos.
15.9.1.2 Os chamados para o suporte técnico serão classificados por severidade, conforme impacto no ambiente computacional do município:
15.9.1.2.1 - Severidade 01: Sistema crítico, em produção, está parado ou fora de funcionamento, não há meios de contornar a não conformidade. Número significativo de usuários afetados, impacto operacional significativo causado.
15.9.1.2.2 - Severidade 02: Sistema crítico, em produção, está apresentando falhas de funcionamento, não causou interrupção do serviço, no entanto, afeta significativamente o desempenho, com impacto crítico aos usuários.
15.9.1.2.3 - Severidade 03: Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impacto moderado aos usuários. Impacto operacional moderado.
15.9.1.2.4 - Severidade 04: Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features ou melhorias. Impacto mínimo aos usuários. Sem impacto operacional.
15.9.1.3 - Para mensurar o nível de criticidade da não conformidade, serão utilizados os indicadores de severidade. Os chamados, conforme o nível de severidade, definidos pelos técnicos da contratante, terão prazo para resolução, contados a partir do momento do registro da solicitação em service desk de comunicação com a contratada. Segue o aprazamento para resolução de não conformidade:

Descrição do Nível de Criticidade	Tempo Máximo para Resolução
Severidade 1	01 hora corrida
Severidade 2	04 horas corridas
Severidade 3	16 horas úteis
Severidade 4	24 horas úteis

15.9.1.4 - Sendo entendido que:
15.9.1.4.1 – Hora corrida é a compreendida entre o período de 0h00min as 24h00min, 07 (dias por semana). Hora útil é a compreendida entre o período de 08h00min às 18h00min, de segunda a sexta-feira, excetuando-se feriados nacionais.
15.9.1.4.2 - Será admitida solução de contorno (redução ou eliminação do impacto de um incidente ou problema para o qual uma solução completa ainda não está disponível), na resolução de chamados de severidade 01 e 02, para fins de atendimento dos prazos estipulados.
15.9.1.4.3 - Considera-se não conformidade plenamente solucionada quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva.
15.9.1.4.4 - A Contratada não será responsabilizada por descumprimento de prazo para resolução de não conformidade, quando a demanda for originada por falha, interrupção, inconsistência de dados e informações gerados pela Contratante ou terceiros da Contratante. Nestas ocorrências, a Contratada deverá emitir parecer comprovando que a não conformidade não se originou no cumprimento do objeto contratado.
15.9.1.4.5 - Toda intervenção no ambiente produtivo da Contratante, que resulte na necessidade de suporte técnico pela Contratada, deverá ser executada somente após autorização do Setor de Tecnologia

de Informação (TI), a partir de informações claras sobre o impacto da ação nos procedimentos que serão adotados.

15.9.1.4.6 - Na finalização do chamado, o técnico responsável pela Contratada realizará, em conjunto com representantes técnicos da Contratante, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema. O tempo utilizado nos testes não será computado no aprazamento de resolução da não conformidade.

15.9.1.4.7 - Ao término dos testes e do atendimento (fechamento do chamado), a Contratada deverá formalizar a Contratante, de forma detalhada, as causas da não conformidade e solução definitiva adotada.

15.9.1.4.8 - Nos casos em que o atendimento não se mostrar satisfatório, a Contratante fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

16. CONDIÇÕES DE PAGAMENTO

16.1. Para a Instalação (Lote 03, item 01): O pagamento será realizado até o 15º (décimo quinto) dia útil, após a instalação do objeto e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços.

16.2. Para Manutenção (demais itens): O pagamento será realizado mensalmente até o 15º (décimo quinto) dia útil, do mês subsequente a execução dos serviços e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços.

Lote	Item	Valor Mensal	Valor Total 12 meses	Valor da Parcela Única
1	1	R$ 39.269,94	R$ 471.239,28	
1	2	R$ 3.466,67	R$ 41.600,04	
2	1	R$ 3.183,33	R$ 38.199,96	
3	1	--	--	R$ 5.600,00
3	2	R$ 1.252,80	R$ 15.033,60	
3	3	R$ 907,65	R$ 10.891,80	
4	1	R$ 907,40	R$ 10.888,80	

Tabela 01 – Parcelas de cada item

16.3. O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.

16.4. A nota fiscal/fatura deverá conter discriminação resumida do item contratado, número da licitação, número do Contrato de Prestação de serviços, não apresentar rasura e/ou entrelinhas, deverão ser impressas de maneira clara, inteligível, inviolável, ordenada e dentro de padrão uniforme.

16.5. Para fazer jus ao pagamento, a empresa deverá apresentar, prova de regularidade para com a Fazenda Federal, Estadual e Municipal, prova de regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS) e Certidão Negativa de Débitos Trabalhistas (CNDT) emitida eletronicamente através do site http://www.tst.jus.br, em cumprimento com as obrigações assumidas na fase de habilitação do processo licitatório.

16.6. O cadastro no SICAF vigente, ou Certificado de Registro Cadastral (CRC) emitido pela Divisão de Licitações do Município de Pato Branco (desde que válidos), poderão substituir os documentos indicados no subitem 16.4.

16.7. O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.

16.8. Os pagamentos correrão por conta dos recursos das Dotações Orçamentárias (Despesas e Desdobramentos respectivamente) conforme planilha em anexo.

16.9. Em caso de atraso de pagamento motivado exclusivamente pela contratante, como critério para correção monetária aplicar-se-á o IPCA - Índice Nacional de Preços ao Consumidor Amplo calculado pelo IBGE. Em caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma

para tanto, serão devidos pela contratante juros moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples. Quando da incidência da correção monetária e juros moratórios, os valores serão computados a partir do vencimento do prazo de pagamento de cada parcela devida.

17. DO REAJUSTE DE PREÇOS

17.1 - Os valores constantes da planilha orçamentária poderão ser reajustados pelo IGPM, apurados e fornecidos pela Fundação Getúlio Vargas, depois de decorrido 01 (um) ano da apresentação da proposta de preços.

17.2 - Não será concedido reajuste de preços resultante de atrasos ocorridos unicamente em decorrência da incapacidade da contratada em cumprir o prazo ajustado.

17.3 - Havendo atraso ou antecipação na execução dos serviços, relativamente à previsão do respectivo cronograma, que decorra da responsabilidade ou iniciativa do contratado, o reajustamento obedecerá às condições seguintes:

a) Quando houver atrasos, sem prejuízo da aplicação das sanções contratuais devidas pela mora, se os preços aumentarem, prevalecerá os índices vigentes na data em que deveria ter sido cumprida a obrigação.

b) Se os preços diminuírem prevalecerá os índices vigentes na data do efetivo cumprimento da obrigação.

c) A posterior recuperação do atraso não ensejará a atualização dos índices no período em que ocorrer a mora.

17.3 - O reajuste dar-se-á mediante solicitação formal da Contratada, e firmada através de Termo de Aditamento de acordo entre as partes.

17.4 - Caso haja alteração imprevisível no custo da prestação do serviço, caberá ao contratado requerer e demonstrar documentalmente, a necessidade de reequilíbrio econômico-financeiro do contrato com fundamento no artigo 65, II, “d” da Lei Federal n.º 8.666/93.

17.5 - Os valores recompostos somente serão repassados após a assinatura, devolução do Termo assinado (conforme o caso) e publicação do Termo de Aditamento.

17.6 - Não se admitirá nenhum encargo financeiro, como juros, despesas bancárias e ônus semelhantes.

18. EXTINÇÃO E RESCISÃO CONTRATUAL

18.1 - Será automaticamente extinto o contrato quando do término do prazo estipulado, e não ocorrendo o acordo de prorrogação.

18.2 - O contrato poderá ser rescindido amigavelmente pelas partes ou unilateralmente pela administração na ocorrência dos casos previstos nos Art. 77, 78 e 79 da Lei nº 8.666/93, cujo direito da administração o contratado expressamente reconhece.

19. ANTICORRUPÇÃO:

19.1 - As licitantes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa (Lei Federal n.º 8.429/1992), a Lei Federal n.º 12.846/2013 e seus regulamentos, se comprometem que para a execução do contrato nenhuma das partes poderá oferecer, dar ou se comprometer a dar, a quem quer que seja, aceitar ou se comprometer a aceitar, de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios indevidos de qualquer espécie, de modo fraudulento que constituam prática ilegal ou de corrupção, bem como de manipular ou fraudar o equilíbrio econômico financeiro do presente contrato, seja de forma direta ou indireta quanto ao objeto deste contrato, devendo garantir, ainda que seus prepostos, administradores e colaboradores ajam da mesma forma.

20. SANÇÕES POR INADIMPLEMENTO

20.1 - Nos termos do Art. 7º da Lei 10.520/02, quem, convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e

contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no Sicaf, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4o desta Lei, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

20.2 - Das Sanções Administrativas, conforme previsto no Art. 5º do Decreto Municipal nº 8.441/19:

20.2.1 - As sanções administrativas serão aplicadas em conformidade com o prescrito na Lei Federal nº 8666/93, e em legislação correlata, podendo ser das seguintes espécies:

a) Advertência.

b) Multa, na forma prevista no instrumento convocatório ou na Ata de Preços.

c) Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração.

d) Declaração de inidoneidade.

e) Descredenciamento do sistema de registro cadastral.

20.2.2 - As sanções previstas nos subitens "a", "c" e "d" do item 20.2.1, poderão ser aplicadas cumulativamente com a do subitem "b".

20.3 - Das Particularidades da Multa, conforme previsto no Art. 7º do Decreto Municipal nº 8.441/19:

20.3.1 - A multa imposta ao contratado ou licitante, se não disposta de forma diferente no contrato, poderá ser:

a) de caráter moratório, na hipótese de atraso injustificado na entrega ou execução do objeto do contrato, quando será aplicada nos seguintes percentuais:

I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplida, quando o atraso não for superior 30 (trinta) dias corridos.

II - 0,66% (sessenta e seis centésimos por cento) por dia de atraso que exceder a alínea anterior, até o limite de 15 (quinze) dias, na entrega de material ou execução de serviços, calculado, desde o trigésimo primeiro dia de atraso, sobre o valor correspondente à parte inadimplida, em caráter excepcional, e a critério do órgão contratante.

b) de caráter compensatório, quando será aplicada nos seguintes percentuais.

I - 15% (quinze por cento) do valor do empenho em caso de inexecução parcial do objeto pela contratada ou nos casos de rescisão do contrato, calculada sobre a parte inadimplida.

II - 20% (vinte por cento) sobre o valor do contrato, pela sua inexecução total ou pela recusa injustificada do licitante adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração.

20.3.2 - O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do primeiro dia útil seguinte ao do vencimento do prazo de entrega ou execução da Ata de Registro de Preços.

20.4 - A instrução obedecerá ao princípio do contraditório, assegurada ao acusado ampla defesa, com a utilização dos meios e recursos admitidos em direito.

20.5 - Na fase de instrução, o indiciado será notificado pelo gestor do contrato e terá o prazo de 05 (cinco) dias úteis, contados a partir do recebimento do correio eletrônico no e-mail registrado em Ata/Contrato, para apresentação da Defesa Prévia, assegurando-se lhe vista do processo, e juntada dos documentos comprobatórios que considerar pertinentes à fundamentação dos fatos alegados na mesma.

20.6 - O extrato da decisão definitiva, bem como toda sanção aplicada, será anotada no histórico cadastral da empresa e nos sistemas cadastrais pertinentes, quando for o caso, além do processo ser apostilado na sua licitação correspondente.

21. DISPOSIÇÕES GERAIS

21.1 - As normas disciplinadoras desta licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que a interpretação não viole a lei e não comprometa o interesse da Administração, a finalidade e a segurança da contratação.

21.2 - O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

21.3 - Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo pregoeiro. O pregoeiro reserva-se o direito de solicitar o original de qualquer documento, sempre que julgar necessário.

21.4 - Será facultado ao Pregoeiro ou à autoridade superior, em qualquer fase do julgamento, promover diligência destinada a esclarecer ou a complementar a instrução do processo, inclusive parecer técnico à Secretaria requerente do certame com relação aos produtos cotados, bem como solicitar aos órgãos competentes, elaboração de parecer técnico destinado a fundamentar a decisão.
21.4.1 - O Pregoeiro poderá, ainda, relevar erros formais, ou simples omissões em quaisquer documentos, para fins de habilitação e classificação da proponente, desde que sejam irrelevantes, não firam o entendimento da proposta e o ato não acarrete violação aos princípios básicos da licitação e não gerem a majoração do preço proposto.
21.5 - As licitantes devem acompanhar rigorosamente todas as fases do certame e as operações no sistema eletrônico, inclusive mensagem via chat, sendo responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem enviada ou emitida pelo Sistema ou de sua desconexão, bem como será responsável pela apresentação dos documentos solicitados nos prazos previstos.
21.6 - Nenhuma indenização será devida às licitantes pela elaboração ou pela apresentação de documentação referente ao presente Edital.
21.7 - A homologação do resultado desta licitação não implicará direito à contratação.
21.8 - Na contagem dos prazos estabelecidos neste Edital, exclui-se o dia do início e inclui-se o do vencimento, observando-se que só se iniciam e vencem prazos em dia de expediente normal na Prefeitura Municipal de Pato Branco, exceto quando explicitamente disposto em contrário.
21.9 - A autoridade competente poderá revogar a presente licitação por razões de interesse público decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de oficio ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado, sem que caiba às Licitantes direito à indenização.
21.10 - A anulação do procedimento licitatório induz a do contrato, ressalvado o disposto no parágrafo único, art. 59 da Lei 8.666/93.
21.11 - O resultado da licitação será divulgado pelo Portal COMPRASNET através do site www.gov.br/compras e estará disponível junto a Divisão de Licitações do Município de Pato Branco.
21.12 - No caso de alteração deste Edital no curso do prazo estabelecido para a realização do Pregão, este prazo será reaberto, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.
21.13 - É obrigação da proponente observar e acompanhar rigorosamente os editais, todas as fases do certame e comunicados oficiais divulgados conforme item anterior, ler e interpretar o conteúdo destes, desobrigando totalmente o órgão licitador, por interpretações errôneas ou inobservâncias.
21.14 - A proponente deverá indicar ao Pregoeiro todos os meios de contato (telefone/endereço eletrônico (e-mail), para comunicação, e obriga-se a manter os dados devidamente atualizados durante todo o decurso processual. Será de sua inteira responsabilidade o retorno imediato de todos os atos comunicados, os quais serão considerados recebidos, não lhe cabendo qualquer alegação de não recebimentos dos documentos.
21.15 - O pregoeiro não se responsabilizará por *e-mails* que, por qualquer motivo, não forem recebidos em virtude de problemas no servidor ou navegador, tanto do Município de Pato Branco quanto do emissor.
21.16 - Incumbirá ao Licitante acompanhar as operações no Sistema Eletrônico, sendo responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem enviada e emitida pelo Sistema ou de sua desconexão.
21.17 - Caso o sistema eletrônico desconectar para o pregoeiro no decorrer da etapa de lances da sessão pública, e permanecendo acessíveis aos licitantes, os lances continuarão sendo recebidos, sem o prejuízo dos atos realizados.
21.18 - Se a desconexão do pregoeiro persistir por tempo superior a 10min (dez minutos), a sessão pública será suspensa e só poderá ser reiniciada após decorrido, no mínimo 24h (vinte e quatro horas), após a comunicação do fato aos participantes em campo próprio no sistema eletrônico.
21.19 - CASO A ETAPA DE LANCES ULTRAPASSE O HORÁRIO DE EXPEDIENTE, O PREGÃO SERÁ SUSPENSO E RETORNARÁ NO HORÁRIO INFORMADO PELO PREGOEIRO VIA CHAT.
21.20 - Não havendo expediente, ocorrendo qualquer fato superveniente, ou mesmo indisponibilidade no Sistema Comprasnet que impeça a realização do certame na data e horário marcado, a sessão pública

será automaticamente transferida para o primeiro dia útil subsequente, no horário estabelecido neste Edital, desde que não haja comunicação do Pregoeiro em contrário.

21.21 - Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

21.22 - Incumbirá ao Licitante acompanhar as operações no Sistema Eletrônico, sendo responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem enviada ou emitida pelo Sistema ou de sua desconexão.

21.23 - Para dirimir, na esfera judicial, as questões oriundas do presente Edital, será competente o Foro da Comarca de Pato Branco - PR.

21.24 - Os casos omissos serão resolvidos pelo Pregoeiro.

21.25 - Fazem parte integrante deste Edital:

21.25.1 - ANEXO I - Termo de Referência.

21.25.2 - ANEXO II - Minuta do Contrato

21.25.3 - ANEXO III - Modelo da Declaração Unificada de Idoneidade, Cumprimento do disposto no Inciso XXXIII do Art. 7º da Constituição Federal, Declaração de comprometimento de manter as condições de habilitação e qualificação durante a vigência do Contrato, Cumprimento art. 9º, inciso III da Lei 8.666/93.

21.25.4 - ANEXO IV - Modelo Proposta de Preços.

Pato Branco, 26 de maio de 2022.

_____

Eduardo José Grezele
Pregoeiro

ANEXO I
TERMO DE REFERÊNCIA

1. APRESENTAÇÃO

1.1 - Em conformidade com as disposições contidas na Lei nº 10.520/2002, Decreto Municipal nº 8.441, de 08 de janeiro de 2019, Decreto Municipal nº 8.574 de 01 de novembro de 2019, Lei Complementar nº 123/2006 e alterações, e subsidiariamente a Lei nº 8.666/1993 suas alterações e demais legislações pertinentes à matéria, elaboramos o presente Termo de Referência, objetivando o fornecimento do objeto abaixo especificado, conforme solicitação feita pela Secretaria Municipal de Administração e Finanças.

2. OBJETO

2.1 - A presente licitação tem por objeto a Contratação de pessoa jurídica para fornecimento de licença de uso, locação de softwares de Firewall – Next Generation, E-mail, Acesso Remoto, Automação e Antivírus, treinamento básico, atualização corretiva, adaptativa e evolutiva, diagnósticos, atendimento e suporte técnico, por tempo determinado, com fornecimento de equipamentos mediante o comodato (*hardware*), em atendimento as necessidades de todas as Secretarias e Departamentos Municipais, conforme segue:

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
AMPLA PARTICIPAÇÃO						
1	1	1	sv	APPLIANCE UTM FIREWALL - Característica do Hardware (Comodato): Deve ser entregue 02 (dois) equipamentos idênticos, para atender a necessidade de equipamento Spare (BACKUP). O equipamento deve ser instalado em rack, com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack. Dispor de fonte de alimentação redundante interna, com tensão de entrada de 110V / 220V AC, automática e frequência de 50-60 Hz, Hot swapping. Possuir painel/led indicador on/off, disco e devices de rede. Suportar no mínimo 30.000.000 (trinta milhões) de conexões simultâneas. Suportar no mínimo 250.000 (duzentos e cinquenta mil) novas conexões por segundo. Possuir throughput mínimo de 12 Gbps, para tráfego IPS/IDS. Possuir throughput mínimo de 13 Gbps, para tráfego VPN IPSEC, com criptografia (AES-128). Possuir throughput mínimo de 07 Gbps, para tráfego VPN SSL, com criptografia (AES-128). Possuir throughput mínimo de 12 Gbps/5.5 Gbps, para tráfego Proxy Web filter/SSL Inspection. Possuir throughput mínimo de 6.8 Gbps, para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo). Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000, com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch.	471.239,28	471.239,28

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				Possuir dispositivo de armazenamento interno de no mínimo 240GB padrão SSD. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento. Especificações Gerais de Software Firewall Next Generation – NGFW: Funções Básicas: Hardware (Appliances) que atuam na segurança e performance do ambiente de rede. VPN SSL, VPN IPSec (Client-to-site e Site-to-site). Controle de Aplicações. Proxy Web e Filtro de Conteúdo Web (URL Filtering). Detecção e prevenção de intrusos – IPS. Qualidade de serviço – QOS. Anti-Malware. SD-WAN (Software-Defined Wide Artea Network). Cluster. Das Características Gerais: O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 07. Interface em português ou inglês. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento. O sistema deve permitir o acesso à interface de gerenciamento WEB, por qualquer interface de rede configurada. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas. A Solução deverá prover inspeção SSL: A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho. Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo. Deve suportar cluster do tipo Failover (HA) com replicação		

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				da tabela de estado. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração: Endereço do servidor. Porta do servidor. Usuário. Senha. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens: Desempenho total (throughput). Conexões simultâneas. Usuários autenticados. Serviços habilitados ou desabilitados. Quantidade de endereços distribuídos pelo DHCP. Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com o sistema central e receba a configuração. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar o sistema central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento. A solução ofertada deverá permitir a criação de perfis de proteção, tais como e não limitado a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e dever ser possível utilizá-los nas políticas de segurança. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX). A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy. Deve		

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				implementar o protocolo ECMP. O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS.Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo. Contemplando treinamento e suporte técnico e remoto.		
1	2	1	sv	Serviço de manutenção preventiva, corretiva e evolutiva, suporte técnico e remoto para o software APPLIANCE UTM FIREWALL (BACKUP).	41.600,04	41.600,04
TOTAL LOTE 01						**R$ 512.839,32**
EXCLUSIVO MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE						
2	1	1	sv	Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud sendo: 600 contas de e-mail de 5 GB, totalizando 3TB, contendo antispam e antivírus e 100 contas de e-mail de 30 GB, totalizando 3TB, contendo antispam, antivírus e backup ilimitado. Contemplando suporte técnico e remoto.	38.199,96	38.199,96
TOTAL LOTE 02						**R$ 38.199,96**
3	1	1	sv	Implantação dos sistemas (acesso remoto e automação), com entrega técnica e treinamento de uso da ferramenta em todos os módulos, orientado a equipe como instalar o agente e antivírus, realizar acessos remotos, configurar e agendar tarefas e realizar controle total do inventário. Deverá ser apresentado escopo detalhado deste serviço para equipe técnica.	5.600,00	5.600,00
3	2	1	sv	Módulo de acesso remoto e controle para 750 máquinas: Do acesso ao software: A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura de armazenamento, processamento transmissão deve ser disponibilizada em Datacenter Nacional e ou Internacional com certificação Tier II ou superior; Deverá prover acesso diretamente por painel web ou via aplicação instalável; A solução deverá compreender quantidade de usuários ilimitados; Deverá contemplar política de permissionamento por usuário ou grupo de	15.033,60	15.033,60

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				usuário de forma detalhada, por rotina e/ou módulo; A solução deverá possibilitar o login do usuário através de autenticação em dois fatores de forma opcional;Deverá possibilitar criação de senha forte, exemplo, letras maiúsculas, minúsculas, número e caracteres especiais e exigir alteração a cada 90 dias; Deverá ser possível configurar qual ou quais computadores ou grupo de computadores o usuário poderá ter acesso remoto; Do acesso remoto: A solução deverá permitir acesso remoto em primeiro e segundo plano, entende-se como acesso em segundo plano o acesso ao computador sem assumir o controle da área de trabalho do usuário; O acesso em segundo plano deverá permitir acessar ao prompt de comando, CMD, e executar comandos remotamente, deverá mostrar de forma intuitiva ao usuário informações sobre aplicações, serviços, programas e drives instalados, bem como, possibilitar interessa como, pausar, reiniciar ou iniciar um serviço do Windows ou até mesmo reiniciar a máquina, tudo em segundo plano sem conectar na máquina do usuário; A solução de acesso e controle remoto deverá permitir multiplicas conexões simultâneas e herdar a quantidade de monitores que o usuário estiver utilizando; A solução de acesso remoto ao computador, em primeiro plano ao acessar a área do usuário, deverá funcionar como login único ou federado e carregar as credenciais de administrador único sem a necessidade de que o usuário precise alterar o usuário do computador para ter privilégios de administrador; A solução de acesso remoto ao computador, em primeiro plano ao acessar a área do usuário deverá possibilitar o compartilhamento de unidade de disco no acesso remoto, facilitando assim a transição dos arquivos; A solução de acesso remoto ao computador, em primeiro plano ao acessar a área do usuário deverá possibilitar desligar o monitor do usuário, bloquear o seu mouse e teclado, compartilhar som e impressora na conexão remota e possuir ferramentas de instrução como lazer point e quadro interativo com o usuário; A ferramenta deverá permitir gravar opcionalmente todo e qualquer acesso remoto e manter a gravação em extensões		

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				de vídeos como .avi, mp3, mp4 por um período configurável; A solução de acesso remoto deverá permitir que o técnico ou o usuário, se com permissão, consiga compartilhar a sua tela/área de trabalho via convite por link ou e-mail para suporte de terceiros e/ou fornecedores de softwares utilizados pelo Município. A ferramenta de gestão de máquinas deverá possuir solução de implantação aos computadores em lote de forma customizável, ou seja, gerando um .msi ou .exe personalizável já com as configurações de grupos e permissionamento pré-definidas, a fim de facilitar o processo de instalação em grandes volumes de máquinas. A ferramenta deverá conter dentro da mesma plataforma módulo de relatórios personalizáveis imprescindivelmente no que diz respeito aos status das ações executadas remotamente, tal como, o log de registros dos acessos remotos por computador e/ou usuários.		
3	3	1	sv	Módulo de automação para 750 máquinas, sendo: Aplicação de atualizações: A ferramenta devera desmobilizar dentro da mesma ferramenta um painel para gestão das atualizações de aplicativos como java, adoble, office e outros, como também gerenciar paches de atualizações do Windows de forma individual, agrupada ou bloquear atualizações específicas; Das automações: A ferramenta deverá conter funcionalidades para execução de ações remotamente e agendáveis por dia, hora, semana, mês, execução imediata, ou ainda, execução quando um critério for identificado, exemplo, quando um determinado serviço, software, programa travar ou parar a ferramenta deverá permitir executar automaticamente as ações: A ações remotas em lote a serem aplicadas em uma ou várias máquinas deverá conter filtros por sistema operacional, apenas máquinas online e selecionar SO 32 ou 64 bits; A ferramenta de execução remota deverá possuir recursos para: Executar um comando remoto via cmd ou powershell; Executar um arquivo em lote ou um executável; Distribuir arquivos em todas as máquinas de forma automático de acordo com os filtros citados acima; Instalar ou atualizar um software, .msi e/ou .exe; Atualizar registros, .reg do Windows e ainda,	10.891,80	10.891,80

Lt	Item	Qtde	Und	Descrição	Valor Un	Valor Total
				deverá possibilitar comando para voltar log sobre o sucesso ou insucesso da execução; A solução deverá possibilitar também a execução de comando ou instalação e atualização para computadores Mac.		
TOTAL LOTE 03						**R$ 31.525,40**
4	1	1	sv	Módulo Antivírus para 750 máquinas, sendo: A ferramenta deverá possuir dentro da mesma solução uma central para gestão dos antivírus onde seja possível executar remotamente para um ou vários computadores as seguintes funções: Recuperar informações mais recentes do antivírus; Executar varredura completa; Atualizar definições de vírus; Ativar ou desativar proteção em tempo real; Bloquear portas usb dos computadores ou ainda exigir varredura imediata quando o usuário conectar em algum porta usb dos computadores do munícipio. A Contratada deverá entregar juntamente o licenciamento de antivírus para 750 computadores compatíveis com os mais conhecidos do mercado, como Kaspersky, bitdefender, avira ou similares.	10.888,80	10.888,80
TOTAL LOTE 04						**R$ 10.888,80**

3. DESCRIÇÃO DOS EQUIPAMENTOS E DOS SERVIÇOS:

3.1. LOTE 01: A locação da solução integrada de **Firewall *Next Generation*** é composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de:

3.1.1 - Filtro de pacotes com controle de estado.

3.1.2 - Filtro de conteúdo web.

3.1.3 - Interceptação SSL.

3.1.4 - Filtro de aplicações.

3.1.5 - Controle da web 2.0.

3.1.6 - Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos.

3.1.7 - Integrar soluções do tipo (IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, SD-WAN, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

3.1.8 - Aquisição de solução para gerenciamento centralizado de Firewall.

3.1.9 - Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 48 meses, onde deverá ser instalado localmente e permitir a atualização do software e do sistema operacional, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

3.1.10 - Treinamento para a equipe do Departamento de Tecnologia de Informação da Prefeitura Municipal de Pato Branco.

3.1.11 - Suporte técnico remoto (24x7).

3.2. LOTE 02: Serviços de E-mail (1):

3.2.1 - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.

3.2.2 - Possuir 600 contas de e-mail de 5 GB, totalizando 3TB, contendo antispam e antivírus.
3.2.2.1 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

3.2.3. Serviços de E-mail (2):
3.2.3.1 - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.
3.2.3.2 - Possuir 100 contas de e-mail de 30 GB, totalizando 3TB, contendo antispam, antivírus e backup ilimitado.
3.2.3.3 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

3.3. LOTE 03: Instalação e Prestação de Serviços do Módulo de Acesso Remoto e de Controle:
3.3.1 - Módulo de Acesso Remoto e de Controle para 750 máquinas
3.3.2 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior
3.3.3 - A solução deverá prover acesso diretamente por painel *web* ou via aplicação instalável
3.3.4 - A ferramenta deverá permitir e gravar opcionalmente todo e qualquer acesso remoto e manter a gravação em extensões de vídeo como: .avi,mp4 por um período configurável.
3.3.5 - A solução deverá permitir acesso remoto em primeiro e segundo plano, entende-se como acesso em segundo plano o acesso ao computador sem assumir o controle da área de trabalho do usuário.
3.3.6 - O acesso em segundo plano deverá permitir acessar ao prompt de comando e executar comandos remotamente, deverá mostrar de forma intuitiva ao usuário informações sobre aplicações, serviços, programas e *drivers* instalados, bem como possibilitar pausar, iniciar ou reiniciar um serviço do *Windows.*
3.3.7 - A solução de acesso remoto ao computador em primeiro plano deverá ao acessar a área do usuário, possibilitar o acesso a esta área, assim como permitir controlar, bloquear monitor e teclado, mouse.

3.3.8. AQUISIÇÃO E PRESTAÇÃO DE SERVIÇOS DO MÓDULO DE AUTOMAÇÃO
3.3.8.1 - Módulo de automação para 750 máquinas
3.3.8.2 - A ferramenta deverá ser integrada junto com a solução de acesso remoto.
3.3.8.3 - A ferramenta deverá conter funcionalidades para execuções de ações remotamente e agendáveis por dia, hora, semana, mês, execução imediata ou executar conforme certos critérios de configurações.
3.3.8.4 - Executar comando remoto via Prompt de Comando ou Powershell.
3.3.8.5 - Executar um arquivo em lote ou executável.
3.3.8.6 - Distribuir arquivos em todas as máquinas de forma automática.
3.3.8.7 - Atualizar registros do *Windows.*
3.3.8.8 - Instalar ou atualizar um software por .msi ou.exe.

3.4. LOTE 04: Prestação de Serviços do Módulo Antivírus:
3.4.1 - Modulo de Antivírus para 750 maquinas.
3.4.2 - A Ferramenta deverá possuir dentro da mesma solução uma central para gestão dos antivírus onde seja possível executar remotamente para um ou vários computadores.
3.4.3 - Executar varredura completa e atualizar definições de vírus.
3.4.4 - Recuperar informações mais recentes do antivírus.
3.4.5 - Ativar ou desativar proteção em tempo real.
3.4.6 - Bloquear portas *usb* dos computadores ou ainda exigir varredura imediata quando o usuário conectar em alguma porta *usb* dos computadores.

3.4.7 - A Contratada deverá entregar juntamente, o licenciamento de antivírus para 750 computadores compatíveis com os mais conhecidos no mercado, como por exemplo: Kaspersky, Bitdefender, avirá ou similares.

3.4.8. DA IMPLANTAÇÃO DOS SISTEMAS:

3.4.8.1 - Deverá contemplar a entrega técnica e o treinamento de uso da ferramenta em todos os módulos.

3.4.8.2 - A Contratada deverá orientar a equipe técnica da Contratante, de como proceder à instalação do agente e do antivírus.

3.4.8.3 - A Contratada deverá orientar a equipe técnica da Contratante, de como realizar o acesso remoto e o agendamento de tarefas.

3.4.8.4 - A Contratada deverá apresentar o escopo detalhado dos serviços contratados para equipe técnica da Contratante.

3.5. DAS ESPECIFICAÇÕES, CARACTERÍSTICAS E FUNCIONALIDADES TÉCNICAS PARA A SOLUÇÃO DE SEGURANÇA "FIREWALL UTM":

3.5.1. APPLIANCE UTM FIREWALL - Característica do Hardware:

3.5.1.1 Deverá ser entregue 02 (dois) equipamentos idênticos, para atender a necessidade de equipamento Spare (BACKUP).

3.5.1.2 O equipamento deverá ser instalado em rack, com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack.

3.5.1.3 Dispor de fonte de alimentação redundante interna, com tensão de entrada de 110V / 220V AC, automática e frequência de 50-60 Hz, Hot swapping.

3.5.1.4 Possuir painel/led indicador on/off, disco e devices de rede.

3.5.1.5 Suportar no mínimo 30.000.000 (trinta milhões) de conexões simultâneas.

3.5.1.6 Suportar no mínimo 250.000 (duzentos e cinquenta mil) novas conexões por segundo.

3.5.1.7 Possuir throughput[1] mínimo de 12 Gbps, para tráfego IPS/IDS.

3.5.1.8 Possuir throughput mínimo de 13 Gbps, para tráfego VPN IPSEC, com criptografia (AES-128).

3.5.1.9 Possuir throughput mínimo de 07 Gbps, para tráfego VPN SSL, com criptografia (AES-128).

3.5.1.10 Possuir throughput mínimo de 12 Gbps/5.5 Gbps, para tráfego Proxy Web filter/SSL Inspection.

3.5.1.11 Possuir throughput mínimo de 6.8 Gbps, para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo).

3.5.1.12 Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000, com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch.

3.5.1.13 Possuir dispositivo de armazenamento interno de no mínimo 240GB padrão SSD.

3.5.1.14 Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento.

3.6. ESPECIFICAÇÕES GERAIS DE SOFTWARE FIREWALL NEXT GENERATION – NGFW:

3.6.1. Funções Básicas:

3.6.1.1 Hardware (Appliances) que atuam na segurança e performance do ambiente de rede.

3.6.1.2 VPN SSL, VPN IPSec (Client-to-site e Site-to-site).

3.6.1.3 Controle de Aplicações.

3.6.1.4 Proxy Web e Filtro de Conteúdo Web (URL Filtering).

3.6.1.5 Detecção e prevenção de intrusos – IPS.

3.6.1.6 Qualidade de serviço – QOS.

3.6.1.7 Anti-Malware.

3.6.1.8 SD-WAN (*Software-Defined Wide Artea Network*).

3.6.1.9 Cluster.

[1] Throughput: Taxa em que os dados são transmitidos. Ele também pode ser definido como a quantidade de dados movidos com êxito de um lugar para outro em um determinado período. A taxa de transferência é medida em bits por segundo (bps).

3.7. DAS CARACTERÍSTICAS GERAIS:

3.7.1 O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade.

3.7.2 A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 07.

3.7.3 Interface em português ou inglês.

3.7.4 Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento.

3.7.5 O sistema deverá permitir o acesso à interface de gerenciamento WEB, por qualquer interface de rede configurada.

3.7.6 O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

3.7.7 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

3.7.8 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

3.7.9 Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas.

3.7.10 A Solução deverá prover inspeção SSL:

3.7.10.1 A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho.

3.7.10.2 Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo.

3.7.10.3 Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

3.7.10.4 Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

3.7.10.4.1 Endereço do servidor.

3.7.10.4.2 Porta do servidor.

3.7.10.4.3 Usuário.

3.7.10.4.4 Senha.

3.7.11 Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

3.7.11.1 Desempenho total (throughput).

3.7.11.2 Conexões simultâneas.

3.7.11.3 Usuários autenticados.

3.7.11.4 Serviços habilitados ou desabilitados.

3.7.11.5 Quantidade de endereços distribuídos pelo DHCP.

3.7.12 Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos.

3.7.13 A Solução deverá permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com o sistema central e receba a configuração.

3.7.14 Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar o sistema central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento.

3.7.15 A solução ofertada deverá permitir a criação de perfis de proteção como: a não limitação a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e deverá ser possível utilizá-los nas políticas de segurança.

3.7.16 Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV.

3.7.17 Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX).
3.7.18 A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança.
3.7.19 Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy.
3.7.20 Deverá implementar o protocolo ECMP.
3.7.21 O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.
3.7.22 Deverá possuir suporte ao protocolo de encapsulamento de redes MPLS.
3.7.23 Esta condição deverá permitir conectar links MPLS, diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

3.8. Das Funcionalidades do Firewall:
3.8.1 Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas.
3.8.2 Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH.
3.8.3 Possibilitar a visualização dos países de origem e destino nos *logs* de eventos, de acessos e de ameaças.
3.8.4 Possuir mecanismo que permita a realização de cópias de segurança (*backups*) do sistema e restauração remota, através da interface gráfica, a solução deverá permitir o agendamento diário ou semanal.
3.8.5 O sistema deverá permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
3.8.6 As cópias de segurança deverão ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup.
3.8.7 O sistema ainda deverá contemplar um recurso de cópia de segurança do tipo *snapshot* (cópia instantânea), que contemple a cópia completa das configurações dos serviços e dos recursos do sistema.
3.8.8 Deverá possibilitar a restauração do *snapshot* através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema.
3.8.9 Deverá permitir habilitar ou desabilitar o registro de *log* por política de *firewall.*
3.8.10 Possuir controle de acesso à internet por endereço IP de origem e de destino.
3.8.11 Possuir controle de acesso à internet por sub-rede.
3.8.12 Possuir suporte a tags de VLAN (802.1q).
3.8.13 Suportar agregação de links, segundo padrão IEEE 802.3ad.
3.8.14 Possuir ferramenta de diagnóstico do tipo *tcpdump*.
3.8.15 Possuir integração com Servidores de Autenticação RADIUS (Remote Authentication Dial In User Service), TACACS+, LDAP e Microsoft Active Directory.
3.8.16 Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e SSH).
3.8.17 Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
3.8.18 Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana.
3.8.19 Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br.
3.8.20 Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
3.8.21 Possuir funcionalidades de DHCP Cliente, Servidor e Relay.
3.8.22 Deverá suportar aplicações multimídia como: H.323, SIP.
3.8.23 Possuir tecnologia de firewall do tipo Stateful.
3.8.24 Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo.
3.8.25 Permitir o funcionamento em modo transparente tipo “bridge”.

3.8.26 Permitir a criação de pelo menos 20 VLANS (rede local virtual) no padrão IEEE 802.1q.
3.8.27 Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando).
3.8.28 Deverá suportar *forwarding* (encaminhamento) de multicast..2.3.29 Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP.
3.8.29 Permitir o agrupamento de serviços.
3.8.30 Permitir o filtro de pacotes sem a utilização de NAT.
3.8.31 Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
3.8.32 Possuir mecanismo de anti-spoofing.
3.8.33 Permitir criação de regras definidas pelo usuário.
3.8.34 Permitir o serviço de autenticação para HTTP e FTP.
3.8.35 Possuir a funcionalidade de balanceamento e contingência de links.

3.9 DA IDENTIFICAÇÃO DO USUÁRIO:
3.9.1 Deverá possuir a capacidade de criação de políticas de acesso de *firewall,* VPN, IPS e ao controle de aplicação integrada ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius.
3.9.2 Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
3.9.3 A solução deverá ser capaz de identificar nome do usuário, *login*, máquina/computador registrados no Microsoft Active Directory.
3.9.4 Na integração com o AD (Active Directory), todos os domain controllers em operação na rede do cliente deverão ser cadastrados de maneira simples e sem utilização de *scritps* de comando.
3.9.5 A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante.
3.9.6 A solução deverá suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o gateway (porta de entrada) tenha que fazer “queries” (consulta) no AD.
3.9.7 O UTM deverá permitir gerenciar múltiplas políticas de controles no serviço de autenticação. As políticas deverão permitir criar controles para autenticação e deverão permitir ou bloquear o acesso ao serviço de autenticação, baseado em condições e de sessão, ou seja, uma vez que o usuário esteja permitido se autenticar no serviço, a política deverá definir os parâmetros de sessão do usuário.
3.9.8 Para o sistema de controle no serviço de autenticação o produto deverá possuir no mínimo, as seguintes condições para o Controle de Autenticação:
3.9.8.1 Usuários e Grupos de Usuários.
3.9.8.2 Datas (Objetos de Datas).
3.9.8.3 Horários (Objetos de Horário).
3.9.8.4 Plataformas (Objetos de Dicionários).
3.9.8.5 Endereços Remotos (Objetos de IPv4 e IPv6).
3.9.8.6 Zona de Rede (Múltiplas Zonas).

3.10 DAS FUNCIONALIDADES DA REDE PRIVADA VIRTUAL VPN (VIRTUAL PRIVATE NETWORK):
3.10.1 Rede Privada Virtual - VPN baseada em appliance.
3.10.2 Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES.
3.10.3 Possuir suporte a VPNs IPSec site-to-site.
3.10.4 Criptografia, 3DES, AES128, AES256, AES-GCM-128, Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC.
3.10.5 Algoritmo Internet Key Exchange (IKE) versões I e II.
3.10.6 AES 128 e 256 (Advanced Encryption Standard).
3.10.7 Suporte a Diffie-Hellman (troca de chaves de maneira segura) Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30.

3.10.8 Possuir suporte a VPN SSL.
3.10.9 Possuir capacidade de realizar SSL VPNs utilizando certificados digitais.
3.10.10 Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:
3.10.10.1 Remote Desktop Protocol.
3.10.10.2 Virtual Network Computing.
3.10.10.3 SSH - Secure Shell.
3.10.10.4 WEB - World Wide Web.
3.10.10.5 SMB - Server Message Block.
3.10.10.6 Deverá permitir a arquitetura de vpn hub and spoke.
3.10.10.7 Suporte a VPNs IPSec client-to-site.
3.10.10.8 Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
3.10.10.9 Suporte à inclusão em autoridades certificadoras (enrollment = inscrição) mediante SCEP (Simple Certificate Enrollment Protocol).
3.10.10.10 Possuir funcionalidades de Auto-Dicovery VPN, capaz de permitir criar túneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).
3.10.10.11 A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de túneis:
3.10.10.11.1 Site-to-Site.
3.10.11.2 Full-Mesh.
3.10.10.11.3 Star.

3.11 DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO: A DETECÇÃO DE INTRUSÃO DEVERÁ SER BASEADA EM *APPLIANCE*:
3.11.1 Possuir no mínimo 25.000 (vinte e cinco mil) assinaturas ou regras de IPS/IDS.
3.11.2 O sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes.
3.11.3 Possuir tecnologia de detecção baseada em assinatura.
3.11.4 Deverá suportar a implantação em modo Gateway, *online* e em modo sniffer (farejador).
3.11.5 Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass.
3.11.6 O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança.
3.11.7 Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.
3.11.8 Possuir capacidade de remontagem de pacotes para identificação de ataques.
3.11.9 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de servidores web.
3.11.10 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
3.11.11 Mecanismos de detecção/proteção de ataques.
3.11.12 Reconhecimento de padrões.
3.11.13 Análise de protocolos.
3.11.14 Detecção de anomalias.
3.11.15 Detecção de ataques de RPC (Remote Procedure Call).
3.11.16 Proteção contra ataques de Windows ou NetBios.
3.11.17 Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol).
3.11.18 Proteção contra ataques DNS (Domain Name System).
3.11.19 Proteção contra ataques a FTP, SSH, Telnet e rlogin (logins remotos).
3.11.20 Proteção contra ataques de ICMP (Internet Control Message Protocol).
3.11.21 Alarmes na console de administração.
3.11.22 Alertas via correio eletrônico.

3.11.23 Monitoração do comportamento do appliance através de SNMP - Simple Network Management Protocol, o dispositivo deverá ser capaz de enviar traps (armadilhas) de SNMP, quando ocorrer um evento relevante para a correta operação da rede.
3.11.24 Capacidade de resposta/logs ativa a ataques.
3.11.25 Terminação de sessões via TCP resets.
3.11.26 Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos.
3.11.27 O sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços.
3.11.28 Possuir filtros de ataques por anomalias.
3.11.29 Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit.
3.11.30 Permitir filtros de anomalias de protocolos.
3.11.31 Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.
3.11.32 Suportar verificação de ataque nas camadas de aplicação.

3.12. DAS FUNCIONALIDADES DO QOS - QUALITY OF SERVICE OU QUALIDADE DE SERVIÇO:
3.12.1 Adotar solução de Qualidade de Serviço baseada em appliance.
3.12.2 Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
3.12.3 Permitir modificação de valores DSCP.
3.12.4 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
3.12.5 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
3.12.6 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
3.12.7 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino.
3.12.8 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

3.13 DAS FUNCIONALIDADES DO ATP - ADVANCED THREAT PREVENTION (PREVENÇÃO AVANÇADA CONTRA AMEAÇAS):
3.13.1 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP.
3.13.2 Permitir o bloqueio de malwares (adware (tipo anúncios, propagandas), spyware (tipo espião), hijackers (tipo cavalo de tróia), keyloggers, etc.).
3.13.3 Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo.
3.13.4 Permitir o bloqueio de download de arquivos por tamanho.

3.14. Das Funcionalidades do Proxy e do Filtro de Conteúdo Web:
3.14.1 Possuir solução de filtro de conteúdo web integrado a solução de segurança.
3.14.2 Possuir pelo menos 80 categorias para classificação de sites web.
3.14.3 Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
3.14.3.1 Webmail.
3.14.3.2 Instituições de Saúde.
3.14.3.3 Notícias.
3.14.3.4 Pornografia.
3.14.3.5 Restaurante.
3.14.3.6 Mídias Sociais.
3.14.3.7 Esporte.
3.14.3.8 Educação.

3.14.3.9 Games.
3.14.3.10 Compras.
3.14.4 Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
3.14.5 Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória.
3.14.6 Deverá permitir a definição do tamanho mínimo dos objetos salvos em cache no disco.
3.14.7 Deverá permitir a definição do tamanho máximo dos objetos salvos em cache em memória.
3.14.8 Deverá atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação.
3.14.9 Possibilitar a integração com servidores de cache WEB externos.
3.14.10 Deverá possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares.
3.14.11 Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
3.14.12 Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
3.14.13 Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante.
3.14.14 Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX, através de: base de URL própria atualizável.
3.14.15 Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual.
3.14.16 Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra.
3.14.17 Deverá permitir o bloqueio de URLs inválidas, cujo campo CN, do certificado SSL, não contém um domínio válido.
3.14.18 Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web.
3.14.19 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
3.14.20 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
3.14.21 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem.
3.14.22 Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP.
3.14.23 Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Áudio, Vídeo e URLs originadas de Spam.
3.14.24 Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueada – lista negra.
3.14.25 Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente.
3.14.26 Deverá permitir configurar a porta do Proxy Explícito.

3.15. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES: AS FUNCIONALIDADES ABAIXO DEVEM SER BASEADAS EM *APPLIANCE*:
3.15.1 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
3.15.1.1 P2P.
3.15.1.2 Web.
3.15.1.3 Transferência de arquivos.
3.15.1.4 Chat.
3.15.1.5 Social.
3.15.2 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
3.15.3 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
3.15.4 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

3.15.**5** Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
3.15.**6** Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
3.15.**7** Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
3.15.**8** Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino.
3.15.**9** Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

3.16. DAS FUNCIONALIDADES DO SD-WAN - (SOFTWARE-DEFINED WAN):
3.16.**1** Entende-se como tecnologia SD-WAN (Software-Defined WAN), a rede de área ampla definida por software que centraliza a gerência da rede WAN, em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN, para comunicação entre os sites remotos.
3.16.**2** Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas.
3.16.**3** Permitir utilizar VPN IPsec para interligar unidades remotas.
3.16.**4** Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link.
3.16.**5** O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes e latência.
3.16.**6** Deverá possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN.
3.16.7 O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação.
3.16.**8** O appliance SD-WAN deverá permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado veja avaliado. Deverá suportar especificar um valor variando de 01 a 100.
3.16.**9** O recurso de SD-WAN deverá permitir o monitoramento de no mínimo 03 (três) endereços alvos, para verificar a disponibilidade e desempenho do link.
3.16.**10** A solução de SD-WAN UTM, deverá permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN, de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras.
3.16.**11** Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:
3.16.**11.1** Consumo de banda.
3.16.**11.2** Perda de pacotes.
3.16.**11.3** Jitter.
3.16.**11.4** Latência.

3.17. **DA ALTA DISPONIBILIDADE:**
3.17.**1** Possuir mecanismo de alta disponibilidade operando em modo Ativo/Standby, com as implementações de Failover (tolerância as falhas).
3.17.**2** Não serão permitidas soluções de cluster (HA), que façam com que o equipamento reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
3.17.**3** O sincronismo dos servidores deverá ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

3.18. DAS SOLUÇÕES DE GERENCIAMENTO CENTRALIZADO DE FIREWALL:
3.18.**1** Funcionalidades de Gerenciamento:
3.18.**1.1** Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto.

3.18.1.2 A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewalls contratados.
3.18.**1.3** O gerenciamento centralizado poderá ser entregue como *appliance* físico ou virtual. Caso seja entregue em *appliance* fisíco deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em *appliance* virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o *appliance* virtual é responsabilidade da Contratante.
3.18.**1.4** Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento.
3.18.**1.5** A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica.
3.18.**1.6** Deverá manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de *logs* e emissão de relatórios.
3.18.**1.7** A solução deverá incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador.
3.18.**1.8** A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.
3.18.1.9 Deverá possibilitar a realização de "backup" e restauração de dados.
3.18.**1.10** Deverá possibilitar o envio dos *"logs"* gerados a outro concentrador de *"logs"* externo a solução.
3.18.1.11 Deverá possibilitar a gerência de *"logs",* realizando as configurações de relatórios de todos os "firewalls" integrados.
3.18.**1.12** Deverá permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.
3.18.**1.13** O gerenciamento deverá permitir/possuir:
3.18.**1.13.1** Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas.
3.18.**1.13.2** Monitoração de *logs*.
3.18.**1.13.3** Debugging (depuração).
3.18.**1.13.4** Acesso concorrente de administradores.
3.18.**1.13.5** Deverá permitir usar palavras chaves para facilitar identificação de regras.
3.18.**1.13.6** Definição de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
3.18.**1.13.7** Autenticação integrada à base de dados local.
3.18.**1.13.8** Deverá possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, sub rede) na base de regras.
3.18.**1.13.9** Criação de regras que fiquem ativas em horário definido.
3.18.**1.13.10** Backup das configurações e rollback de configuração para a última configuração salva.
3.18.**1.13.11** Habilidade de upgrade via interface de gerenciamento.
3.18.**1.13.12** Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado.
3.18.**1.13.13** Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções.
3.18.**1.13.14** Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção.
3.18.**1.13.15** Deverá permitir a criação de objetos e políticas compartilhadas.
3.18.1.13.16 Capacidade de definir administradores com diferentes perfis de acesso com no mínimo, as permissões de Leitura/Escrita e somente Leitura.
3.18.**1.13.17** Solução deverá ser capaz de detectar ataques de tentativa de *login* e senha utilizando tipos diferentes de credencias.

3.18.1.13.18 O sistema deverá ser capaz de gerenciar de modo central as políticas de backup dos equipamentos remotos.
3.18.1.13.19 O sistema deverá permitir habilitar uma mensagem de disclaimer (isenção de responsabilidade) na página de *login* da Interface de Administração. Ou seja, a página de *login* deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.
3.18.1.13.20 Deverá suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada.
3.18.1.13.21 Deverá suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider).

3.19 DAS FUNCIONALIDADES DE ANÁLISE DE LOG:
3.19.1 Deverá prover análise de tráfego de rede de modo centralizado.
3.19.2 Deverá possuir análise de tráfego de rede e ameaças por geolocalização.
3.19.3 Deverá ser capaz de receber os *logs* e eventos com o objetivo de prover os seguintes tipos de análises:
3.19.3.1 Análise de ameaças e incidentes de segurança.
3.19.3.2 Análise de tráfego e uso de categorias Web.
3.19.3.3 Análise de tráfego e uso de aplicativos.
3.19.3.4 Análise de tráfego e ameaças por usuário.
3.19.3.5 Análise de desempenho de políticas de segurança.
3.19.3.6 A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de *logs*, consolidação de *logs*, arquivamento de *logs*, busca avançada de *logs.*
3.19.3.7 Deverá possuir ferramenta para salvar consultas avançadas.
3.19.3.8 Deverá possuir relatórios personalizados.
3.19.3.9 Deverá ser capaz de efetuar o arquivamento de relatórios.
3.19.3.10 Deverá possuir agendamento de relatórios.
3.19.3.11 Os relatórios deverão no mínimo, serem exportados em formatos flexíveis (PDF, CSV).

4. JUSTIFICATIVAS

4.1. JUSTIFICATIVA DE CONTRATAÇÃO
4.1.1 - **O *firewall*** é um ativo de segurança da informação, fundamental numa rede de dados, uma vez que ele regula e monitora todo o tráfego de entrada e saída na rede de computadores.
4.1.2 - Por meio da introspecção dos dados de rede, *o firewall* é capaz de bloquear acessos não autorizados ou nocivos, mediar o uso de internet, criar conexões de rede seguras, bem como oferecer atualizações para ameaças.
4.1.3 - As soluções de *firewall* da próxima geração (*Next Generation Firewall*) são tecnologias modernas que representam um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes confiáveis (rede interna) e não confiáveis (*Internet*) e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Isso é possível, através de um sistema de detecção de intrusões, *anti-malware* na camada de rede, filtragem de tráfego *web* malicioso e a inspeção de tráfego SSL, na busca de ameaças camufladas sobre acamada de criptografia.
4.1.4 - Tendo em vista a pandemia que se iniciou no ano de 2020 de COVID-19, junto com as medidas adotadas para tentar frear a contaminação da população, houve uma mudança no paradigma da interação das pessoas com a procura de serviços públicos, demandando da gestão, disponibilizar mais serviços no âmbito da internet, impactando na atual estrutura de Tecnologia de Informação do município.
4.1.5 - Essa estrutura, principalmente a de *firewall e e-mail,* está muito defasada, ocasionando problemas frequentes como: longas interrupções na internet, lentidão para navegação, lentidão de sistemas hospedados em nuvens e falta de espaço local para mais contas de *e-mail* que o município necessite.
4.1.6 - Com essa defasagem de equipamento, pode ocorrer uma parada crítica onde o mesmo não volte mais a funcionar, tendo forte impacto nos serviços disponibilizados e incapacidade de alguns setores de atender ao público, entre outros serviços internos.

4.1.7 - Hoje, *e-mail* e *firewall* se encontram em um mesmo equipamento, próprio do município e nele estão os softwares, os quais não possuem mais suporte caso ocorra algum problema, pois o fabricante descontinuou a versão desde o ano de 2018. Sendo assim, além dos problemas citados acima, ainda ocorre que esse tipo de estrutura fica muito vulnerável a *cyber*-ataques, colocando em risco a segurança das informações.
4.1.8 - Além dessas constatações, ainda está em processo de migração para *cloud computing* (computação em nuvem) o *software* utilizado na Secretaria Municipal de Saúde, o qual será utilizado em nuvem onde terá uma grande necessidade de controle de tráfego de internet, na qual a estrutura atual mesmo sem esse acréscimo, já apresenta falhas freqüentes.
4.1.9 - Com todos esses avanços necessários, aumentará ainda mais o tráfego de dados na rede, e ainda considerando que atualmente o município possui um equipamento não apropriado e *software* de *firewall* e *e-mail* defasados, será imprescindível proteger o que entra ou sai da rede interna da prefeitura. Para realizar essa proteção, é necessário equipamento com especificações superiores – *Next Generation Firewall*, uma vez que o tráfego a ser analisado será substancialmente maior.
4.1.10 - Os **gerenciadores de e-mails** são programas para computadores que gerenciam contas de e-mail, para que possam ser operadas sem o uso de navegadores.
4.1.11 - O **acesso remoto** permite tanto que seus colaboradores acessem dados, e-mails e outros tipos de documentos por meio de qualquer dispositivo, como também possibilita que o suporte técnico de uma empresa manipule uma máquina e solucione o problema sem estar presente no mesmo local.
4.1.12 - Através da instalação e configuração de **módulos de automação (I/O - Input/Output)** e suas respectivas licenças no software de gerenciamento do CFTV é possível integrar, por exemplo, um sistema de controle de acesso, permitindo monitorar status de equipamentos e, também, controlar os mesmos.
4.1.13 - Os sistemas I/O (Input/Output) são módulos que têm a função de organizar e controlar o fluxo de dados produzidos pelas máquinas da empresa (entrada/input e saída/output).
4.1.14 - Os módulos de I/O geralmente executam algumas das seguintes funções: controle e temporização, comunicação com o processador, comunicação com periférico, armazenamento temporário de dados e detecção de erros.
4.1.15 - O **módulo de antivírus** serve para scanear ativamente os dados transferidos ao navegar na internet para evitar que malware seja baixado e executado no computador.
4.1.16 - Podemos citar alguns benefícios deste módulo como: segurança, automação, locais de trabalho mais seguros e aeroportos mais rápidos.

5. CONDIÇÕES DE PRAZOS, LOCAL, ENTREGA E VIGÊNCIA CONTRATUAL
5.1 Os serviços deverão ser executados mediante solicitação formal da contratante, por meio de Nota de Empenho, na sede da Prefeitura Municipal, localizada na Rua Caramuru, 271, Centro, Pato Branco - PR.
5.2 O recebimento do objeto se dará conforme o disposto no artigo 73, inciso I alíneas “a” e “b” e art. 76 da Lei n.º 8.666/93, e compreenderá duas etapas distintas, a seguir discriminadas:
a) Recebimento Provisório: Deverá começar no início da prestação de serviços (instalação) e consistirá na mera verificação da conformidade com as especificações técnicas. Deverá ser finalizado em **até 24 (vinte e quatro) horas** após a conclusão do serviço.
b) Recebimento Definitivo: Ocorrerá em até **48 (quarenta e oito) horas**, após o Recebimento Provisório, pela Comissão de Avaliação Técnica e constará de:
I - Verificação da conformidade com as especificações técnicas exigidas em cada etapa e se estas atendem plenamente aos requisitos de forma aderente aos termos contratuais.
II - O recebimento definitivo dar-se-á mediante termo circunstanciado de Recebimento Definitivo e posterior certificação na Nota Fiscal, autorizando assim o pagamento.
III - Constatada(s) irregularidade(s) nos serviços contratados, a Administração Municipal poderá rejeitá-los no todo ou em parte, determinando o seu ajuste, às suas expensas, em um prazo que **deverá se iniciar no máximo em até 02 (dois) dias**, contados da assinatura do recebimento da notificação formal, pela Contratada, observando o disposto no art. 69, da Lei 8.666/93 e deverá ser concluído **em até 05(cinco) dias.**

5.3 Os serviços serão considerados aceitos somente após emissão do termo circunstanciado de Recebimento Definitivo devidamente documentado e assinado pelo gestor e/ou fiscal do Contrato de Prestação de Serviços.
5.4 Na hipótese de verificação a que se refere o recebimento definitivo, não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.
5.5 A fiscalização por parte do município e o recebimento provisório ou definitivo não excluem a responsabilidade civil da Contratada pela correção e/ou substituição do objeto contratual, bem como pelos danos e prejuízos ao município ou a terceiros, decorrentes da má execução/desconformidades com as normas técnicas exigíveis, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

5.6 Prazo de Execução: O prazo de execução será de até 15 (quinze) dias, contados a partir do Recebimento da Nota de Empenho.

5.7 Prazo de Vigência: O prazo de vigência será de 12 (doze) meses, contados a partir da assinatura do Contrato de Prestação de Serviços, podendo ser prorrogado conforme legislação vigente e de acordo entre as partes, conforme contempla o Artigo 57, da Lei nº 8.666/93, mediante Termo de Aditamento.

5.8. PRESTAÇÃO DE SERVIÇO DE INSTALAÇÃO
5.8.1 - Para as soluções ofertadas, a Contratada deverá cotar um valor total para a instalação, configuração e treinamento para os dispositivos adquiridos.
5.8.2 - Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, funcionalidades e políticas.
5.8.3 - A instalação deverá ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante.
5.8.4 - Deverá ser realizada a configuração das regras de entrada, saída.
5.8.5 - Configuração do Active Directory.

5.8.6. TREINAMENTO PARA O SISTEMA FIREWALL UTM:
5.8.6.1 - Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware e software) para a equipe do setor de tecnologia da informação (T.I) da Contratante.
5.8.6.2 - Este treinamento deverá possuir carga horária mínima de 08 horas.
5.8.6.3 - O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação.
5.8.6.4 - O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas.
5.8.6.5 - O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta.
5.8.6.6 - Deverá ser incluso, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada.
5.8.6.7 - Os cursos deverão ser realizados em horários e data a serem acordados pela Contratada e pela Contratante.

5.9. PRESTAÇÃO DE SERVIÇOS DE SUPORTE TÉCNICO E REMOTO:
5.9.1 - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis 24 x 07 x 365 (vinte e quatro horas por dia sete dias por semana e trezentos e sessenta e cinco dias no ano), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR), com as seguintes características:
5.9.1.1 - A Contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede, relativos aos equipamentos e/ou produtos fornecidos.

5.9.1.2 Os chamados para o suporte técnico serão classificados por severidade, conforme impacto no ambiente computacional do município:
5.9.1.2.1 - Severidade 01: Sistema crítico, em produção, está parado ou fora de funcionamento, não há meios de contornar a não conformidade. Número significativo de usuários afetados, impacto operacional significativo causado.
5.9.1.2.2 - Severidade 02: Sistema crítico, em produção, está apresentando falhas de funcionamento, não causou interrupção do serviço, no entanto, afeta significativamente o desempenho, com impacto crítico aos usuários.
5.9.1.2.3 - Severidade 03: Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impacto moderado aos usuários. Impacto operacional moderado.
5.9.1.2.4 - Severidade 04: Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features ou melhorias. Impacto mínimo aos usuários. Sem impacto operacional.
5.9.1.3 - Para mensurar o nível de criticidade da não conformidade, serão utilizados os indicadores de severidade. Os chamados, conforme o nível de severidade, definidos pelos técnicos da contratante, terão prazo para resolução, contados a partir do momento do registro da solicitação em service desk de comunicação com a contratada. Segue o aprazamento para resolução de não conformidade:

Descrição do Nível de Criticidade	Tempo Máximo para Resolução
Severidade 1	01 hora corrida
Severidade 2	04 horas corridas
Severidade 3	16 horas úteis
Severidade 4	24 horas úteis

5.9.1.4 - Sendo entendido que:
5.9.1.4.1 – Hora corrida é a compreendida entre o período de 0h00min as 24h00min, 07 (dias por semana). Hora útil é a compreendida entre o período de 08h00min às 18h00min, de segunda a sexta-feira, excetuando-se feriados nacionais.
5.9.1.4.2 - Será admitida solução de contorno (redução ou eliminação do impacto de um incidente ou problema para o qual uma solução completa ainda não está disponível), na resolução de chamados de severidade 01 e 02, para fins de atendimento dos prazos estipulados.
5.9.1.4.3 - Considera-se não conformidade plenamente solucionada quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva.
5.9.1.4.4 - A Contratada não será responsabilizada por descumprimento de prazo para resolução de não conformidade, quando a demanda for originada por falha, interrupção, inconsistência de dados e informações gerados pela Contratante ou terceiros da Contratante. Nestas ocorrências, a Contratada deverá emitir parecer comprovando que a não conformidade não se originou no cumprimento do objeto contratado.
5.9.1.4.5 - Toda intervenção no ambiente produtivo da Contratante, que resulte na necessidade de suporte técnico pela Contratada, deverá ser executada somente após autorização do Setor de Tecnologia de Informação (TI), a partir de informações claras sobre o impacto da ação nos procedimentos que serão adotados.
5.9.1.4.6 - Na finalização do chamado, o técnico responsável pela Contratada realizará, em conjunto com representantes técnicos da Contratante, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema. O tempo utilizado nos testes não será computado no aprazamento de resolução da não conformidade.
5.9.1.4.7 - Ao término dos testes e do atendimento (fechamento do chamado), a Contratada deverá formalizar a Contratante, de forma detalhada, as causas da não conformidade e solução definitiva adotada.
5.9.1.4.8 - Nos casos em que o atendimento não se mostrar satisfatório, a Contratante fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

6. OBRIGAÇÕES DA CONTRATADA

6.1. Manter todas as condições de habilitação, qualificação e as obrigações exigidas durante toda a vigência Contratual, de acordo com o art. 55, XIII, da Lei 8.666/93, informando a Contratante à ocorrência de qualquer alteração nas referidas condições.
6.2. Prestar os serviços contratados, em estrita conformidade com as especificações contidas no contrato e na proposta de preços apresentada, aos quais se vincula, não sendo admitidas retificações, cancelamentos, quer seja de preços, quer seja nas condições estabelecidas.
6.3. Comunicar imediatamente a Contratante, no caso de ocorrência de qualquer fato que possa implicar no atraso dos serviços contratados e a qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias.
6.4. Executar os serviços com pontualidade, atendendo a todas as condições estabelecidas:
6.5. Os equipamentos contemplados no lote 01 deverão ser novos em número de 02 (dois), serão de propriedade da Contratada e serão disponibilizados durante todo o prazo contratual para o uso da Contratante, em forma de comodato.
6.6. Todos os equipamentos cedidos em comodato (lote 01) para a execução do serviço deverão ser de boa qualidade e desempenho e caso seja necessário, deverá possuir certificação do órgão responsável e/ou garantia do fabricante.
6.7. A Contratada deverá realizar a instalação dos produtos contratados, bem como apresentar carta do fabricante quanto ao fornecimento, garantia e funcionalidade dos produtos ofertados.
6.8. A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante.
6.9. Os serviços de manutenção (preventiva, corretiva e/ou evolutiva) deverão ser realizados por profissionais qualificados, de forma que consigam executar os serviços com perfeição e rapidez e possam prestar qualquer informação técnica solicitada a respeito do sistema. Nos casos de manutenção preventiva deverá ser feita a verificação de todo o objeto, a fim de detectar inconformidades capazes de prejudicar o funcionamento do sistema.
6.10. Toda e qualquer substituição e/ou manutenção corretiva dos equipamentos correrão por conta e as expensas da Contratada e não serão em nenhuma hipótese de responsabilidade da Contratante.
6.11. Em caso de falha verificada por parte da Contratante, a mesma através do gestor do contrato ou pessoa designada por ele, solicitará visita técnica para a Contratada, para o envio de profissional qualificado e devidamente identificado.
6.12. Responder por danos e desaparecimentos de bens materiais e avarias que venham a ser causadas por seus empregados ou preposto à Contratante ou a terceiros, desde que fique comprovada sua culpa ou dolo, não excluindo ou reduzindo sua responsabilidade a fiscalização ou o acompanhamento realizado pela Contratante, de acordo com o art. 70 da Lei n.º 8.666/93.
6.13. Observar rigorosamente as normas técnicas, regulamentadoras, de segurança, de higiene, ambientais e medicina do trabalho. Além disso, deverão obedecer às normas técnicas de proteção ao meio ambiente e adotar boas práticas de otimização de recursos, redução de desperdícios, menor poluição, conforme legislação vigente**.**
6.14. A Contratada deverá garantir a qualidade dos serviços prestados e materiais empregados, devendo reparar, corrigir, remover, substituir às suas expensas, no total ou em parte, os materiais e/ou serviços prestados que se verificarem vícios, defeitos, incorreções ou má qualidade no serviço realizado.
6.15. Constatada(s) irregularidade(s) nos serviços contratados, a Administração Municipal poderá rejeitá-los no todo ou em parte, determinando o seu ajuste, às suas expensas (caso não se enquadre serviços de atendimento e suporte técnico, subitem 6.23), em um prazo que **deverá se iniciar no máximo em até 02 (dois) dias**, contados da assinatura do recebimento da notificação formal, pela Contratada, observando o disposto no art. 69, da Lei 8.666/93 e deverá ser concluído **em até 05 (cinco) dias**.
6.16. É de responsabilidade da Contratada, selecionar e contratar pessoal devidamente habilitado para a função a ser exercida na execução dos serviços, em seu nome, observando rigorosamente todas as prescrições relativas às leis trabalhistas, previdenciárias, assistenciais, securitárias e sindicais, indenizações e despesas por acidentes de trabalho que eventualmente ocorram durante a prestação de serviço, sendo considerada como única empregadora.
6.17. Responsabiliza-se perante o Município, por todos os atos de seus subordinados durante a execução dos serviços, devendo afastar, dentro de 24 (vinte e quatro) horas, por comunicação escrita,

qualquer de seus empregados cuja permanência nos serviços for julgada, inconveniente. Os empregados eventualmente afastados deverão ser substituídos por outros de categoria profissional idêntica.

6.18. Manter atualizada a relação de funcionários que poderão atuar junto a Contratante, na execução do contrato. Em caso de desligamento, a Contratada deverá imediatamente, retirar todas as credenciais que permitam ao(s) funcionário(s), qualquer acesso ao serviço provido, bem como, deverá informar o fato ao gestor e/ou fiscal do contrato.

6.19. Manter por si, por seus prepostos e contratados, irrestrito e total sigilo sobre quaisquer dados confidenciais da Contratante a que tiver acesso, inerentes do objeto da licitação, respondendo contratual e legalmente pela inobservância desta alínea, inclusive após o término do contrato.

6.20. A expressão "informação irrestrito e total sigilo" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível.

6.21. Guardar todas as informações confidenciais em local seguro, de forma que estejam adequadamente protegidas contra roubo, dano, perda ou acesso não autorizado, de acordo com padrões que sejam, no mínimo, equivalentes àqueles aplicados às informações confidenciais da Contratada.

6.22. Não utilizar nome/marca ou qualquer material desenvolvido pela Contratante, assim como os dados dos funcionários a que tenha acesso no decorrer das atividades inerentes a este Contrato de Prestação de Serviços, em ações desenvolvidas pela Contratada fora do âmbito de atuação deste processo de licitação.

6.23. Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis 24 x 07 x 365 (vinte e quatro horas por dia sete dias por semana e trezentos e sessenta e cinco dias no ano), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR), com as seguintes características:

6.23.1 - A Contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede, relativos aos equipamentos e/ou produtos fornecidos

6.23.2 - Os chamados para o suporte técnico serão classificados por severidade, conforme impacto no ambiente computacional do município:

6.23.2.1 -**Severidade 01**: Sistema crítico, em produção, está parado ou fora de funcionamento, não há meios de contornar a não conformidade. Número significativo de usuários afetados, impacto operacional significativo causado.

6.23.2.2 -**Severidade 02**: Sistema crítico, em produção, está apresentando falhas de funcionamento, não causou interrupção do serviço, no entanto, afeta significativamente o desempenho, com impacto crítico aos usuários.

6.23.2.3 - **Severidade 03**: Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impacto moderado aos usuários. Impacto operacional moderado.

6.23.2.4 - **Severidade 04:** Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features[2] ou melhorias. Impacto mínimo aos usuários. Sem impacto operacional.

6.24 – Para mensurar o nível de criticidade da não conformidade, serão utilizados os indicadores de severidade. Os chamados, conforme o nível de severidade, definidos pelos técnicos da contratante, terão prazo para resolução, contados a partir do momento do registro da solicitação em service desk[3] de comunicação com a contratada. Segue o aprazamento para resolução de não conformidade:

Descrição do Nível de Criticidade	Tempo Máximo para Resolução
Severidade 1	01 hora corrida
Severidade 2	04 horas corridas
Severidade 3	16 horas úteis

[2] Features são funcionalidades ou recursos desenvolvidos por um time de pessoas, geralmente de produtos e plataformas digitais que tem como propósito adicionar uma nova entrega de valor e experiência para seus usuários.

[3] O Service Desk é um conceito que tem como objetivo centralizar e unir todas as necessidades de uma empresa em um único lugar, gerindo todo o apoio operacional aos usuários de um sistema e registrando todas interações como forma de controle e monitoramento da organização.

Severidade 4	24 horas úteis

6.24.1 - Sendo entendido que:
6.24.1.1 -Hora corrida é a compreendida entre o período de 0h00min as 24h00min, 07 (dias por semana). Hora útil é a compreendida entre o período de 08h00min às 18h00min, de segunda a sexta-feira, excetuando-se feriados nacionais
6.24.1.2 - Será admitida solução de contorno (redução ou eliminação do impacto de um incidente ou problema para o qual uma solução completa ainda não está disponível), na resolução de chamados de severidade 01 e 02, para fins de atendimento dos prazos estipulados
6.24.1.3 - Considera-se não conformidade plenamente solucionada quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva
6.24.1.4 - A Contratada não será responsabilizada por descumprimento de prazo para resolução de não conformidade, quando a demanda for originada por falha, interrupção, inconsistência de dados e informações gerados pela Contratante ou terceiros da Contratante. Nestas ocorrências, a Contratada deverá emitir parecer comprovando que a não conformidade não se originou no cumprimento do objeto contratado
6.24.1.5 - Toda intervenção no ambiente produtivo da Contratante, que resulte na necessidade de suporte técnico pela Contratada, deverá ser executada somente após autorização do Setor de Tecnologia de Informação (TI), a partir de informações claras sobre o impacto da ação nos procedimentos que serão adotados
6.24.1.6 - Na finalização do chamado, o técnico da Contratada realizará, em conjunto com representantes técnicos da Contratante, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema. O tempo utilizado nos testes não será computado no aprazamento de resolução da não conformidade
6.24.1.7 - Ao término dos testes e do atendimento (fechamento do chamado), a Contratada deverá formalizar a Contratante, de forma detalhada, as causas da não conformidade e solução definitiva adotada
6.24.1.8 - Nos casos em que o atendimento não se mostrar satisfatório, a Contratante fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado
6.24.1.9 - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis em horário comercial, de segunda a sexta-feira das 08h00min às 17h30min, (exceto feriados), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR).
6.25 – A Contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativas aos equipamentos e/ou produtos fornecidos
6.26 - A Contratada deverá iniciar o atendimento de suporte técnico em até 08 horas úteis, após a abertura do chamado
6.27 - Disponibilizar instrutores para o(s) treinamento(s) de utilização dos softwares em local definido em conjunto com o fiscal e/ou gestor do contrato
6.28 - Disponibilizar (caso haja a necessidade), de treinamento(s) adicional (is), o(s) qual (is), deverá(ão) ser(em) aplicado(s), para os servidores municipais diretamente ligados a área de tecnologia de informação do município e, em conjunto com o fiscal e/ou gestor do contrato.
6.29 - Apresentar os seus empregados devidamente uniformizados e identificados por meio de crachá, além de fornecer a todos os seus funcionários e preposto(s) o tipo adequado de equipamento de proteção individual – EPI, bem como fiscalizar o uso dos mesmos. A Contratada, em qualquer hipótese, não se eximirá da total responsabilidade quanto à negligência ou descumprimento da Lei nº 6.514 de 22/12/77 – Portaria nº 3.214, de 08/06/78 - Normas Regulamentadoras
6.30 - Não manter em seu quadro de pessoal, menores de idade, em horário noturno de trabalho ou em serviços perigosos ou insalubres, não manter, ainda, em qualquer trabalho, menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos
6.31 Todas as decisões e entendimentos havidos entre as partes durante o andamento dos trabalhos e que impliquem em modificações ou implementações nos planos, cronogramas ou atividades pactuadas, deverão ser prévia e formalmente acordados e documentadas entre as partes

6.32 Nos preços cotados deverão estar inclusos todos os equipamentos, insumos e demais custos que compõem a demanda, bem como as despesas com impostos, tributos, taxas, fretes, seguros e quaisquer outros que incidam direta ou indiretamente execução dos serviços, como por exemplo: transporte, carga e descarga, deslocamento, hospedagens, alimentação e outros eventuais custos envolvidos
6.33 Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que se está obrigada
6.34 Todos os casos atípicos não mencionados neste Edital deverão ser apresentados à fiscalização para sua definição e determinação
6.35 Cumprir com outras obrigações decorrentes da aplicação do Código de Proteção e Defesa do Consumidor - conforme Lei nº 8.078/90, que sejam compatíveis com o regime de direito público.
6.36 Para os Lotes 02 e 03: Apresentar certificação Data Center TIER 3, conforme preconiza a norma TIA 942, para o gestor e/ou fiscal do contrato em até 72 (setenta e duas) horas, contados a partir do Recebimento da Nota de Empenho.

7. OBRIGAÇÕES DA CONTRATADA RELATIVAS A CRITÉRIOS DE SUSTENTABILIDADE
7.1. As boas práticas de otimização de recursos, redução de desperdícios e menor poluição se pautam em alguns pressupostos e exigências, que deverão ser observados pela Contratada, que deverá fazer uso racional do consumo de energia e água, adotando medidas para evitar o desperdício.
7.2. Colaborar com as medidas de redução de consumo e uso racional da água, cujo(s) encarregado(s) deve(m) atuar como facilitador (es) das mudanças de comportamento.
7.3. Dar preferência à aquisição e uso de equipamentos e complementos que promovam a redução do consumo de água e que apresentem eficiência energética e redução de consumo.
7.4. Evitar ao máximo o uso de extensões elétricas.
7.5. Repassar a seus empregados todas as orientações referentes à redução do consumo de energia e água.
7.6. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução dos serviços.
7.7. Dar preferência a descarga e torneira com controle de vazão, evitando o desperdício de água.
7.8. Proporcionar treinamento periódico aos empregados sobre práticas de sustentabilidade, em especial sobre redução de consumo de energia elétrica, de consumo de água e destinação de resíduos sólidos, observadas as normas ambientais vigentes.
7.9. Proibir quaisquer atos de preconceito de raça, cor, sexo, crenças religiosas, orientação sexual ou estado civil na seleção de colaboradores no quadro da empresa.
7.10. Conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e à saúde dos trabalhadores e envolvidos na prestação dos serviços.
7.11. Destinar de forma ambientalmente adequada todos os materiais e/ou insumos que forem utilizados pela empresa na prestação dos serviços, inclusive os potencialmente poluidores, tais como, pilhas, baterias, lâmpadas fluorescentes e frascos de aerossóis, pneumáticos inservíveis, produtos e componentes eletroeletrônicos que estejam em desuso e sujeitos à disposição final, considerados lixo tecnológico.
7.12. É proibido incinerar qualquer resíduo gerado.
7.13. Não é permitida a emissão de ruídos de alta intensidade.
7.14. Priorizar a aquisição de bens que sejam constituídos por material renovável, reciclado, atóxico ou biodegradável.
7.15. Priorizar o aproveitamento da água da chuva, agregando ao sistema hidráulico elementos que possibilitem a captação, transporte, armazenamento e seu aproveitamento.
7.16. Colaborar para a não geração de resíduos e, secundariamente, a redução, a reutilização, a reciclagem, o tratamento dos resíduos sólidos e a disposição final ambientalmente adequada dos rejeitos.
7.17. A Contratada deverá observar no que couber, durante a execução contratual, critérios e práticas de sustentabilidade, como:
6.17.1 Dar preferência ao envio de documentos na forma digital, a fim de reduzir a impressão de documentos.

6.17.2 Em caso de necessidade de envio de documentos à Contratante, usar preferencialmente a função "duplex" (frente e verso), bem como de papel confeccionado com madeira de origem legal.
7.18. Capacitar seus empregados, orientando que os resíduos não poderão ser dispostos em aterros de resíduos domiciliares, áreas de "bota fora", encostas, corpos d' água, lotes vagos e áreas protegidas por Lei, bem como em áreas não licenciadas.
7.19. Deverá, se possível, adotar práticas de sustentabilidade e de racionalização no uso de materiais e serviços, incluindo uma política de separação dos resíduos recicláveis descartados e sua destinação às associações e cooperativas dos catadores de materiais recicláveis.
7.20. Armazenar, transportar e destinar os resíduos em conformidade com as normas técnicas específicas.

8. OBRIGAÇÕES DA CONTRATANTE
8.1. Designar pessoa responsável para o acompanhamento dos serviços contratados, no local indicado, sendo que ele atestará a execução, conforme disposto nas condições e demais especificações contidas no Contrato de Prestação de Serviços e na Nota de Empenho.
8.2. Cumprir com todos os compromissos financeiros assumidos com a Contratada.
8.3. Comunicar prontamente a Contratada, qualquer anormalidade no objeto desde Contrato de Prestação de Serviços, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas.
8.4. Responsabilizar-se pelos custos da infraestrutura necessária para suportar o *appliance* virtual (caso seja necessário).
8.5. Os treinamentos serão aplicados nas dependências da prefeitura municipal, que por sua vez, deverá disponibilizar os funcionários (setor de Tecnologia da Informação), providenciar as instalações físicas e os demais equipamentos necessários para a execução do treinamento.
8.6. Aplicar as sanções administrativas contratuais, em caso de inadimplência.
8.7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.
8.8. Permitir que os funcionários da Contratada tenham acesso aos locais de execução dos serviços.
8.9. Todas as decisões e entendimentos havidos entre as partes durante o andamento dos trabalhos e que impliquem em modificações ou implementações nos planos, cronogramas ou atividades pactuadas, deverão ser prévia e formalmente acordados e documentadas entre as partes.
8.10. Proceder ao recebimento provisório do objeto e, não havendo mais pendências, a administração promoverá o recebimento definitivo dos serviços, mediante vistoria detalhada realizada pela Comissão de Fiscalização e Recebimento de Bens, designada pelo Município, nos termos da Lei 8.666/93, em seu artigo 73, inciso I.
8.11. Fornecer, a qualquer tempo, mediante solicitação escrita da Contratada, informações adicionais, dirimir dúvidas e orientar em todos os casos omissos.

9. CONDIÇÕES DE PAGAMENTO
9.1 Para a Instalação (Lote 03, item 01): O pagamento será realizado até o 15º (décimo quinto) dia útil, após a instalação do objeto e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços.
9.2 Para Manutenção (demais itens): O pagamento será realizado mensalmente até o 15º (décimo quinto) dia útil, do mês subsequente a execução dos serviços e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços

Lote	Item	Valor Mensal	Valor Total 12 meses	Valor da Parcela Única
1	1	R$ 39.269,94	R$ 471.239,28	
1	2	R$ 3.466,67	R$ 41.600,04	
2	1	R$ 3.183,33	R$ 38.199,96	
3	1	--	--	R$ 5.600,00

3	2	R$ 1.252,80	R$ 15.033,60	
3	3	R$ 907,65	R$ 10.891,80	
4	1	R$ 907,40	R$ 10.888,80	

Tabela 01 – Parcelas de cada item

9.3 O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.
9.4 A nota fiscal/fatura deverá conter discriminação resumida do item contratado, número da licitação, número do Contrato de Prestação de serviços, não apresentar rasura e/ou entrelinhas, deverão ser impressas de maneira clara, inteligível, inviolável, ordenada e dentro de padrão uniforme.
9.5 Para fazer jus ao pagamento, a empresa deverá apresentar, prova de regularidade para com a Fazenda Federal, Estadual e Municipal, prova de regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS) e Certidão Negativa de Débitos Trabalhistas (CNDT) emitida eletronicamente através do site http://www.tst.jus.br, em cumprimento com as obrigações assumidas na fase de habilitação do processo licitatório.
9.6 O cadastro no SICAF vigente, ou Certificado de Registro Cadastral (CRC) emitido pela Divisão de Licitações do Município de Pato Branco (desde que válidos), poderão substituir os documentos indicados no subitem 9.5.
9.7 O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.
9.8 Os pagamentos correrão por conta dos recursos das Dotações Orçamentárias (Despesas e Desdobramentos respectivamente) conforme planilha em anexo.
9.9 Em caso de atraso de pagamento motivado exclusivamente pela contratante, como critério para correção monetária aplicar-se-á o IPCA - Índice Nacional de Preços ao Consumidor Amplo calculado pelo IBGE. Em caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante juros moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples. Quando da incidência da correção monetária e juros moratórios, os valores serão computados a partir do vencimento do prazo de pagamento de cada parcela devida.

10. DOTAÇÃO ORÇAMENTÁRIA
10.1 - As despesas decorrentes desta licitação ocorrerão por conta do recurso da Dotação Orçamentária:
a) 04 SEC.MUN.DE PLANEJAMENTO URBANO - 04.02 DEPARTAMENTO DE DESENVOLVIMENTO URBANO - 1545100182238000 Manutencao do Departamento de Planejamento Urbano - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2238 – Despesa 101 – Desdobramentos (9857-9873).
b) 05 SEC.MUN.DE ADMINISTRAÇÃO E FINANÇAS - 05.02 DEPARTAMENTO ADMINISTRATIVO - 0412200072216000 Manutencao das atividades do Departamento Administrativo - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 510 Recursos Ordinarios (Livres) – Ação 2216 – Despesa 184 – Desdobramentos (2015-3251).
c) 06 SEC.MUN.DE ENGENHARIA E OBRAS E SERVIÇOS PÚBLICOS - 06.02 DEPARTAMENTO DE ENGENHARIA - 1545200192021000 Manutencao das atividades do Departamento DE Engenharia e Obras - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2021 – Despesa 414 – Desdobramentos (2021-3460).
d) 07 SEC.MUN.DE EDUCAÇÃO E CULTURA - 07.02 DEPARTAMENTO ADMINISTRATIVO - 1236500392095000 Manutencao dos Centros de Educação Infantil - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 103 Recursos Ordinarios (Livres) – Ação 2095 – Despesa 1726 – Desdobramentos (9357-9875).
e) 08 SEC.MUN.DE DE SAÚDE - 08.02 ADMINISTRAÇÃO DA SAUDE - 1030100432388000 Manutencao das atividades da Saude - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 303 Recursos Ordinarios (Livres) – Ação 2388– Despesa 1652 – Desdobramentos (2407-3416).

f) 09 SEC.MUN.DE ASSISTÊNCIA SOCIAL – 09.04 FUNDO MUNICIPAL DE ASSISTÊNCIA SOCIAL - 0824400242202000 Manutencao das atividades da Gestão de Assistência Social - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2202 – Despesa 751 – Desdobramentos (9884-9876).
g) 10 SEC.MUN.DE DESENVOLVIMENTO ECONÔMICO - 10.02 DEPARTAMENTO DE DESENVOLVIMENTO ECONÔMICO - 2369100272029000 Manter Aeroporto - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2029 – Despesa 891 – Desdobramentos (9862-9877).
h) 10 SEC.MUN.DE DESENVOLVIMENTO ECONÔMICO - 10.02 DEPARTAMENTO DE DESENVOLVIMENTO ECONÔMICO – 2369500282062000 Fomento ao Turismo - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2062 – Despesa 907 – Desdobramentos (9863-9878).
i) 11 SEC.MUN.DE AGRICULTURA - 11.02 DEPARTAMENTO DE AGRICULTURA – 2060600292070000 Manutenção das atividades de Desenvolvimento Rural - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2070 – Despesa 957– Desdobramentos (9864-9879).
j) 11 SEC.MUN.DE AGRICULTURA - 11.02 DEPARTAMENTO DE AGRICULTURA – 2060600292073000 Manutenção das atividades do Interior - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2073 – Despesa 978– Desdobramentos (9865-9880).
k) 16 SEC.MUN.DE ESPORTE E LAZER - 16.02 DEPARTAMENTO DE ESPORTE E LAZER – 2781200412224000 Manutenção das atividades do Dpto de Esporte e Lazer - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2224 – Despesa 1194 – Desdobramentos (9866-9881).
l) 17 SEC.MUN.DE CIÊNCIA E TECNOLOGIA - 17.02 DEPARTAMENTO DO PARQUE TECNOLÓGICO - 1957300252241000 Manutenção das atividades Do Departamento Administração e Financeiro - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2241 – Despesa 1243 – Desdobramentos (9279-9882).

10. DO REAJUSTE DE PREÇOS

10.1 - Os valores constantes da planilha orçamentária poderão ser reajustados pelo IGPM, apurados e fornecidos pela Fundação Getúlio Vargas, depois de decorrido 01 (um) ano da apresentação da proposta de preços.
10.2 - Não será concedido reajuste de preços resultante de atrasos ocorridos unicamente em decorrência da incapacidade da contratada em cumprir o prazo ajustado.
10.3 - Havendo atraso ou antecipação na execução dos serviços, relativamente à previsão do respectivo cronograma, que decorra da responsabilidade ou iniciativa do contratado, o reajustamento obedecerá às condições seguintes:
a) Quando houver atrasos, sem prejuízo da aplicação das sanções contratuais devidas pela mora, se os preços aumentarem, prevalecerá os índices vigentes na data em que deveria ter sido cumprida a obrigação.
b) Se os preços diminuírem prevalecerá os índices vigentes na data do efetivo cumprimento da obrigação.
c) A posterior recuperação do atraso não ensejará a atualização dos índices no período em que ocorrer a mora.
10.3 - O reajuste dar-se-á mediante solicitação formal da Contratada, e firmada através de Termo de Aditamento de acordado entre as partes.
10.4 - Caso haja alteração imprevisível no custo da prestação do serviço, caberá ao contratado requerer e demonstrar documentalmente, a necessidade de reequilíbrio econômico-financeiro do contrato com fundamento no artigo 65, II, “d” da Lei Federal n.º 8.666/93.
10.5 - Os valores recompostos somente serão repassados após a assinatura, devolução do Termo assinado (conforme o caso) e publicação do Termo de Aditamento.
10.6 - Não se admitirá nenhum encargo financeiro, como juros, despesas bancárias e ônus semelhantes.

11. EXTINÇÃO E RESCISÃO CONTRATUAL

11.1 - Será automaticamente extinto o contrato quando do término do prazo estipulado, e não ocorrendo o acordo de prorrogação.

11.2 - O contrato poderá ser rescindido amigavelmente pelas partes ou unilateralmente pela administração na ocorrência dos casos previstos nos Art. 77, 78 e 79 da Lei nº 8.666/93, cujo direito da administração o contratado expressamente reconhece.

12. ANTICORRUPÇÃO:

12.1 - As partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa (Lei Federal n.º 8.429/1992), a Lei Federal n.º 12.846/2013 e seus regulamentos, se comprometem que para a execução do contrato nenhuma das partes poderá oferecer, dar ou se comprometer a dar, a quem quer que seja, aceitar ou se comprometer a aceitar, de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios indevidos de qualquer espécie, de modo fraudulento que constituam prática ilegal ou de corrupção, bem como de manipular ou fraudar o equilíbrio econômico financeiro do contrato, seja de forma direta ou indireta quanto ao objeto do contrato, devendo garantir, ainda que seus prepostos, administradores e colaboradores ajam da mesma forma.

13. GESTOR DO REGISTRO DE PREÇOS

13.1 - A administração indica como **gestor** do contrato o Secretário de Administração e Finanças, ***Mauro José Sbarain***, matrícula n° 11.041-8/4.

13.2 - Entre suas atribuições está a de apurar a ocorrência de quaisquer circunstancias que incidam especificamente no art. 77, 78 e 88 da Lei 8666/93 que trata das Sanções Administrativas para o caso de inadimplemento contratual e cometimento de outros atos ilícitos.

13.3 - Compete ao gestor da Ata de Registro de Preços, no que couber, as atribuições previstas no Decreto Municipal nº 8.296 de 17 de abril de 2018.

13.4 - As decisões e providências que ultrapassarem a competência destes deverão ser solicitadas a autoridade superior, em tempo hábil, para a adoção das medidas convenientes.

14. FISCAL DO REGISTRO DE PREÇOS

14.1 - A administração indica como **fiscal técnico** do contrato, o servidor ***Eduardo Mello Amorim***, matrícula 10.145-1/1.

14.2 - Compete ao fiscal da Ata de Registro de Preços, no que couber, as atribuições previstas no Decreto Municipal nº 8.296 de 17 de abril de 2018.

14.3 - As decisões e providências que ultrapassarem a competência destes deverão ser solicitadas a autoridade superior, em tempo hábil, para a adoção das medidas convenientes.

15. SANÇÕES POR INADIMPLEMENTO

15.1 - Nos termos do Art. 7º da Lei 10.520/02, quem, convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e, será descredenciado no Sicaf, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4o desta Lei, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

15.2 - Das Sanções Administrativas, conforme previsto no Art. 5º do Decreto Municipal nº 8.441/19:

15.2.1 - As sanções administrativas serão aplicadas em conformidade com o prescrito na Lei Federal nº 8666/93, e em legislação correlata, podendo ser das seguintes espécies:

a) Advertência.

b) Multa, na forma prevista no instrumento convocatório ou na Ata de Preços.

c) Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração.

d) Declaração de inidoneidade.
e) Descredenciamento do sistema de registro cadastral.
15.2.2 - As sanções previstas nos subitens “a”, “c” e “d” do item 15.2.1, poderão ser aplicadas cumulativamente com a do subitem “b”.
15.3 - Das Particularidades da Multa, conforme previsto no Art. 7º do Decreto Municipal nº 8.441/19:
15.3.1 - A multa imposta ao contratado ou licitante, se não disposta de forma diferente no contrato, poderá ser:
a) de caráter moratório, na hipótese de atraso injustificado na entrega ou execução do objeto do contrato, quando será aplicada nos seguintes percentuais:
I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplida, quando o atraso não for superior 30 (trinta) dias corridos.
II - 0,66% (sessenta e seis centésimos por cento) por dia de atraso que exceder a alínea anterior, até o limite de 15 (quinze) dias, na entrega de material ou execução de serviços, calculado, desde o trigésimo primeiro dia de atraso, sobre o valor correspondente à parte inadimplida, em caráter excepcional, e a critério do órgão contratante.
b) de caráter compensatório, quando será aplicada nos seguintes percentuais.
I - 15% (quinze por cento) do valor do empenho em caso de inexecução parcial do objeto pela contratada ou nos casos de rescisão do contrato, calculada sobre a parte inadimplida.
II - 20% (vinte por cento) sobre o valor do contrato, pela sua inexecução total ou pela recusa injustificada do licitante adjudicatário em assinar a Ata de Registro de Preços ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração.
15.3.2 - O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do primeiro dia útil seguinte ao do vencimento do prazo de entrega ou execução do contrato.
15.4 - A instrução obedecerá ao princípio do contraditório, assegurada ao acusado ampla defesa, com a utilização dos meios e recursos admitidos em direito.
15.5 - Na fase de instrução, o indiciado será notificado pelo gestor do contrato e terá o prazo de 05 (cinco) dias úteis, contados a partir do recebimento do correio eletrônico no e-mail registrado em Ata/Contrato, para apresentação da Defesa Prévia, assegurando-se lhe vista do processo, e juntada dos documentos comprobatórios que considerar pertinentes à fundamentação dos fatos alegados na mesma.
15.6 - O extrato da decisão definitiva, bem como toda sanção aplicada, será anotada no histórico cadastral da empresa e nos sistemas cadastrais pertinentes, quando for o caso, além do processo ser apostilado na sua licitação correspondente.

Contrato nº __/2022/GP.

ANEXO II
CONTRATO DE PRESTAÇÃO DE SERVIÇOS

Que entre si celebram, o ***Município de Pato Branco,*** pessoa jurídica de direito público interno, inscrito no CNPJ sob nº 76.995.448/0001 -54 com sede e foro na Rua Caramuru, nº 271, centro, CEP: 85.501-064 em Pato Branco - PR, neste ato representado pelo seu Prefeito, o Sr. ***Robson Cantu***, brasileiro, portador do RG nº 1.816.183-4 SESP/PR, inscrito no CPF nº 441.436.649-68, residente e domiciliado na Rua Argentina n.º 02, Apto 702, Bairro Jardim das Américas, CEP 85.502-040, em Pato Branco – PR, de ora em diante denominado **CONTRATANTE**, e _____, pessoa jurídica de direito privado, inscrita no CNPJ nº _____, Inscrição Estadual nº _____ estabelecida _____,em _____, neste ato representada por _____, _____, inscrito no CPF nº _____, portador do RG nº _____, residente e domiciliado em _____, de ora em diante denominada **CONTRATADA,** tendo certa e ajustada a contratação, adiante especificada, cuja licitação foi promovida através do ***Edital de Pregão Eletrônico nº 82/2022*** - ***Processo n° 160/2022***, conforme autorização constante do protocolo nº 451136/2022, que independente da sua transcrição, integra o presente contrato que será regido pelas disposições da Lei nº 8.666/93 e suas posteriores alterações, do Código Civil e do Código do Consumidor, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - OBJETO

I - Constitui objeto do presente contrato o fornecimento de licença de uso, locação de softwares de Firewall – Next Generation, E-mail, Acesso Remoto, Automação e Antivírus, treinamento básico, atualização corretiva, adaptativa e evolutiva, diagnósticos, atendimento e suporte técnico, por tempo determinado, com fornecimento de equipamentos mediante o comodato (*hardware*), em atendimento as necessidades de todas as Secretarias e Departamentos Municipais, conforme segue:

Item	Qtde	Und	Descrição	Valor Unit	Valor Total

CLÁUSULA SEGUNDA - VALOR

I - O valor certo e ajustado para a contratação do objeto do presente contrato é de..... R$

***CLÁUSULA TERCEIRA* - DESCRIÇÃO DOS EQUIPAMENTOS E DOS SERVIÇOS:**

I - LOTE 01: A locação da solução integrada de **Firewall *Next Generation*** é composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) entendendo-se como tais o conjunto de serviços e recursos de:

A - Filtro de pacotes com controle de estado.

B - Filtro de conteúdo web.

C - Interceptação SSL.

D - Filtro de aplicações.

E - Controle da web 2.0.

F - Inspeção com proteção contra ataques de Malwares, vírus, worm, e aplicativos maliciosos.

G- Integrar soluções do tipo (IPS, ATP, QoS, Balanceamento de serviços, Redundância de links, SD-WAN, VPN, DHCP e DNS). Com a capacidade de integrar todos os recursos em um único dispositivo.

H - Aquisição de solução para gerenciamento centralizado de Firewall.

I - Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 48 meses, onde deverá ser instalado localmente e permitir a atualização do software e do sistema operacional, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato.

J - Treinamento para a equipe do Departamento de Tecnologia de Informação da Prefeitura Municipal de Pato Branco.

K - Suporte técnico remoto (24x7).

II - LOTE 02: Serviços de E-mail (1):

A - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.
B - Possuir 600 contas de e-mail de 5 GB, totalizando 3TB, contendo antispam e antivírus.
1 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

C Serviços de E-mail (2):
1 - Serviço de E-mail Gerenciado com interface para o usuário (exemplo Cpanel entre outros) em cloud.
2 - Possuir 100 contas de e-mail de 30 GB, totalizando 3TB, contendo antispam, antivírus e backup ilimitado.
3 - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior.

III - LOTE 03: Instalação e Prestação de Serviços do Módulo de Acesso Remoto e de Controle:
A - Módulo de Acesso Remoto e de Controle para 750 máquinas
B - A solução deverá ser provida por computação em nuvem, fornecida como serviço (Software as a Service – SAAS). A infraestrutura deve ser disponibilizada em datacenter com certificação TIER II ou Superior
C - A solução deverá prover acesso diretamente por painel *web* ou via aplicação instalável
D - A ferramenta deverá permitir e gravar opcionalmente todo e qualquer acesso remoto e manter a gravação em extensões de vídeo como: .avi,mp4 por um período configurável.
E - A solução deverá permitir acesso remoto em primeiro e segundo plano, entende-se como acesso em segundo plano o acesso ao computador sem assumir o controle da área de trabalho do usuário.
F - O acesso em segundo plano deverá permitir acessar ao prompt de comando e executar comandos remotamente, deverá mostrar de forma intuitiva ao usuário informações sobre aplicações, serviços, programas e *drivers* instalados, bem como possibilitar pausar, iniciar ou reiniciar um serviço do *Windows.*
G - A solução de acesso remoto ao computador em primeiro plano deverá ao acessar a área do usuário, possibilitar o acesso a esta área, assim como permitir controlar, bloquear monitor e teclado, mouse.

H - AQUISIÇÃO E PRESTAÇÃO DE SERVIÇOS DO MÓDULO DE AUTOMAÇÃO
1 - Módulo de automação para 750 máquinas
2 - A ferramenta deverá ser integrada junto com a solução de acesso remoto.
3 - A ferramenta deverá conter funcionalidades para execuções de ações remotamente e agendáveis por dia, hora, semana, mês, execução imediata ou executar conforme certos critérios de configurações.
4 - Executar comando remoto via Prompt de Comando ou Powershell.
5 - Executar um arquivo em lote ou executável.
6 - Distribuir arquivos em todas as máquinas de forma automática.
7 - Atualizar registros do *Windows.*
8 - Instalar ou atualizar um software por .msi ou.exe.

IV - LOTE 04: Prestação de Serviços do Módulo Antivírus:
A - Modulo de Antivírus para 750 maquinas.
B - A Ferramenta deverá possuir dentro da mesma solução uma central para gestão dos antivírus onde seja possível executar remotamente para um ou vários computadores.
C - Executar varredura completa e atualizar definições de vírus.
D - Recuperar informações mais recentes do antivírus.
E - Ativar ou desativar proteção em tempo real.
F - Bloquear portas *usb* dos computadores ou ainda exigir varredura imediata quando o usuário conectar em alguma porta *usb* dos computadores.
G - A Contratada deverá entregar juntamente, o licenciamento de antivírus para 750 computadores compatíveis com os mais conhecidos no mercado, como por exemplo: Kaspersky, Bitdefender, avirá ou similares.

H - DA IMPLANTAÇÃO DOS SISTEMAS:

1 - Deverá contemplar a entrega técnica e o treinamento de uso da ferramenta em todos os módulos.

2 - A Contratada deverá orientar a equipe técnica da Contratante, de como proceder à instalação do agente e do antivírus.

3 - A Contratada deverá orientar a equipe técnica da Contratante, de como realizar o acesso remoto e o agendamento de tarefas.

4 - A Contratada deverá apresentar o escopo detalhado dos serviços contratados para equipe técnica da Contratante.

V - DAS ESPECIFICAÇÕES, CARACTERÍSTICAS E FUNCIONALIDADES TÉCNICAS PARA A SOLUÇÃO DE SEGURANÇA "FIREWALL UTM":

A - APPLIANCE UTM FIREWALL - Característica do Hardware:

1 - Deverá ser entregue 02 (dois) equipamentos idênticos, para atender a necessidade de equipamento Spare (BACKUP).

2 - O equipamento deverá ser instalado em rack, com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack.

3 - Dispor de fonte de alimentação redundante interna, com tensão de entrada de 110V / 220V AC, automática e frequência de 50-60 Hz, Hot swapping.

4 - Possuir painel/led indicador on/off, disco e devices de rede.

5 - Suportar no mínimo 30.000.000 (trinta milhões) de conexões simultâneas.

6 - Suportar no mínimo 250.000 (duzentos e cinquenta mil) novas conexões por segundo.

7 - Possuir throughput mínimo de 12 Gbps, para tráfego IPS/IDS.

8 - Possuir throughput mínimo de 13 Gbps, para tráfego VPN IPSEC, com criptografia (AES-128).

9 - Possuir throughput mínimo de 07 Gbps, para tráfego VPN SSL, com criptografia (AES-128).

10 - Possuir throughput mínimo de 12 Gbps/5.5 Gbps, para tráfego Proxy Web filter/SSL Inspection.

11 - Possuir throughput mínimo de 6.8 Gbps, para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo).

12 - Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000, com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch.

13 - Possuir dispositivo de armazenamento interno de no mínimo 240GB padrão SSD.

14 - Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento.

VI - ESPECIFICAÇÕES GERAIS DE SOFTWARE FIREWALL NEXT GENERATION – NGFW:

A - Funções Básicas:

1 - Hardware (Appliances) que atuam na segurança e performance do ambiente de rede.

2 - VPN SSL, VPN IPSec (Client-to-site e Site-to-site).

3 - Controle de Aplicações.

4 - Proxy Web e Filtro de Conteúdo Web (URL Filtering).

5 - Detecção e prevenção de intrusos – IPS.

6 - Qualidade de serviço – QOS.

7 - Anti-Malware.

8 - SD-WAN (*Software-Defined Wide Artea Network*).

9 - Cluster.

VII - DAS CARACTERÍSTICAS GERAIS:

A - O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de maior capacidade.

B - A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 07.

C - Interface em português ou inglês.

D - Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento.
E - O sistema deverá permitir o acesso à interface de gerenciamento WEB, por qualquer interface de rede configurada.
F - O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
G - Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
H - Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
I - Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas.
J - A Solução deverá prover inspeção SSL:
1 - A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho.
2 - Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo.
3 - Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.
4 - Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:
a) Endereço do servidor.
b) Porta do servidor.
c) Usuário.
d) Senha.
K - Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:
1 - Desempenho total (throughput).
2 - Conexões simultâneas.
3 - Usuários autenticados.
4 - Serviços habilitados ou desabilitados.
5 - Quantidade de endereços distribuídos pelo DHCP.
L - Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, mesmo antes do equipamento ser conectado à rede, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos.
M - A Solução deverá permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde ele será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com o sistema central e receba a configuração.
N - Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar o sistema central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento.
O - A solução ofertada deverá permitir a criação de perfis de proteção como: a não limitação a perfil de IPS, perfil de controle WEB/aplicações e perfil de SD-WAN e deverá ser possível utilizá-los nas políticas de segurança.
P - Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV.
Q - Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX).
R - A solução deverá possuir uma única janela para a criação, configuração e edição dos recursos de segurança.
S - Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única policy.

T - Deverá implementar o protocolo ECMP.
U - O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.
V - Deverá possuir suporte ao protocolo de encapsulamento de redes MPLS.
W - Esta condição deverá permitir conectar links MPLS, diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

VIII - Das Funcionalidades do Firewall:
A - Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas.
B - Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH.
C - Possibilitar a visualização dos países de origem e destino nos *logs* de eventos, de acessos e de ameaças.
D - Possuir mecanismo que permita a realização de cópias de segurança (*backups*) do sistema e restauração remota, através da interface gráfica, a solução deverá permitir o agendamento diário ou semanal.
E - O sistema deverá permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
F - As cópias de segurança deverão ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup.
G - O sistema ainda deverá contemplar um recurso de cópia de segurança do tipo *snapshot* (cópia instantânea), que contemple a cópia completa das configurações dos serviços e dos recursos do sistema.
H - Deverá possibilitar a restauração do *snapshot* através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema.
I - Deverá permitir habilitar ou desabilitar o registro de *log* por política de *firewall.*
J - Possuir controle de acesso à internet por endereço IP de origem e de destino.
K - Possuir controle de acesso à internet por sub-rede.
L - Possuir suporte a tags de VLAN (802.1q).
M - Suportar agregação de links, segundo padrão IEEE 802.3ad.
N - Possuir ferramenta de diagnóstico do tipo *tcpdump*.
O - Possuir integração com Servidores de Autenticação RADIUS (Remote Authentication Dial In User Service), TACACS+, LDAP e Microsoft Active Directory.
P - Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e SSH).
Q - Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
R - Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana.
S - Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br.
T - Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
U - Possuir funcionalidades de DHCP Cliente, Servidor e Relay.
V - Deverá suportar aplicações multimídia como: H.323, SIP.
W - Possuir tecnologia de firewall do tipo Stateful.
X - Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo.
Y - Permitir o funcionamento em modo transparente tipo “bridge”.
Z - Permitir a criação de pelo menos 20 VLANS (rede local virtual) no padrão IEEE 802.1q.
AA - Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando).
AB - Deverá suportar *forwarding* (encaminhamento) de multicast..2.3.29 Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP.
AC - Permitir o agrupamento de serviços.

AD - Permitir o filtro de pacotes sem a utilização de NAT.
AE - Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
AF - Possuir mecanismo de anti-spoofing.
AG - Permitir criação de regras definidas pelo usuário.
AH - Permitir o serviço de autenticação para HTTP e FTP.
AI - Possuir a funcionalidade de balanceamento e contingência de links.

IX - DA IDENTIFICAÇÃO DO USUÁRIO:
A - Deverá possuir a capacidade de criação de políticas de acesso de *firewall,* VPN, IPS e ao controle de aplicação integrada ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius.
B - Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
C - A solução deverá ser capaz de identificar nome do usuário, *login*, máquina/computador registrados no Microsoft Active Directory.
D - Na integração com o AD (Active Directory), todos os domain controllers em operação na rede do cliente deverão ser cadastrados de maneira simples e sem utilização de *scritps* de comando.
E - A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante.
F - A solução deverá suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o gateway (porta de entrada) tenha que fazer “queries” (consulta) no AD.
G - O UTM deverá permitir gerenciar múltiplas políticas de controles no serviço de autenticação. As políticas deverão permitir criar controles para autenticação e deverão permitir ou bloquear o acesso ao serviço de autenticação, baseado em condições e de sessão, ou seja, uma vez que o usuário esteja permitido se autenticar no serviço, a política deverá definir os parâmetros de sessão do usuário.
H - Para o sistema de controle no serviço de autenticação o produto deverá possuir no mínimo, as seguintes condições para o Controle de Autenticação:
1 - Usuários e Grupos de Usuários.
2 - Datas (Objetos de Datas).
3 - Horários (Objetos de Horário).
4 - Plataformas (Objetos de Dicionários).
5 - Endereços Remotos (Objetos de IPv4 e IPv6).
6 - Zona de Rede (Múltiplas Zonas).

X - DAS FUNCIONALIDADES DA REDE PRIVADA VIRTUAL VPN (VIRTUAL PRIVATE NETWORK):
A - Rede Privada Virtual - VPN baseada em appliance.
B - Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES.
C - Possuir suporte a VPNs IPSec site-to-site.
D - Criptografia, 3DES, AES128, AES256, AES-GCM-128, Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC.
E - Algoritmo Internet Key Exchange (IKE) versões I e II.
F - AES 128 e 256 (Advanced Encryption Standard).
G - Suporte a Diffie-Hellman (troca de chaves de maneira segura) Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30.
H - Possuir suporte a VPN SSL.
I - Possuir capacidade de realizar SSL VPNs utilizando certificados digitais.
J - Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:
1 - Remote Desktop Protocol.
2 - Virtual Network Computing.
3 - SSH - Secure Shell.
4 - WEB - World Wide Web.

5 - SMB - Server Message Block.
6 - Deverá permitir a arquitetura de vpn hub and spoke.
7 - Suporte a VPNs IPSec client-to-site.
8 - Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
9 - Suporte à inclusão em autoridades certificadoras (enrollment = inscrição) mediante SCEP (Simple Certificate Enrollment Protocol).
10 - Possuir funcionalidades de Auto-Dicovery VPN, capaz de permitir criar túneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).
11 - A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de túneis:
a) Site-to-Site.
b) Full-Mesh.
c) Star.

XI - DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO: A DETECÇÃO DE INTRUSÃO DEVERÁ SER BASEADA EM *APPLIANCE*:
1 - Possuir no mínimo 25.000 (vinte e cinco mil) assinaturas ou regras de IPS/IDS.
2 - O sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes.
3 - Possuir tecnologia de detecção baseada em assinatura.
4 - Deverá suportar a implantação em modo Gateway, *online* e em modo sniffer (farejador).
5 - Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass.
6 - O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança.
7 - Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.
8 - Possuir capacidade de remontagem de pacotes para identificação de ataques.
9 - Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de servidores web.
10 - Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
11 - Mecanismos de detecção/proteção de ataques.
12 - Reconhecimento de padrões.
13 - Análise de protocolos.
14 - Detecção de anomalias.
15 - Detecção de ataques de RPC (Remote Procedure Call).
16 - Proteção contra ataques de Windows ou NetBios.
17 - Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol).
18 - Proteção contra ataques DNS (Domain Name System).
19 - Proteção contra ataques a FTP, SSH, Telnet e rlogin (logins remotos).
20 - Proteção contra ataques de ICMP (Internet Control Message Protocol).
21 - Alarmes na console de administração.
22 - Alertas via correio eletrônico.
23 - Monitoração do comportamento do appliance através de SNMP - Simple Network Management Protocol, o dispositivo deverá ser capaz de enviar traps (armadilhas) de SNMP, quando ocorrer um evento relevante para a correta operação da rede.
24 - Capacidade de resposta/logs ativa a ataques.
25 - Terminação de sessões via TCP resets.
26 - Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos.
27 - O sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços.
28 - Possuir filtros de ataques por anomalias.
29 - Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit.

30 - Permitir filtros de anomalias de protocolos.
31 - Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.
32 - Suportar verificação de ataque nas camadas de aplicação.

XII - DAS FUNCIONALIDADES DO QOS - QUALITY OF SERVICE OU QUALIDADE DE SERVIÇO:
A - Adotar solução de Qualidade de Serviço baseada em appliance.
B - Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
C - Permitir modificação de valores DSCP.
D - Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
E - Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
F - Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
G - Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino.
H - Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

XIII - DAS FUNCIONALIDADES DO ATP - ADVANCED THREAT PREVENTION (PREVENÇÃO AVANÇADA CONTRA AMEAÇAS):
A - Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP.
B - Permitir o bloqueio de malwares (adware (tipo anúncios, propagandas), spyware (tipo espião), hijackers (tipo cavalo de tróia), keyloggers, etc.).
C - Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo.
D - Permitir o bloqueio de download de arquivos por tamanho.

XIV - Das Funcionalidades do Proxy e do Filtro de Conteúdo Web:
A - Possuir solução de filtro de conteúdo web integrado a solução de segurança.
B - Possuir pelo menos 80 categorias para classificação de sites web.
C - Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
1 - Webmail.
2 - Instituições de Saúde.
3 - Notícias.
4 - Pornografia.
5 - Restaurante.
6 - Mídias Sociais.
7 - Esporte.
8 - Educação.
9 - Games.
10 - Compras.
D - Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
E - Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória.
F - Deverá permitir a definição do tamanho mínimo dos objetos salvos em cache no disco.
G - Deverá permitir a definição do tamanho máximo dos objetos salvos em cache em memória.
H - Deverá atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação.
I - Possibilitar a integração com servidores de cache WEB externos.
J - Deverá possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares.

K - Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
L - Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
M - Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante.
N - Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX, através de: base de URL própria atualizável.
O - Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual.
P - Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra.
Q - Deverá permitir o bloqueio de URLs inválidas, cujo campo CN, do certificado SSL, não contém um domínio válido.
R - Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web.
S - Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
T - Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
U - Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem.
V - Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP.
W - Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Áudio, Vídeo e URLs originadas de Spam.
X - Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueada – lista negra.
Y - Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente.
Z - Deverá permitir configurar a porta do Proxy Explícito.

XV - DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES: AS FUNCIONALIDADES ABAIXO DEVEM SER BASEADAS EM *APPLIANCE*:
A - Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
1 - P2P.
2 - Web.
3 - Transferência de arquivos.
4 - Chat.
5 - Social.
B - Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
C - Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
D - Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
E - Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
F - Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
G - Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
H - Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino.
I - Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

XVI - DAS FUNCIONALIDADES DO SD-WAN - (SOFTWARE-DEFINED WAN):

A - Entende-se como tecnologia SD-WAN (Software-Defined WAN), a rede de área ampla definida por software que centraliza a gerência da rede WAN, em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN, para comunicação entre os sites remotos.
B - Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas.
C - Permitir utilizar VPN IPsec para interligar unidades remotas.
D - Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link.
E - O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes e latência.
F - Deverá possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN.
G - O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação.
H - O appliance SD-WAN deverá permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado veja avaliado. Deverá suportar especificar um valor variando de 01 a 100.
I - O recurso de SD-WAN deverá permitir o monitoramento de no mínimo 03 (três) endereços alvos, para verificar a disponibilidade e desempenho do link.
J - A solução de SD-WAN UTM, deverá permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN, de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras.
K - Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:
1 - Consumo de banda.
2 - Perda de pacotes.
3 - Jitter.
4 - Latência.

XVII - DA ALTA DISPONIBILIDADE:
A - Possuir mecanismo de alta disponibilidade operando em modo Ativo/Standby, com as implementações de Failover (tolerância as falhas).
B - Não serão permitidas soluções de cluster (HA), que façam com que o equipamento reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
C - O sincronismo dos servidores deverá ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

XVIII - DAS SOLUÇÕES DE GERENCIAMENTO CENTRALIZADO DE FIREWALL:
A - Funcionalidades de Gerenciamento:
1 - Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto.
2 - A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewalls contratados.
3 - gerenciamento centralizado poderá ser entregue como *appliance* físico ou virtual. Caso seja entregue em *appliance* fisíco deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em *appliance* virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o *appliance* virtual é responsabilidade da Contratante.
4 - Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento.
5 - A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica.

6 - Deverá manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de *logs* e emissão de relatórios.
7 - A solução deverá incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador.
8 - A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.
9 - Deverá possibilitar a realização de "backup" e restauração de dados.
10 - Deverá possibilitar o envio dos *"logs"* gerados a outro concentrador de *"logs"* externo a solução.
11 - Deverá possibilitar a gerência de *"logs",* realizando as configurações de relatórios de todos os "firewalls" integrados.
12 - Deverá permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.
13 - gerenciamento deverá permitir/possuir:
a) Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas.
b) Monitoração de *logs*.
c) Debugging (depuração).
d) Acesso concorrente de administradores.
e) Deverá permitir usar palavras chaves para facilitar identificação de regras.
f) Definição de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
g) Autenticação integrada à base de dados local.
h) Deverá possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, sub rede) na base de regras.
i) Criação de regras que fiquem ativas em horário definido.
j) Backup das configurações e rollback de configuração para a última configuração salva.
k) Habilidade de upgrade via interface de gerenciamento.
l) Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado.
m) Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções.
n) Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção.
o) Deverá permitir a criação de objetos e políticas compartilhadas.
p) Capacidade de definir administradores com diferentes perfis de acesso com no mínimo, as permissões de Leitura/Escrita e somente Leitura.
q) Solução deverá ser capaz de detectar ataques de tentativa de *login* e senha utilizando tipos diferentes de credencias.
r) sistema deverá ser capaz de gerenciar de modo central as políticas de backup dos equipamentos remotos.
s) sistema deverá permitir habilitar uma mensagem de disclaimer (isenção de responsabilidade) na página de *login* da Interface de Administração. Ou seja, a página de *login* deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.
t) Deverá suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada.
u) Deverá suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider).

XIX - DAS FUNCIONALIDADES DE ANÁLISE DE LOG:

A - Deverá prover análise de tráfego de rede de modo centralizado.

B - Deverá possuir análise de tráfego de rede e ameaças por geolocalização.

C - Deverá ser capaz de receber os *logs* e eventos com o objetivo de prover os seguintes tipos de análises:

1 - Análise de ameaças e incidentes de segurança.

2 - Análise de tráfego e uso de categorias Web.

3 - Análise de tráfego e uso de aplicativos.

4 - Análise de tráfego e ameaças por usuário.

5 - Análise de desempenho de políticas de segurança.

6 - A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de *logs*, consolidação de *logs*, arquivamento de *logs*, busca avançada de *logs.*

7 - Deverá possuir ferramenta para salvar consultas avançadas.

8 - Deverá possuir relatórios personalizados.

9 - Deverá ser capaz de efetuar o arquivamento de relatórios.

10 - Deverá possuir agendamento de relatórios.

11 - Os relatórios deverão no mínimo, serem exportados em formatos flexíveis (PDF, CSV).

***CLÁUSULA QUARTA* - CONDIÇÕES DE EXECUÇÃO E PRAZOS**

I - Os serviços deverão ser executados mediante solicitação formal da contratante, por meio de Nota de Empenho, na sede da Prefeitura Municipal, localizada na Rua Caramuru, 271, Centro, Pato Branco - PR.

II - O recebimento do objeto se dará conforme o disposto no artigo 73, inciso I alíneas “a” e “b” e art. 76 da Lei n.º 8.666/93, e compreenderá duas etapas distintas, a seguir discriminadas:

a) Recebimento Provisório: Deverá começar no início da prestação de serviços (instalação) e consistirá na mera verificação da conformidade com as especificações técnicas. Deverá ser finalizado em **até 24 (vinte e quatro) horas** após a conclusão do serviço.

b) Recebimento Definitivo: Ocorrerá em até **48 (quarenta e oito) horas**, após o Recebimento Provisório, pela Comissão de Avaliação Técnica e constará de:

III - Verificação da conformidade com as especificações técnicas exigidas em cada etapa e se estas atendem plenamente aos requisitos de forma aderente aos termos contratuais.

IV - O recebimento definitivo dar-se-á mediante termo circunstanciado de Recebimento Definitivo e posterior certificação na Nota Fiscal, autorizando assim o pagamento.

V - Constatada(s) irregularidade(s) nos serviços contratados, a Administração Municipal poderá rejeitá-los no todo ou em parte, determinando o seu ajuste, às suas expensas, em um prazo que **deverá se iniciar no máximo em até 02 (dois) dias**, contados da assinatura do recebimento da notificação formal, pela Contratada, observando o disposto no art. 69, da Lei 8.666/93 e deverá ser concluído **em até 05(cinco) dias.**

VI - Os serviços serão considerados aceitos somente após emissão do termo circunstanciado de Recebimento Definitivo devidamente documentado e assinado pelo gestor e/ou fiscal do Contrato de Prestação de Serviços.

VII - Na hipótese de verificação a que se refere o recebimento definitivo, não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

VIII - A fiscalização por parte do município e o recebimento provisório ou definitivo não excluem a responsabilidade civil da Contratada pela correção e/ou substituição do objeto contratual, bem como pelos danos e prejuízos ao município ou a terceiros, decorrentes da má execução/desconformidades com as normas técnicas exigíveis, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

IX - Prazo de Execução: O prazo de execução será de até 15 (quinze) dias, contados a partir do Recebimento da Nota de Empenho.

X - Prazo de Vigência: O prazo de vigência será de 12 (doze) meses, contados a partir da assinatura do Contrato de Prestação de Serviços, podendo ser prorrogado conforme legislação vigente e de acordo entre as partes, conforme contempla o Artigo 57, da Lei nº 8.666/93, mediante Termo de Aditamento.

VIII. PRESTAÇÃO DE SERVIÇO DE INSTALAÇÃO

a) - Para as soluções ofertadas, a Contratada deverá cotar um valor total para a instalação, configuração e treinamento para os dispositivos adquiridos.

b) - Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, funcionalidades e políticas.

c) - A instalação deverá ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante.

d) - Deverá ser realizada a configuração das regras de entrada, saída.

e) - Configuração do Active Directory.

IX. TREINAMENTO PARA O SISTEMA FIREWALL UTM:

a) - Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware e software) para a equipe do setor de tecnologia da informação (T.I) da Contratante.

b) - Este treinamento deverá possuir carga horária mínima de 08 horas.

c) - O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação.

d) - O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas.

e) - O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta.

f) - Deverá ser incluso, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada.

g) - Os cursos deverão ser realizados em horários e data a serem acordados pela Contratada e pela Contratante.

X. PRESTAÇÃO DE SERVIÇOS DE SUPORTE TÉCNICO E REMOTO:

a) - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis 24 x 07 x 365 (vinte e quatro horas por dia sete dias por semana e trezentos e sessenta e cinco dias no ano), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR), com as seguintes características:

i) - A Contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede, relativos aos equipamentos e/ou produtos fornecidos.

ii) Os chamados para o suporte técnico serão classificados por severidade, conforme impacto no ambiente computacional do município:

a) - Severidade 01: Sistema crítico, em produção, está parado ou fora de funcionamento, não há meios de contornar a não conformidade. Número significativo de usuários afetados, impacto operacional significativo causado.

b) - Severidade 02: Sistema crítico, em produção, está apresentando falhas de funcionamento, não causou interrupção do serviço, no entanto, afeta significativamente o desempenho, com impacto crítico aos usuários.

c) - Severidade 03: Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impacto moderado aos usuários. Impacto operacional moderado.

d) - Severidade 04: Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features ou melhorias. Impacto mínimo aos usuários. Sem impacto operacional.

iii) - Para mensurar o nível de criticidade da não conformidade, serão utilizados os indicadores de severidade. Os chamados, conforme o nível de severidade, definidos pelos técnicos da contratante, terão

prazo para resolução, contados a partir do momento do registro da solicitação em service desk de comunicação com a contratada. Segue o aprazamento para resolução de não conformidade:

Descrição do Nível de Criticidade	Tempo Máximo para Resolução
Severidade 1	01 hora corrida
Severidade 2	04 horas corridas
Severidade 3	16 horas úteis
Severidade 4	24 horas úteis

b) - Sendo entendido que:
i) – Hora corrida é a compreendida entre o período de 0h00min as 24h00min, 07 (dias por semana). Hora útil é a compreendida entre o período de 08h00min às 18h00min, de segunda a sexta-feira, excetuando-se feriados nacionais.
ii) - Será admitida solução de contorno (redução ou eliminação do impacto de um incidente ou problema para o qual uma solução completa ainda não está disponível), na resolução de chamados de severidade 01 e 02, para fins de atendimento dos prazos estipulados.
iii) - Considera-se não conformidade plenamente solucionada quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva.
iv) - A Contratada não será responsabilizada por descumprimento de prazo para resolução de não conformidade, quando a demanda for originada por falha, interrupção, inconsistência de dados e informações gerados pela Contratante ou terceiros da Contratante. Nestas ocorrências, a Contratada deverá emitir parecer comprovando que a não conformidade não se originou no cumprimento do objeto contratado.
v) - Toda intervenção no ambiente produtivo da Contratante, que resulte na necessidade de suporte técnico pela Contratada, deverá ser executada somente após autorização do Setor de Tecnologia de Informação (TI), a partir de informações claras sobre o impacto da ação nos procedimentos que serão adotados.
vi) - Na finalização do chamado, o técnico responsável pela Contratada realizará, em conjunto com representantes técnicos da Contratante, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema. O tempo utilizado nos testes não será computado no aprazamento de resolução da não conformidade.
vii) - Ao término dos testes e do atendimento (fechamento do chamado), a Contratada deverá formalizar a Contratante, de forma detalhada, as causas da não conformidade e solução definitiva adotada.
viii) - Nos casos em que o atendimento não se mostrar satisfatório, a Contratante fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

CLÁUSULA QUINTA - CONDIÇÕES DE PAGAMENTO

I - Para a Instalação (Lote 03, item 01): O pagamento será realizado até o 15º (décimo quinto) dia útil, após a instalação do objeto e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços.

II - Para Manutenção (demais itens): O pagamento será realizado mensalmente até o 15º (décimo quinto) dia útil, do mês subsequente a execução dos serviços e mediante emissão do Termo de Recebimento Definitivo, apresentação da respectiva nota fiscal/fatura atestada pelo Gestor, Fiscal do Contrato de Prestação de Serviços e pela Comissão de Recebimento de Bens e Serviços.

Lote	Item	Valor Mensal	Valor Total 12 meses	Valor da Parcela Única
1	1	R$ 39.269,94	R$ 471.239,28	
1	2	R$ 3.466,67	R$ 41.600,04	
2	1	R$ 3.183,33	R$ 38.199,96	
3	1	--	--	R$ 5.600,00

3	2	R$ 1.252,80	R$ 15.033,60	
3	3	R$ 907,65	R$ 10.891,80	
4	1	R$ 907,40	R$ 10.888,80	

16 Tabela 01 – Parcelas de cada item

III - O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.
IV - A nota fiscal/fatura deverá conter discriminação resumida do item contratado, número da licitação, número do Contrato de Prestação de serviços, não apresentar rasura e/ou entrelinhas, deverão ser impressas de maneira clara, inteligível, inviolável, ordenada e dentro de padrão uniforme.
V - Para fazer jus ao pagamento, a empresa deverá apresentar, prova de regularidade para com a Fazenda Federal, Estadual e Municipal, prova de regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS) e Certidão Negativa de Débitos Trabalhistas (CNDT) emitida eletronicamente através do site http://www.tst.jus.br, em cumprimento com as obrigações assumidas na fase de habilitação do processo licitatório.
VI - O cadastro no SICAF vigente, ou Certificado de Registro Cadastral (CRC) emitido pela Divisão de Licitações do Município de Pato Branco (desde que válidos), poderão substituir os documentos indicados no subitem V.
VII - O pagamento poderá ser realizado preferencialmente por meio de ordem bancária, creditada na conta corrente da Contratada, ou por meio de fatura com utilização do código de barras.
VIII - Os pagamentos correrão por conta dos recursos das Dotações Orçamentárias (Despesas e Desdobramentos respectivamente) conforme planilha em anexo.
IX - Em caso de atraso de pagamento motivado exclusivamente pela contratante, como critério para correção monetária aplicar-se-á o IPCA - Índice Nacional de Preços ao Consumidor Amplo calculado pelo IBGE. Em caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante juros moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples. Quando da incidência da correção monetária e juros moratórios, os valores serão computados a partir do vencimento do prazo de pagamento de cada parcela devida.

CLÁUSULA SEXTA - DOTAÇÃO ORÇAMENTÁRIA

I - As despesas decorrentes desta licitação ocorrerão por conta do recurso da Dotação Orçamentária:
a) 04 SEC.MUN.DE PLANEJAMENTO URBANO - 04.02 DEPARTAMENTO DE DESENVOLVIMENTO URBANO - 1545100182238000 Manutencao do Departamento de Planejamento Urbano - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2238 – Despesa 101 – Desdobramentos (9857-9873).
b) 05 SEC.MUN.DE ADMINISTRAÇÃO E FINANÇAS - 05.02 DEPARTAMENTO ADMINISTRATIVO - 0412200072216000 Manutencao das atividades do Departamento Administrativo - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 510 Recursos Ordinarios (Livres) – Ação 2216 – Despesa 184 – Desdobramentos (2015-3251).
c) 06 SEC.MUN.DE ENGENHARIA E OBRAS E SERVIÇOS PÚBLICOS - 06.02 DEPARTAMENTO DE ENGENHARIA - 1545200192021000 Manutencao das atividades do Departamento DE Engenharia e Obras - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2021 – Despesa 414 – Desdobramentos (2021-3460).
d) 07 SEC.MUN.DE EDUCAÇÃO E CULTURA - 07.02 DEPARTAMENTO ADMINISTRATIVO - 1236500392095000 Manutencao dos Centros de Educação Infantil - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 103 Recursos Ordinarios (Livres) – Ação 2095 – Despesa 1726 – Desdobramentos (9357-9875).
e) 08 SEC.MUN.DE DE SAÚDE - 08.02 ADMINISTRAÇÃO DA SAUDE - 1030100432388000 Manutencao das atividades da Saude - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 303 Recursos Ordinarios (Livres) – Ação 2388– Despesa 1652 – Desdobramentos (2407-3416).

f) 09 SEC.MUN.DE ASSISTÊNCIA SOCIAL – 09.04 FUNDO MUNICIPAL DE ASSISTÊNCIA SOCIAL - 0824400242202000 Manutencao das atividades da Gestão de Assistência Social - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2202 – Despesa 751 – Desdobramentos (9884-9876).
g) 10 SEC.MUN.DE DESENVOLVIMENTO ECONÔMICO - 10.02 DEPARTAMENTO DE DESENVOLVIMENTO ECONÔMICO - 2369100272029000 Manter Aeroporto - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2029 – Despesa 891 – Desdobramentos (9862-9877).
h) 10 SEC.MUN.DE DESENVOLVIMENTO ECONÔMICO - 10.02 DEPARTAMENTO DE DESENVOLVIMENTO ECONÔMICO – 2369500282062000 Fomento ao Turismo - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2062 – Despesa 907 – Desdobramentos (9863-9878).
i) 11 SEC.MUN.DE AGRICULTURA - 11.02 DEPARTAMENTO DE AGRICULTURA – 2060600292070000 Manutenção das atividades de Desenvolvimento Rural - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2070 – Despesa 957– Desdobramentos (9864-9879).
j) 11 SEC.MUN.DE AGRICULTURA - 11.02 DEPARTAMENTO DE AGRICULTURA – 2060600292073000 Manutenção das atividades do Interior - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2073 – Despesa 978– Desdobramentos (9865-9880).
k) 16 SEC.MUN.DE ESPORTE E LAZER - 16.02 DEPARTAMENTO DE ESPORTE E LAZER – 2781200412224000 Manutenção das atividades do Dpto de Esporte e Lazer - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2224 – Despesa 1194 – Desdobramentos (9866-9881).
l) 17 SEC.MUN.DE CIÊNCIA E TECNOLOGIA - 17.02 DEPARTAMENTO DO PARQUE TECNOLÓGICO - 1957300252241000 Manutenção das atividades Do Departamento Administração e Financeiro - 3.3.90.40.00.00.00 SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - PESSOA JU - Fonte....: 0 Recursos Ordinarios (Livres) – Ação 2241 – Despesa 1243 – Desdobramentos (9279-9882).

CLÁUSULA SÉTIMA - OBRIGAÇÕES DA CONTRATADA

I - Manter todas as condições de habilitação, qualificação e as obrigações exigidas durante toda a vigência Contratual, de acordo com o art. 55, XIII, da Lei 8.666/93, informando a Contratante à ocorrência de qualquer alteração nas referidas condições.
II - Prestar os serviços contratados, em estrita conformidade com as especificações contidas no contrato e na proposta de preços apresentada, aos quais se vincula, não sendo admitidas retificações, cancelamentos, quer seja de preços, quer seja nas condições estabelecidas.
III - Comunicar imediatamente a Contratante, no caso de ocorrência de qualquer fato que possa implicar no atraso dos serviços contratados e a qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias.
IV - Executar os serviços com pontualidade, atendendo a todas as condições estabelecidas:
V - Os equipamentos contemplados no lote 01 deverão ser novos em número de 02 (dois), serão de propriedade da Contratada e serão disponibilizados durante todo o prazo contratual para o uso da Contratante, em forma de comodato.
VI - Todos os equipamentos cedidos em comodato (lote 01) para a execução do serviço deverão ser de boa qualidade e desempenho e caso seja necessário, deverá possuir certificação do órgão responsável e/ou garantia do fabricante.
VII - A Contratada deverá realizar a instalação dos produtos contratados, bem como apresentar carta do fabricante quanto ao fornecimento, garantia e funcionalidade dos produtos ofertados.
VIII - A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante.
IX - Os serviços de manutenção (preventiva, corretiva e/ou evolutiva) deverão ser realizados por profissionais qualificados, de forma que consigam executar os serviços com perfeição e rapidez e possam prestar qualquer informação técnica solicitada a respeito do sistema. Nos casos de manutenção

preventiva deverá ser feita a verificação de todo o objeto, a fim de detectar inconformidades capazes de prejudicar o funcionamento do sistema.

X - Toda e qualquer substituição e/ou manutenção corretiva dos equipamentos correrão por conta e as expensas da Contratada e não serão em nenhuma hipótese de responsabilidade da Contratante.

XI - Em caso de falha verificada por parte da Contratante, a mesma através do gestor do contrato ou pessoa designada por ele, solicitará visita técnica à Contratada, para o envio de profissional qualificado e devidamente identificado.

XII - Responder por danos e desaparecimentos de bens materiais e avarias que venham a ser causadas por seus empregados ou preposto à Contratante ou a terceiros, desde que fique comprovada sua culpa ou dolo, não excluindo ou reduzindo sua responsabilidade a fiscalização ou o acompanhamento realizado pela Contratante, de acordo com o art. 70 da Lei n.º 8.666/93.

XIII - Observar rigorosamente as normas técnicas, regulamentadoras, de segurança, de higiene, ambientais e medicina do trabalho. Além disso, deverão obedecer às normas técnicas de proteção ao meio ambiente e adotar boas práticas de otimização de recursos, redução de desperdícios, menor poluição, conforme legislação vigente**.**

XIV - A Contratada deverá garantir a qualidade dos serviços prestados e materiais empregados, devendo reparar, corrigir, remover, substituir às suas expensas, no total ou em parte, os materiais e/ou serviços prestados que se verificarem vícios, defeitos, incorreções ou má qualidade no serviço realizado.

XV - Constatada(s) irregularidade(s) nos serviços contratados, a Administração Municipal poderá rejeitá-los no todo ou em parte, determinando o seu ajuste, às suas expensas (caso não se enquadre serviços de atendimento e suporte técnico, subitem XXIII), em um prazo que **deverá se iniciar no máximo em até 02 (dois) dias**, contados da assinatura do recebimento da notificação formal, pela Contratada, observando o disposto no art. 69, da Lei 8.666/93 e deverá ser concluído **em até 05 (cinco) dias**.

XVI - É de responsabilidade da Contratada, selecionar e contratar pessoal devidamente habilitado para a função a ser exercida na execução dos serviços, em seu nome, observando rigorosamente todas as prescrições relativas às leis trabalhistas, previdenciárias, assistenciais, securitárias e sindicais, indenizações e despesas por acidentes de trabalho que eventualmente ocorram durante a prestação de serviço, sendo considerada como única empregadora.

XVII - Responsabiliza-se perante o Município, por todos os atos de seus subordinados durante a execução dos serviços, devendo afastar, dentro de 24 (vinte e quatro) horas, por comunicação escrita, qualquer de seus empregados cuja permanência nos serviços for julgada, inconveniente. Os empregados eventualmente afastados deverão ser substituídos por outros de categoria profissional idêntica.

XVIII - Manter atualizada a relação de funcionários que poderão atuar junto a Contratante, na execução do contrato. Em caso de desligamento, a Contratada deverá imediatamente, retirar todas as credenciais que permitam ao(s) funcionário(s), qualquer acesso ao serviço provido, bem como, deverá informar o fato ao gestor e/ou fiscal do contrato.

XIX - Manter por si, por seus prepostos e contratados, irrestrito e total sigilo sobre quaisquer dados confidenciais da Contratante a que tiver acesso, inerentes do objeto da licitação, respondendo contratual e legalmente pela inobservância desta alínea, inclusive após o término do contrato.

XX - A expressão “informação irrestrito e total sigilo” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível.

XXI - Guardar todas as informações confidenciais em local seguro, de forma que estejam adequadamente protegidas contra roubo, dano, perda ou acesso não autorizado, de acordo com padrões que sejam, no mínimo, equivalentes àqueles aplicados às informações confidenciais da Contratada.

XXII - Não utilizar nome/marca ou qualquer material desenvolvido pela Contratante, assim como os dados dos funcionários a que tenha acesso no decorrer das atividades inerentes a este Contrato de Prestação de Serviços, em ações desenvolvidas pela Contratada fora do âmbito de atuação deste processo de licitação.

XXIII - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis 24 x 07 x 365 (vinte e quatro horas por dia sete dias por semana e trezentos e sessenta e cinco dias no ano), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR), com as seguintes características:

A) A Contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede, relativos aos equipamentos e/ou produtos fornecidos

B) Os chamados para o suporte técnico serão classificados por severidade, conforme impacto no ambiente computacional do município:

1) -Severidade 01: Sistema crítico, em produção, está parado ou fora de funcionamento, não há meios de contornar a não conformidade. Número significativo de usuários afetados, impacto operacional significativo causado.

2) -**Severidade 02**: Sistema crítico, em produção, está apresentando falhas de funcionamento, não causou interrupção do serviço, no entanto, afeta significativamente o desempenho, com impacto crítico aos usuários.

3) - **Severidade 03**: Sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impacto moderado aos usuários. Impacto operacional moderado.

4) - **Severidade 04:** Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features[4] ou melhorias. Impacto mínimo aos usuários. Sem impacto operacional.

XXIV – Para mensurar o nível de criticidade da não conformidade, serão utilizados os indicadores de severidade. Os chamados, conforme o nível de severidade, definidos pelos técnicos da contratante, terão prazo para resolução, contados a partir do momento do registro da solicitação em service desk[5] de comunicação com a contratada. Segue o aprazamento para resolução de não conformidade:

Descrição do Nível de Criticidade	Tempo Máximo para Resolução
Severidade 1	01 hora corrida
Severidade 2	04 horas corridas
Severidade 3	16 horas úteis
Severidade 4	24 horas úteis

A) - Sendo entendido que:

1 - Hora corrida é a compreendida entre o período de 0h00min as 24h00min, 07 (dias por semana). Hora útil é a compreendida entre o período de 08h00min às 18h00min, de segunda a sexta-feira, excetuando-se feriados nacionais

2 - Será admitida solução de contorno (redução ou eliminação do impacto de um incidente ou problema para o qual uma solução completa ainda não está disponível), na resolução de chamados de severidade 01 e 02, para fins de atendimento dos prazos estipulados

3 - Considera-se não conformidade plenamente solucionada quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva

4 - A Contratada não será responsabilizada por descumprimento de prazo para resolução de não conformidade, quando a demanda for originada por falha, interrupção, inconsistência de dados e informações gerados pela Contratante ou terceiros da Contratante. Nestas ocorrências, a Contratada deverá emitir parecer comprovando que a não conformidade não se originou no cumprimento do objeto contratado

5 - Toda intervenção no ambiente produtivo da Contratante, que resulte na necessidade de suporte técnico pela Contratada, deverá ser executada somente após autorização do Setor de Tecnologia de Informação (TI), a partir de informações claras sobre o impacto da ação nos procedimentos que serão adotados

6 - Na finalização do chamado, o técnico da Contratada realizará, em conjunto com representantes técnicos da Contratante, testes para verificação dos resultados obtidos, certificando-se do

[4] Features são funcionalidades ou recursos desenvolvidos por um time de pessoas, geralmente de produtos e plataformas digitais que tem como propósito adicionar uma nova entrega de valor e experiência para seus usuários.

[5] O Service Desk é um conceito que tem como objetivo centralizar e unir todas as necessidades de uma empresa em um único lugar, gerindo todo o apoio operacional aos usuários de um sistema e registrando todas interações como forma de controle e monitoramento da organização.

restabelecimento à normalidade e/ou resolução do problema. O tempo utilizado nos testes não será computado no aprazamento de resolução da não conformidade

7 - Ao término dos testes e do atendimento (fechamento do chamado), a Contratada deverá formalizar a Contratante, de forma detalhada, as causas da não conformidade e solução definitiva adotada

8 - Nos casos em que o atendimento não se mostrar satisfatório, a Contratante fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado

9 - Garantir os serviços de atendimento e suporte técnico, pelo período de validade do Contrato de Prestação de Serviços, disponíveis em horário comercial, de segunda a sexta-feira das 08h00min às 17h30min, (exceto feriados), presencial e/ou através de telefone ou via web. Atendimento em língua portuguesa (BR).

XXV – A Contratada deverá possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativas aos equipamentos e/ou produtos fornecidos

XXVI - A Contratada deverá iniciar o atendimento de suporte técnico em até 08 horas úteis, após a abertura do chamado

XXVII - Disponibilizar instrutores para o(s) treinamento(s) de utilização dos softwares em local definido em conjunto com o fiscal e/ou gestor do contrato

XXVIII - Disponibilizar (caso haja a necessidade), de treinamento(s) adicional (is), o(s) qual (is), deverá(ão) ser(em) aplicado(s), para os servidores municipais diretamente ligados a área de tecnologia de informação do município e, em conjunto com o fiscal e/ou gestor do contrato.

XXIX - Apresentar os seus empregados devidamente uniformizados e identificados por meio de crachá, além de fornecer a todos os seus funcionários e preposto(s) o tipo adequado de equipamento de proteção individual – EPI, bem como fiscalizar o uso dos mesmos. A Contratada, em qualquer hipótese, não se eximirá da total responsabilidade quanto à negligência ou descumprimento da Lei nº 6.514 de 22/12/77 – Portaria nº 3.214, de 08/06/78 - Normas Regulamentadoras

XXX - Não manter em seu quadro de pessoal, menores de idade, em horário noturno de trabalho ou em serviços perigosos ou insalubres, não manter, ainda, em qualquer trabalho, menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos

XXXI Todas as decisões e entendimentos havidos entre as partes durante o andamento dos trabalhos e que impliquem em modificações ou implementações nos planos, cronogramas ou atividades pactuadas, deverão ser prévia e formalmente acordados e documentadas entre as partes

XXXII Nos preços cotados deverão estar inclusos todos os equipamentos, insumos e demais custos que compõem a demanda, bem como as despesas com impostos, tributos, taxas, fretes, seguros e quaisquer outros que incidam direta ou indiretamente execução dos serviços, como por exemplo: transporte, carga e descarga, deslocamento, hospedagens, alimentação e outros eventuais custos envolvidos

XXXIII Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que se está obrigada

XXXIV Todos os casos atípicos não mencionados neste Edital deverão ser apresentados à fiscalização para sua definição e determinação

XXXVI Cumprir com outras obrigações decorrentes da aplicação do Código de Proteção e Defesa do Consumidor - conforme Lei nº 8.078/90, que sejam compatíveis com o regime de direito público.

XXXVII Para os Lotes 02 e 03: Apresentar certificação Data Center TIER 3, conforme preconiza a norma TIA 942, para o gestor e/ou fiscal do contrato em até 72 (setenta e duas) horas, contados a partir do Recebimento da Nota de Empenho.

CLÁUSULA OITAVA - DAS OBRIGAÇÕES DA CONTRATADA RELATIVAS A CRITÉRIOS DE SUSTENTABILIDADE

I - As boas práticas de otimização de recursos, redução de desperdícios e menor poluição se pautam em alguns pressupostos e exigências, que deverão ser observados pela Contratada, que deverá fazer uso racional do consumo de energia e água, adotando medidas para evitar o desperdício.

II - Colaborar com as medidas de redução de consumo e uso racional da água, cujo(s) encarregado(s) deve(m) atuar como facilitador (es) das mudanças de comportamento.

III - Dar preferência à aquisição e uso de equipamentos e complementos que promovam a redução do consumo de água e que apresentem eficiência energética e redução de consumo.
IV - Evitar ao máximo o uso de extensões elétricas.
V - Repassar a seus empregados todas as orientações referentes à redução do consumo de energia e água.
VI - Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução dos serviços.
VII - Dar preferência a descarga e torneira com controle de vazão, evitando o desperdício de água.
VIII - Proporcionar treinamento periódico aos empregados sobre práticas de sustentabilidade, em especial sobre redução de consumo de energia elétrica, de consumo de água e destinação de resíduos sólidos, observadas as normas ambientais vigentes.
IX - Proibir quaisquer atos de preconceito de raça, cor, sexo, crenças religiosas, orientação sexual ou estado civil na seleção de colaboradores no quadro da empresa.
X - Conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e à saúde dos trabalhadores e envolvidos na prestação dos serviços.
XI - Destinar de forma ambientalmente adequada todos os materiais e/ou insumos que forem utilizados pela empresa na prestação dos serviços, inclusive os potencialmente poluidores, tais como, pilhas, baterias, lâmpadas fluorescentes e frascos de aerossóis, pneumáticos inservíveis, produtos e componentes eletroeletrônicos que estejam em desuso e sujeitos à disposição final, considerados lixo tecnológico.
XII - É proibido incinerar qualquer resíduo gerado.
XIII - Não é permitida a emissão de ruídos de alta intensidade.
XIV - Priorizar a aquisição de bens que sejam constituídos por material renovável, reciclado, atóxico ou biodegradável.
XV - Priorizar o aproveitamento da água da chuva, agregando ao sistema hidráulico elementos que possibilitem a captação, transporte, armazenamento e seu aproveitamento.
XVI - Colaborar para a não geração de resíduos e, secundariamente, a redução, a reutilização, a reciclagem, o tratamento dos resíduos sólidos e a disposição final ambientalmente adequada dos rejeitos.
XVII - A Contratada deverá observar no que couber, durante a execução contratual, critérios e práticas de sustentabilidade, como:
A - Dar preferência ao envio de documentos na forma digital, a fim de reduzir a impressão de documentos.
B - Em caso de necessidade de envio de documentos à Contratante, usar preferencialmente a função "duplex" (frente e verso), bem como de papel confeccionado com madeira de origem legal.
XVIII - Capacitar seus empregados, orientando que os resíduos não poderão ser dispostos em aterros de resíduos domiciliares, áreas de "bota fora", encostas, corpos d' água, lotes vagos e áreas protegidas por Lei, bem como em áreas não licenciadas.
XIX - Deverá, se possível, adotar práticas de sustentabilidade e de racionalização no uso de materiais e serviços, incluindo uma política de separação dos resíduos recicláveis descartados e sua destinação às associações e cooperativas dos catadores de materiais recicláveis.
XX - Armazenar, transportar e destinar os resíduos em conformidade com as normas técnicas específicas.

CLÁUSULA NONA - OBRIGAÇÕES DA CONTRATANTE

I Designar pessoa responsável para o acompanhamento dos serviços contratados, no local indicado, sendo que ele atestará a execução, conforme disposto nas condições e demais especificações contidas no Contrato de Prestação de Serviços e na Nota de Empenho.

II Cumprir com todos os compromissos financeiros assumidos com a Contratada.

III Comunicar prontamente a Contratada, qualquer anormalidade no objeto desde Contrato de Prestação de Serviços, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas.

IV Responsabilizar-se pelos custos da infraestrutura necessária para suportar o *appliance* virtual (caso seja necessário).

V Os treinamentos serão aplicados nas dependências da prefeitura municipal, que por sua vez, deverá disponibilizar os funcionários (setor de Tecnologia da Informação), providenciar as instalações físicas e os demais equipamentos necessários para a execução do treinamento.
VI Aplicar as sanções administrativas contratuais, em caso de inadimplência.
VII Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.
VIII Permitir que os funcionários da Contratada tenham acesso aos locais de execução dos serviços.
IX Todas as decisões e entendimentos havidos entre as partes durante o andamento dos trabalhos e que impliquem em modificações ou implementações nos planos, cronogramas ou atividades pactuadas, deverão ser prévia e formalmente acordados e documentadas entre as partes.
X Proceder ao recebimento provisório do objeto e, não havendo mais pendências, a administração promoverá o recebimento definitivo dos serviços, mediante vistoria detalhada realizada pela Comissão de Fiscalização e Recebimento de Bens, designada pelo Município, nos termos da Lei 8.666/93, em seu artigo 73, inciso I.
XI Fornecer, a qualquer tempo, mediante solicitação escrita da Contratada, informações adicionais, dirimir dúvidas e orientar em todos os casos omissos.

CLÁUSULA DÉCIMA - GESTOR DO CONTRATO
I - A administração indica como **gestor** do contrato o Secretário de Administração e Finanças, ***Mauro José Sbarain***, matrícula n° 11.041-8/4.
II - Entre suas atribuições está a de apurar a ocorrência de quaisquer circunstancias que incidam especificamente no art. 77, 78 e 88 da Lei 8666/93 que trata das Sanções Administrativas para o caso de inadimplemento contratual e cometimento de outros atos ilícitos.
III - Compete ao gestor da Ata de Registro de Preços, no que couber, as atribuições previstas no Decreto Municipal nº 8.296 de 17 de abril de 2018.
IV - As decisões e providências que ultrapassarem a competência destes deverão ser solicitadas a autoridade superior, em tempo hábil, para a adoção das medidas convenientes.

CLÁUSULA DÉCIMA PRIMEIRA - FISCAL DO CONTRATO
I - A administração indica como **fiscal técnico** do contrato, o servidor ***Eduardo Mello Amorim***, matrícula 10.145-1/1.
II - Compete ao fiscal da Ata de Registro de Preços, no que couber, as atribuições previstas no Decreto Municipal nº 8.296 de 17 de abril de 2018.
III - As decisões e providências que ultrapassarem a competência destes deverão ser solicitadas a autoridade superior, em tempo hábil, para a adoção das medidas convenientes

CLÁUSULA DÉCIMA SEGUNDA - SANÇÕES POR INADIMPLEMENTO
I - A licitante vencedora que ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a administração pública pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais, conforme disposto no Artigo 7º da Lei 10.520/2002, e Decreto Municipal nº 8.441, de 08 de janeiro de 2019.
II - Das Sanções Administrativas, conforme previsto no Art. 5º do Decreto Municipal nº 8.441/19:
a) As sanções administrativas serão aplicadas em conformidade com o prescrito na Lei Federal nº 8666/93, e em legislação correlata, podendo ser das seguintes espécies:
I Advertência;
II Multa, na forma prevista no instrumento convocatório ou no contrato;
III Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração;
IV Declaração de inidoneidade;
V Descredenciamento do sistema de registro cadastral.
b) As sanções previstas nos incisos I, III e IV do item anterior poderão ser aplicadas cumulativamente com a do inciso II.
III - Das Particularidades da Multa, conforme previsto no Art. 7º do Decreto Municipal nº 8.441/19:

a) A multa imposta ao contratado ou licitante, se não disposta de forma diferente no contrato, poderá ser:
I De caráter moratório, na hipótese de atraso injustificado na entrega ou execução do objeto do contrato, quando será aplicada nos seguintes percentuais:
a) 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplida, quando o atraso não for superior 30 (trinta) dias corridos;
b) 0,66% (sessenta e seis centésimos por cento) por dia de atraso que exceder a alínea anterior, até o limite de 15 (quinze) dias, na entrega de material ou execução de serviços, calculado, desde o trigésimo primeiro dia de atraso, sobre o valor correspondente à parte inadimplida, em caráter excepcional, e a critério do órgão contratante.
II De caráter compensatório, quando será aplicada nos seguintes percentuais:
a) 15% (quinze por cento) do valor do empenho em caso de inexecução parcial do objeto pela contratada ou nos casos de rescisão do contrato, calculada sobre a parte inadimplida;
b) 20% (vinte por cento) sobre o valor do contrato, pela sua inexecução total ou pela recusa injustificada do licitante adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração.
b) O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do primeiro dia útil seguinte ao do vencimento do prazo de entrega ou execução do contrato.
IV - A instrução obedecerá ao princípio do contraditório, assegurada ao acusado ampla defesa, com a utilização dos meios e recursos admitidos em direito.
V - Na fase de instrução, o indiciado será notificado pelo gestor do Contrato e terá o prazo de 05 (cinco) dias úteis, contados a partir do recebimento do correio eletrônico no e-mail registrado em Ata/Contrato, para apresentação da Defesa Prévia, assegurando-se-lhe vista do processo, e juntada dos documentos comprobatórios que considerar pertinentes à fundamentação dos fatos alegados na mesma.
VI - O extrato da decisão definitiva, bem como toda sanção aplicada, será anotada no histórico cadastral da empresa e nos sistemas cadastrais pertinentes, quando for o caso, além do processo ser apostilado na sua licitação correspondente.

CLÁUSULA DÉCIMA TERCEIRA **- ANTICORRUPÇÃO:**
I - As partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa (Lei Federal n.º 8.429/1992), a Lei Federal n.º 12.846/2013 e seus regulamentos, se comprometem que para a execução deste contrato nenhuma das partes poderá oferecer, dar ou se comprometer a dar, a quem quer que seja, aceitar ou se comprometer a aceitar, de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios indevidos de qualquer espécie, de modo fraudulento que constituam prática ilegal ou de corrupção, bem como de manipular ou fraudar o equilíbrio econômico financeiro do presente contrato, seja de forma direta ou indireta quanto ao objeto deste contrato, devendo garantir, ainda que seus prepostos, administradores e colaboradores ajam da mesma forma.

CLÁUSULA DÉCIMA QUARTA - EXTINÇÃO E RESCISÃO CONTRATUAL
I - Será automaticamente extinto o contrato quando do término do prazo estipulado, e não ocorrendo o acordo de prorrogação.
II - O contrato poderá ser rescindido amigavelmente pelas partes ou unilateralmente pela administração na ocorrência dos casos previstos nos Art. 77, 78 e 79 da Lei nº 8.666/93, cujo direito da administração o contratado expressamente reconhece.

CLÁUSULA DÉCIMA QUINTA - DO REAJUSTE DE PREÇOS
I - Os valor contratado poderá ser reajustado pelo IGPM, apurados e fornecidos pela Fundação Getúlio Vargas, depois de decorrido 01 (um) ano da apresentação da proposta de preços.
II - Não será concedido reajuste de preços resultante de atrasos ocorridos unicamente em decorrência da incapacidade da contratada em cumprir o prazo ajustado.

III - Havendo atraso ou antecipação na execução dos serviços, relativamente à previsão do respectivo cronograma, que decorra da responsabilidade ou iniciativa do contratado, o reajustamento obedecerá às condições seguintes:
a) Quando houver atrasos, sem prejuízo da aplicação das sanções contratuais devidas pela mora, se os preços aumentarem, prevalecerá os índices vigentes na data em que deveria ter sido cumprida a obrigação.
b) Se os preços diminuírem prevalecerá os índices vigentes na data do efetivo cumprimento da obrigação.
c) A posterior recuperação do atraso não ensejará a atualização dos índices no período em que ocorrer a mora.
IV - O reajuste dar-se-á mediante solicitação formal da Contratada, e firmada através de Termo de Aditamento de acordado entre as partes.
V - Caso haja alteração imprevisível no custo da prestação do serviço, caberá ao contratado requerer e demonstrar documentalmente, a necessidade de reequilíbrio econômico-financeiro do contrato com fundamento no artigo 65, II, "d" da Lei Federal n.º 8.666/93.
VI - Os valores recompostos somente serão repassados após a assinatura, devolução do Termo assinado (conforme o caso) e publicação do Termo de Aditamento.
VII - Não se admitirá nenhum encargo financeiro, como juros, despesas bancárias e ônus semelhantes.

CLÁUSULA DÉCIMA SEXTA - FORO
I - Fica eleito o foro da Comarca de Pato Branco - PR para dirimir questões relativas ao presente contrato, com a expressa e formal renúncia de outro qualquer, por mais privilegiado que seja.
Assim, por estarem certos e ajustados obrigando-se a bem e fielmente cumprir todas as disposições do Contrato, firmam-no em 02 (duas) vias de igual teor e forma.

Pato Branco, ___ de _____ de 2022.

Município de Pato Branco - Contratante
Robson Cantu - ***Prefeito***

- Contratada
- Representante Legal

ANEXO III
MODELO DA DECLARAÇÃO UNIFICADA DE IDONEIDADE, CUMPRIMENTO DO DISPOSTO NO INCISO XXXIII DO ART. 7º DA CONSTITUIÇÃO FEDERAL E DECLARAÇÃO DE COMPROMETIMENTO E CUMPRIMENTO AO ART. 9º, INCISO III DA LEI 8.666/93

A/C
Pregoeiro do
Município de Pato Branco - PR
Pregão Eletrônico nº 82/2022

A Empresa _____, devidamente inscrita no CNPJ nº _____, com endereço na Rua _____, nº_____, CEP: _____ na cidade de _____ Estado do _____, telefone (___) _____-_____ por intermédio de seu representante legal, o (a) Sr (a) _____, portador (a) da Carteira de Identidade nº _____e do CPF nº _____, DECLARA expressamente que:

I - Até a presente data inexistem fatos supervenientes impeditivos para habilitação no presente processo licitatório, estando ciente da obrigatoriedade de declarar ocorrências posteriores.

II - Não foi declarada inidônea por nenhum órgão público de qualquer esfera de governo, estando apta a contratar com o poder público.

III - Para cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, não empregamos menores de dezoito anos em trabalho noturno, perigoso ou insalubre e nem menores de dezesseis anos, em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos de idade, em cumprimento ao que determina o inciso V do art. 27 da Lei nº 8.666/93, acrescida pela Lei nº 9.854/99.

IV - Comprometo-me a manter durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

V - Não possuímos em nosso quadro societário e de empregados, servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação, nos termos do inciso III, do artigo 9° da Lei n° 8.666, de 21 de junho de 1993,

Local e Data.

_____
Assinatura do Representante Legal

ANEXO IV
MODELO PROPOSTA DE PREÇOS

A/C
Pregoeiro do
Município de Pato Branco - PR
Pregão Eletrônico nº 82/2022

A Empresa _____, devidamente inscrita no CNPJ nº _____, com endereço na Rua _____, nº_____, CEP: _____ na cidade de _____ Estado do _____, telefone (___) _____-_____; e-mail _____@____ por intermédio de seu representante legal, o (a) Sr (a) _____, portador (a) da Carteira de Identidade nº _____e do CPF nº _____, vem por meio desta, apresentar Proposta de Preços ao Edital em epigrafe que tem por objeto a Contratação de pessoa jurídica para fornecimento de licença de uso, locação de softwares de Firewall – Next Generation, E-mail, Acesso Remoto, Automação e Antivírus, treinamento básico, atualização corretiva, adaptativa e evolutiva, diagnósticos, atendimento e suporte técnico, por tempo determinado, com fornecimento de equipamentos mediante a comodato (*hardware*), em atendimento as necessidades de todas as Secretarias e Departamentos Municipais, conforme segue:

Item	Qtde Estimada	Und	Descrição	Valor Unit	Valor Total	Marca

Prazo de Validade da Proposta é de: 90 dias

A apresentação da proposta implicará na plena aceitação das condições estabelecidas neste edital e seus anexos.

Local e Data.

_____
Assinatura do Representante Legal