CONSULTA PÚBLICA DE PREÇOS Nº 126/2022

CONSULTA PÚBLICA DE PREÇOS: Constitui o presente objeto a aquisição de hardware e software como Segurança de Perímetro de Rede de Última Geração ligado em cluster com alta disponibilidade agindo inclusive como servidor proxy com controle de acesso.

1. Período para apresentação da proposta: de 09/08/2022 a 16/08/2022

2. A proposta poderá ser entregue pessoalmente no endereço: Praça José Rodrigues do Nascimento, 30 – Bairro Água Fria – Cajamar/SP (Secretaria Municipal de Fazenda e Gestão Estratégica – Departamento de Compras e Contratos) entre 08:00 e 17:00 horas ou enviar com papel timbrado da empresa para o e-mail Kimily.freitas@cajamar.sp.gov.br, conforme modelo abaixo:

MODELO - FORMULÁRIO - COTAÇÃO DE PREÇOS

Nome da Empresa:		
E-mail institucional:		
E-mail pessoal:		
Endereço:		
Bairro:		**CEP:**
Cidade:		**Estado:**
CNPJ Nº:	**Inscrição Estadual:**	
Fone:	**Fax:**	

3. DISPOSIÇÕES GERAIS:

4.1. O proponente responderá pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase desta coleta de preços.

4.2. O presente procedimento não gera qualquer obrigação contratual entre a proponente e a Prefeitura do Município de Cajamar, e tem como finalidade apenas a verificação de preços no mercado em questão.

ANEXO I
TERMO DE REFERÊNCIA

1 – DO OBJETO

Constitui o presente objeto a aquisição de hardware e software como Segurança de Perímetro de Rede de Última Geração ligado em cluster com alta disponibilidade agindo inclusive como servidor proxy com controle de acesso.

2 – DA JUSTIFICATIVA

A aquisição dos equipamentos se faz necessária em função da necessidade de atualização das ferramentas utilizadas para controle de acesso aos conteúdos, bem como pelo fato da Secretaria Municipal de Modernização Tecnologia e Inovação não dispor de equipamentos suficientes para manter o atendimento das demandas em questão, objetivando o pleno funcionamento do parque computacional desta administração e seus setores.

Considerando o momento crítico que vivemos no quesito de segurança da informação, é necessário ressaltar a importância que as atividades desempenhadas seja como serviço de natureza contínua. Somente assim é possível auxiliar nas medidas de prevenção e combate a ataques cibernéticos, vírus, falhas de segurança, tentativas de invasão, roubo de dados, perda de dados e interrupções nas atividades operacionais e administrativas.

A contratação é imprescindível à administração pública para o desempenho de suas atribuições, onde a interrupção de qualquer um dos itens pode comprometer a continuidade das atividades da prefeitura. Tendo em vista que toda a infraestrutura de

computadores, e-mails, e websites em uso na área administrativa funciona de forma totalmente integrada, faz-se necessária a contratação de uma empresa que comercialize softwares de segurança cibernetica, de forma integrada e que ainda, o suporte a todas as soluções seja diretamente com o fabricante das soluções em regime irrestrito. E que possa garantir os itens descritos neste documento de forma a garantir um monitoramento e gerenciamento adequados de todo o ambiente sem prejuízo para os usuários.

As boas práticas de segurança da informação sempre relacionam que o investimento necessário seja proporcional ao risco e impacto de uma ocorrência danosa ao ambiente de rede, bem como todos os sistemas e processos que o envolvem.

Analisando o risco e o impacto, percebemos um cenário com uma probabilidade cada vez maior de ocorrência, dado o aumento vertiginoso de quantidade de ameaças a cada momento. Nestes últimos anos, vivenciamos situações altamente perigosas com até mesmo instituições, até então altamente protegidas com altos investimentos em segurança da informação, tiveram seus dados comprometidos e muitas vezes tornando-os públicos, o que infringe em muitos casos a LGPD (Lei Geral de Proteção de Dados - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018), em vigor desde 2020.

É de conhecimento de todos que o ataque mais popular atualmente é referente ao sequestro de informação, na imensa maioria das vezes sendo comprometido por meio de um malware denominado “ransomware”. Por ransomware, entende-se que é um tipo de malware que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate, em dinheiro ou criptomoedas para que o acesso possa ser restabelecido. Desde que se vivenciou um grande aumento de infecção por ransomware, foi natural o aumento do uso de sistemas de backup como uma alternativa para minimizar os danos, para que caso tenha os dados comprometidos, possa restaurar de maneira rápida reduzindo a chance de prejuízo. Porém, como podemos observar diante as informações publicadas na mídia, a tática adotada pelos criminosos tem sido que além do “sequestro de dados”, ameaçam com a divulgação de dados na mídia, acarretando pesadas consequências para a instituição que sofre tais tipos de ataque. Isso faz com que o backup não seja a única ação necessária para minimizar os dados de um ataque de ransomware, sendo necessário proteção completa.

As ameaças não se limitam apenas ao ransomware, poderíamos listar pelo menos milhares de ameaças a mais que vão desde ataques diretos para explorar alguma falha e vulnerabilidade com intuito de invasão direta aos servidores e desktops. Assim como também a negação de serviço entre os mais explorados.

Muitos dos ataques são com objetivos financeiros, como tem ocorrido em diversos órgãos governamentais conforme reportagens a seguir:

Prefeitura de Barroso:

https://www.barbacenamais.com.br/policia-mais/62-policia-militar/20138-conta-bancaria-da-prefeitura-de-barroso-e-invadida-por-hacker

Prefeitura de Taboão da Serra:

https://g1.globo.com/sp/sao-paulo/noticia/2021/09/17/piratas-digitais-invadem-sistema-da-prefeitura-de-taboao-da-serra-na-grande-sp-e-deixam-populacao-sem-servicos-publicos.ghtml

Prefeitura de Candiota:

https://g1.globo.com/rs/rio-grande-do-sul/noticia/2020/10/15/hackers-invadem-sistemas-da-prefeitura-de-candiota-e-prejudicam-funcionamento-de-servicos.ghtml

Prefeitura de Brumadinho:

https://hojeemdia.com.br/minas/site-da-prefeitura-de-brumadinho-e-invadido-e-hackers-publicam-video-atacando-a-mineradora-vale-1.868906

Como pode-se verificar, os prejuízos somados chegam em altíssimas cifras de centenas de milhões.

O problema torna-se ainda mais grave, quando o alvo são instituições consideradas críticas para população, assim como ocorreu com a invasão à usina de água no estado da florida nos Estados Unidos em que um hacker tentou manipular as misturas quimicas na água, podendo causar um grande desastre para a população:

Florida EUA:

https://g1.globo.com/economia/tecnologia/noticia/2021/02/08/hacker-tentou-contaminar-agua-com-aditivo-quimico-em-cidade-da-florida.ghtml

Segundo a CNN Brasil, somente no primeiro mês deste ano, já temos mais de 20 instituições públicas que sofreram ataques cibernéticos.

Infelizmente a tendência é que tais atos, sejam cada vez mais frequentes. Recentemente o fórum econômico mundial, em seu evento anual, classificou problemas de Cibersegurança entre as maiores ameaças mundiais nos próximos anos, apelidado pelo seu presidente (Klaus Swab) como “Ciber Pandemia”, reforçando ainda mais o grau de atenção à segurança da informação nos momentos atuais.

Fórum Econômico Mundial: https://www.weforum.org/

Dado estas informações, podemos considerar o risco como alto, justificando a abrangência de soluções conforme descrito neste termo.

3 - DO FABRICANTE E CONTRATADA

3.1 O fabricante do produto deverá ser uma empresa atuante na área de segurança da informação a fim de garantir eficácia das soluções de proteção.

3.2 A solução deverá possuir em um único painel em nuvem que agregue em grande parte o gerenciamento e monitoramento das soluções listadas. As funções de gerenciamento e monitoramento que deverão ter no painel em nuvem estão listadas neste documento.

3.3 A solução entregue por um único fornecedor precisará deter a capacidade de fazer ajustes/correções, mesmo que no código fonte do sistema em nuvem.

3.4 A proponente deverá garantir que ao longo do presente contrato, nenhum produto, software, hardware ou peças necessárias, estejam em uma versão considerada não oficial, não comercializada, “end-of-life, end-of-sale ou end-of-support”. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte e vida. Devendo estar em linha de produção do fabricante, sempre em sua versão mais atualizada (seja software, sistema e hardware, caso o fabricante lance uma nova versão, etc.) A proponente deverá garantir que estão cobertos por garantia ao longo do contrato.

3.5 Todas as funcionalidades descritas, deverão ser comprovadas por meio de documento oficial do fabricante, a fim de garantir que as funcionalidades de grande importância para proteção estejam contempladas.

3.6 Apresentar Carta emitida pelo próprio Fabricante, dirigida ao CONTRATANTE, referenciando ao edital em epígrafe, informando que a Proponente é revenda autorizada a comercializar seus produtos e serviços, e o Fabricante confirma que atende a todos os itens listados no referente edital.

3.7 Será feita a verificação da compatibilidade dos recursos e das capacidades, facilidades operacionais informadas na proposta para cada item ofertado com base nas informações dos catálogos, folhetos, manuais técnicos e semelhantes produzidos pelo fabricante. Documentos estes que deverão ser

anexados a proposta comercial, referenciando o endereço web para consultas e diligências de todo material apresentado. Salienta-se que não serão aceitos materiais produzidos pela Proponente a não ser que o material seja fornecido diretamente pela fabricante.

3.8 Apresentar no mínimo 1 técnico certificado em todas as soluções ofertadas. Este deverá ser comprovado através de documento emitido pelo fabricante da solução ou empresa devidamente autorizada para emissão de certificados, no caso de a certificação não ser realizada pelo fabricante da solução, deverá apresentar comprovação que a empresa fornecedora da certificação é devidamente credenciada para emitir tal documentação.

3.9 Apresentar no mínimo 1 técnico certificado com cursos voltados para segurança da informação, oferecidos por empresas cujo foco seja segurança da informação.

3.10 A proponente deverá disponibilizar serviços de treinamento especializado em segurança da informação oficiais do fabricante da solução, com certificado do fabricante, de forma a atender aos seguintes requisitos: carga horária mínima de 40 horas, 20 participantes na turma.

3.11 A proponente deverá efetuar visita técnica presencial antes da apresentação da proposta para verificar requisitos físicos a serem providos para a correta instalação dos equipamentos e prestação de serviços.

3.12 As visitas somente poderão ocorrer de segunda a sexta, das 10hs às 12hs ou 14hs as 16hs.

4 – DA INSTALAÇÃO

4.1 A instalação deverá ser executada dentro do horário comercial que compreende (das 09:00 às 17 horas).

4.2 A contratante deverá dispor de tempo para que a contratada realize levantamento técnico remoto com o intuito de análise e preparação de documentação da implantação do mesmo.

4.3 Um técnico certificado pelo fabricante deverá executar a instalação e configuração do firewall no contratante, executando as configurações de firewall, configuração de NAT para entrada e saída, configuração de VPN para colaboradores com no máximo até 5 túneis, dar treinamento básico sobre filtro de conteúdo durante a instalação, dar treinamento básico sobre definições de políticas durante a instalação, ativar filtro de conteúdo web com regras gerais sem bloqueio e disponibilizar um técnico certificado pelo fabricante remotamente por 24 horas corridas após a implantação para dúvidas e ajustes.

5 – DA GARANTIA

5.1 A garantia do hardware de Segurança de Borda de Rede de Última Geração, via appliance, é de responsabilidade do fabricante e precisa ser de no mínimo 12 (doze) meses, garantindo inclusive todas as atualizações de hardware caso seja necessário, uma vez mantidas as condições de dispositivos conectados dentro de sua capacidade, como solicitado e acordado durante a contratação do serviço. Quer dizer, se a quantidade de dispositivos atingir um número acima do contratado inicialmente, se faz necessário a troca de equipamento e o reajuste dos valores do mesmo; e ainda a troca de hardware em caso de mal funcionamento ou end-of-life do hardware.

5.2 O acréscimo de hardware ao appliance como interfaces adicionais ou a troca das interfaces nativas por novas tecnologias, incidem em reajustes de preço, não constando como itens que possam ser atualizados ou somados dentro da garantia. Ou seja, a garantia não contempla acréscimo de interfaces ou atualização das já existentes por interfaces de tecnologias novas ou com funções e recursos diferentes das nativas no ato da contratação.

6- DO HARDWARE E SERVIÇOS

Item	Descrição	Qtd

01	Appliance (hardware) de Segurança para Perimetro de Rede de Ultima Geração	02
02	Central de Monitoramento e Alertas	01
03	Treinamento Tecnico Certificado	06
04	Serviços de Suporte do Fabricante 24/7	01

6.1 Item 01 – Appliance (hardware) de Segurança para Perimetro de Rede de Ultima Geraçao

6.1.1 A solução de segurança de redes, também chamado de Firewall UTM ou Firewall NG, deverá permitir acesso as informações do produto, em idioma Português (Brasil), não somente através de um acesso direto ao equipamento e ao seu painel, como também acesso à um servidor em Cloud (nuvem). Permitindo assim ser acessado de qualquer lugar, sem restrições de origem, através de login e senha com possibilidade de possuir dupla autenticação a fim de aumentar o nível de segurança de acesso.

6.1.2 O painel em Cloud (nuvem), permitirá visualizar informações essenciais dos produtos em tempo real, a fim de monitoramento, tais como informações do hardware, processamento, memória, disco, informações de qualidade do link, disponibilidade, latência e perda de pacotes.

6.1.3 O servidor em nuvem, deverá efetuar backup das configurações dos produtos, no mínimo diariamente, a fim de aumentar a segurança em caso de algum incidente que afete as configurações ou o hardware.

6.1.4 O servidor em nuvem, deverá avaliar o nível de risco do produto, no que se refere as melhores práticas de configuração de segurança de redes, sendo analisado pelo menos as regras de firewall, regras de NAT, qualidade da senha de acesso, configurações de VPN, entre outros. Tal análise tem que ser no mínimo diária.

6.1.5 Deverá possuir aprendizado de máquina (Machine Learning) trabalhando na prevenção de ataques em todas as camadas segundo o modelo OSI, referenciando arquivos.

6.1.6 Estabelecer comunicação contínua com mecanismos em nuvem para receber atualizações de informações de maneira contínua, visando aperfeiçoamento e reciclagem de conteúdo.

6.1.7 Possuir recurso para recomendação de boas práticas relacionadas a controle, gestão e segurança através de alertas, gráficos e análise de risco. Existir ainda a possibilidade de configurar as recomendações para reduzir as chances de falhas humanas, automatizando alertas.

6.1.8 Em caso de impossibilidade de configuração via interface gráfica, devido à algum incidente, a solução deverá permitir também o acesso via console de linha de comando, podendo ser acessível através de protocolo de acesso remoto. Tal como: SSH ou conexão direta via cabo console. As configurações mínimas permitidas por meio de linha de comando deverá ser:

6.1.9 Configuração de interface de rede, configuração de senha de acesso à WEB, “resetar” equipamento para a configuração “padrão de fábrica”, reiniciar o sistema, parar o sistema, acesso ao sistema operacional, lista das atividades do firewall, visualizar filtro do firewall, reiniciar o serviço de acesso à WEB, acessar o sistema operacional como “desenvolver”, à fim de reparação de algum bug. Atualização do sistema, habilitar acesso via SSH, efetuar download de módulos, pacotes ou atualizações, logout e ping.

6.1.10 Com objetivo de ter uma instalação fácil, prática e rápida. A solução deverá permitir a utilização de um auxiliador de configuração (wizard) nos casos de primeira instalação do sistema.

6.1.11 A solução deverá suportar uso de VLANs 802.1Q.

6.1.12 A solução deverá suportar regras de Firewall tradicionais, permitindo filtrar por: origem e IP de destino, porta de origem do protocolo, e destino IP para o tráfego TCP e UDP, com limite de conexões simultâneas por regra, com possibilidade de alteração do gateway para cada regra, podendo fazer balanceamento de carga ou failover por regra. As regras de Firewall devem permitir também gestão da tabela de estado das conexões.

6.1.13 A solução deverá permitir efetuar regras de Firewall por Objetos. Por objetos considerasse um IP, Porta, URL, sub-redes, entre outros.

6.1.14 A solução deverá fazer bloqueios na camada de aplicação (considerando camada 7 no modelo de camadas OSI de comunicação), também chamado de Firewall por aplicação permitindo assim:

6.1.15 Reconhecer aplicações independente de porta e protocolo, tendo a capacidade de bloquear e liberar aplicações diretamente através de configuração por meio da interface gráfica com poucos cliques, podendo configurar regras por grupo e usuário.

6.1.16 Efetuar regras por usuário ou grupo através de integração com Microsoft Active Directory ou base local.

6.1.17 A solução deverá reconhecer pelo menos aplicações nas seguintes categorias: redes sociais, ameaças, pornografia, antivírus, portais.

6.1.18 A solução deve mostrar por meio de um painel o percentual do tráfego de cada rede social, tais como: facebook, twitter, instagram, whatsapp, linkedin, youtube e as aplicações que estão sendo utilizadas no momento, com informações sobre a aplicação, data e hora, nome de usuário que está originando o tráfego e se o tráfego está liberado ou bloqueado.

6.1.19 A solução deverá prover relatório de acesso do uso das aplicações.

6.1.20 A solução deverá possuir proteção contra tráfego malicioso, ataques, independente de porta e protocolo, ou seja, proteção na camada 7 (camada de aplicação segundo modelo OSI), permitindo visualizar em um dashboard de maneira gráfica e georreferenciada de acordo com a origem dos ataques.

6.1.21 A proteção na camada 7 contra tráfego malicioso, deverá garantir bloqueio de no mínimo worms, trojans, malwares, além de protocolos de uso não recomendados como: UltraSurf, UltraVPN, CyberGhost, Express VPN etc.

6.1.22 Deverá ainda ter proteção em tempo real de forma distinta da proteção na camada de aplicação.

6.1.23 Uma vez que seja uma ferramenta de proteção de borda nativamente na interface WAN, deverá englobar todas as ferramentas de proteção como antivírus, antiphishing, antispyware, antiransomware e IDS/IPS.

6.1.24 Deve possuir dashboard exclusivo com gráficos de informações dos principais países de origem das tentativas de invasões.

6.1.25 Ter recurso para exibir um resumo das tentativas de invasão, infecções identificadas e nível de risco de cada uma delas.

6.1.26 Deverá possuir proteção integrada de IPs com assinaturas mantidas também pelo fabricante.

6.1.27 Deverá ter disponível uma ferramenta responsável por identificar e bloquear aplicações ou serviços independente de uso de um Proxy nos dispositivos. Com capacidade de bloquear até mesmo tráfego de dispositivos móveis.

6.1.28 Oferecer opção de separação de gráficos e as porcentagens de acesso por rede/interface.

6.1.29 Exibir consumo por aplicações e detalhes de pelo menos as 5 principais aplicações que mais consomem banda da internet.

6.1.30 As informações de navegação devem ser em tempo real, com a possibilidade de separar interface/rede.

6.1.31 Deverá ter gráfico com porcentagem de navegação separado por categoria.

6.1.32 Deverá possuir a seleção total ou parcial de bloqueios ou liberações de aplicativos ou websites.

6.1.33 A solução deve possuir a possibilidade de uso de regras separadas por redes (book de regras), e ainda ser possível configurar políticas de navegação distintas entre as redes.

6.1.34 Deve ainda possuir um modo simplificado de uso do recurso agindo na camada de aplicação, para uso em equipamentos com hardware com carga alta de consumo.

6.1.35 Deve possuir recurso de limpeza de log e data base de log de navegação, com recurso de limpeza automática, com possibilidade de personalização e alterações de configurações.

6.1.36 A solução deverá permitir efetuar bloqueio de conexões recebidas por determinado país ou continente, tendo como uma das funcionalidades, permitir visualizar países ou continentes líderes no ranking de tráfego malicioso e assim fazer bloqueios de entrada e saída.

6.1.37 A solução deverá permitir regras de redirecionamento de portas, atuando como um recurso para informar ao equipamento qual o destino a ser dado aos pacotes.

6.1.38 A solução deverá permitir regras de NAT (Network Address Translator), entre os hosts da rede interna e a internet, traduzindo os IPs com as seguintes características: Encaminhamento de portas, incluindo faixas de rede e o uso de múltiplos IPs públicos, NAT para IPs individuais ou sub-redes inteiras, NAT de saída, NAT de saída avançado, permitindo que seu comportamento padrão seja desativado e permitindo a criação de múltiplas flexões de regras de NAT, NAT Reflection, possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.

6.1.39 A solução deverá fazer proxy do protocolo IGMP entre segmentos de rede, bem como interface de upstream e downstream.

6.1.40 A solução deverá, através de funcionalidade, permitir suporte ao protocolo Universal Plug and Play (UPnP) e NAT Port Mapping Protocol (NAT-PMP), podendo configurar download e upload máximo caso necessário.

6.1.41 A solução deverá possuir suporte para ser configurado o serviço de Wake on LAN, através de suporte no hardware, com objetivo de ligar o computador através de um pacote específico de rede.

6.1.42 A solução deverá possuir suporte para atualização automática da base de seu sistema, sempre que existir alguma disponível.

6.1.43 A solução deverá permitir criação de tabela de horários para agendamento de regras, bem como vincular uma regra a uma agenda definida para que elas vigorem a partir de ou durante datas e horários previamente especificados.

6.1.44 A solução deverá fornecer recursos de gerência de tráfego de rede, sendo possível a criação de regras dos seguintes tipos: Priorização de tráfego, definindo quais protocolos possui prioridade, Limite de tráfego por protocolo, definindo qual limite máximo de um protocolo, reserva de tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.

6.1.45 Permitir que o DHCP Relay encaminhe requisições para um servidor definido em outro segmento de rede.

6.1.46 A solução deverá dispor de servidor DHCP, que permita atribuir endereços IPs e configurações relacionadas aos dispositivos da rede, por meio de MACAddress.

6.1.47 A solução deverá permitir uso de DNS dinâmico para que seja registrado o endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usados para conectar-se à VPNs, Web Servers e também Mail Servers. Podendo ser usado conta em serviço de terceiros no mínimo as seguintes opções: DynDNS, No-IP, OpenDNS, ZoneEdit e DyNS.

6.1.48 A solução deverá permitir gravar logs separando por pelo menos as seguintes categorias: Firewall, DHCP, Autenticação, IPSec, PPP, VPN, Load Balance, OpenVPN, NTP.

6.1.49 A solução deverá permitir gravar logs em servidor externo podendo configurar até 3 servidores.

6.1.50 O sistema deverá permitir envio de informações pré-programadas referente ao status do link, permitindo selecionar o gráfico a ser enviado, bem como enviar e-mail informando quando houver queda de link.

6.1.51 O sistema deverá permitir gerenciar certificados através de modo gráfico, e criar e/ou revogar novos certificados através do painel web.

6.1.52 O sistema deverá permitir efetuar controle de permissão para acesso às funcionalidades da solução.

6.1.53 A solução deverá permitir load balancing e/ou failover no tráfego de saída para Internet, permitindo configurar de acordo com a qualidade do link ou queda do mesmo.

6.1.54 Possibilidade de sincronização de horário do equipamento utilizando protocolo NTP.

6.1.55 A solução deverá possuir suporte, através de um serviço do sistema operacional para OLSR (Optimized Link State Routing Protocol).

6.1.56 A solução deverá permitir utilização do protocolo Netflow versão 1, 5 ou 9 para envio de informações referente à tráfego/link, permitindo configurar no mínimo: IP de destino, porta, IP de origem e restrição de direção.

6.1.57 A solução deverá permitir configurar roteamento dinâmico, tal como: RIP versão 1 e 2, OSPF padrão RFC 1583 ou BGP.

6.1.58 A solução deverá suportar utilizar protocolo SNMP.

6.1.59 A solução deverá possuir no mínimo os seguintes gráficos: memória, throughput, links, VPN, qualidade dos links, processamento.

6.1.60 A solução deverá permitir configurar um servidor PPPoE Server no equipamento, podendo ter autenticação por: base local, RADIUS, ou acessar um servidor PPPoE para ativar algum link.

6.1.61 A solução deverá permitir no mínimo as seguintes opções de VPN (Site-to-Site ou Client-to-Site): IPSec, OpenVPN e o L2TP, podendo a solução ser o server ou o client e permitindo uso de VPN com outros equipamentos de outros fornecedores, sem limite de licenças.

6.1.62 A solução deverá permitir uso de um cliente OpenVPN do fabricante, com opção de autenticação em base AD (Active Directory) ou LDAP, podendo ser instalado em estações de trabalho Windows, MAC OS X, ou dispositivos móveis como IOS (IPhone/IPad), Android.

6.1.63 Deverá possuir a funcionalidade de enviar e-mail sempre que: algum usuário se conectar ou desconectar no túnel VPN. A solução deverá ainda gravar logs das conexões de VPN, permitindo visualizar relatórios.

6.1.64 Todos os equipamentos deverão suportar funcionamento em modo Cluster e todas licenças para seu uso deverão estar inclusas no fornecimento, permitindo a configuração de dois firewalls como um grupo de “failover”, se uma interface falhar no primário ou ficar “off-line” completamente, o secundário se torna ativo, sem qualquer prejuízo de parada, lentidão ou interrupções de atividade de operação, tendo o secundário mesma capacidade que o primário (quantidade de usuários, conexões simultâneas, troughput, etc.) especificadas no dimensionamento.

6.1.65 A solução deverá disponibilizar funcionalidade para fazer cópias seguras de seus dados, tais como configuração e relatórios, podendo ou não ser agendados.

6.1.66 A solução deverá permitir também efetuar backup em servidor em nuvem (cloud) de maneira automática e deverá estar incluso no contrato o serviço em nuvem para manter ao menos 5 copias das configurações do equipamento.

6.1.67 A solução deverá possuir módulo de liberação e bloqueio de maneira fácil e rápida e atualizados diariamente comuns para liberação ou bloqueio em uma rede considerada comum, tais como: Windows Update, Java, Caixa/Conectividade Social, Bancos, Microsoft, Governo, Acesso remoto, Redes sociais.

6.1.68 A solução deverá permitir gerenciamento de visitantes para acesso à redes para visitantes, com possibilidade de autenticação para usuários, por meio de cadastro, facebook, AD / LDAP, RADIUS.

6.1.69 A solução deverá permitir bloqueio de acesso à sites, por meio de categoria (atualizado diariamente com no mínimo 48 categorias), com regras que permita a escolha de trabalhar com proxy transparente ou autenticado. No caso de autenticação, os usuários poderão se autenticar através de: base local, LDAP, Active Directory (AD), RADIUS, NTdomain e Single-Sign-on.

6.1.70 A solução deverá permitir a criação de categorias personalizadas sem limite de quantidades, bem como permitir criação de lista brancas/negras como exceções. A solução deverá também scanear arquivos que forem efetuados download para verificar de vírus/malwares (todas licenças inclusas).

6.1.71 A solução deverá ter módulo de diagnóstico de bloqueio ou liberação de URL por usuário, mostrando qual regra está permitindo ou bloqueando o acesso a fim de diagnóstico rápido de ajuste da regra. A solução deverá também permitir o usuário justificar o acesso à uma URL bloqueado, podendo assim acessar mediante somente a justificativa ou mediante aprovação após a justificativa por parte de usuário com acesso administrativo.

6.1.72 A solução deverá compor suíte de relatórios no mesmo equipamento ou em caso de necessidade de uso de outro equipamento ou software o fornecedor deverá incluir todas os valores e licenças bem como equipamentos para atender ao quesito “relatórios de gerenciamento”; A suíte de relatórios deverá possuir capacidade de ser acessada por meio de smartphones IOS/Iphone e Android e poder gerenciar os usuários que possuem acesso à ferramenta.

6.1.73 A suíte de relatório deverá permitir a personalização da marca estampada no cabeçalho do relatório, e possuir ao menos as seguintes informações de acesso: usuários, consumo de link, acessos por IP, acessos por usuário, acesso por categoria, acesso por meio de VPN.

6.1.74 A solução deverá permitir visualizar estrutura de rede conectada entre unidades por meio do painel em Cloud, permitindo visualizar problemas de rotas de conexão entre unidades, e permitir fazer failover sobre conexões de VPN de maneira automática sem intervenção manual.

6.1.75 A solução deverá fornecer sistema de detecção e prevenção de intrusão com capacidade de inspecionar o “payload” do pacote, fazendo o registro dos pacotes, além de detectar as invasões. Capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades, além de permitir a configuração de avisos ao administrador do ambiente sobre o ataque.

6.1.76 A solução deverá ser fornecida em appliance, ou seja, integração do hardware com software do mesmo integrador. Não serão aceitos equipamentos de uso genérico.

6.1.77 Caso o fabricante tenha um novo modelo durante o período do contrato, a CONTRATADA deverá efetuar a substituição pelo modelo mais novo sem ônus adicional à CONTRATANTE.

6.1.78 Não serão aceitos modelos do tipo SOHO ou quaisquer appliances preparados para modelos do tipo “Home office”.

6.1.79 No caso de módulos opcionais, caso o equipamento não permita a substituição, deverá ser contemplado o equipamento considerando o opcional como permanente.

6.1.80 Características Físicas do Firewall UTM NGFW

- Memória mínima: 12GB
- Interfaces de rede mínimo: 10 interfaces (Gbps)
- Possuir capacidade para adicionar módulo opcional substituindo 4 interfaces 1GB por interface com:
- Capacidade para 2 interface 10gb
- Capacidade para 2 interfaces fibra
- Capacidade para colocar 8 interfaces 1gb
- Interfaces Bypass mínimo: 2
- Processador:
- Número de núcleos: 4
- Nº de threads 8
- Frequência mínima em processador: 4.00 GHz
- Conector console RJ45
- Conector HDMI/VGA
- Portas USB: 2
- Fonte de Alimentação Full Range.
- Disco: 240GB SSD
- Quantidade dispositivos simultâneos: 3.000
- Throughput mínimo de Firewall: 9.7GB

6.2 Item 02 – Central de Monitoramento e Alertas

6.2.1 A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação e o módulo deverá prover painel próprio de monitoramento na plataforma web com atualização em tempo real do alerta bem como prover App para ser instalado em dispositivos móveis da família Android e IOS.

6.2.2 Deverá disponibilizar função modo TV para facilitar a análise das informações, permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta e monitores do grupo segurança de redes.

6.2.3 Se o serviço de backup das configurações foi executado com sucesso ou não, se o número de hosts está superando o contratado, se a versão do sistema operacional está atualizada ou não é o monitoramento configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo CPU, memória e carga média.

6.2.4 Permitir monitorar as interfaces da solução, permitir monitorar links, gerando alertas e caso de perda de pacotes, latência ou queda de link e a solução deverá permitir o monitoramento dos serviços de filtro de conteúdo web entre outros.

6.3 Item 03 – Treinamento Técnico Certificado

6.3.1 A Contratada fornecerá treinamento oficial do fabricante da solução, com instrutor certificado pelo fabricante e deverá ter carga horária mínima de 16 (dezesseis) horas e deverão participar no mínimo 1 (um) servidor do Departamento de Tecnologia da Informação.

6.3.2 O período de realização do treinamento oficial do fabricante será fixado pelo Departamento de Tecnologia da Informação em conjunto com a Contratada, no prazo máximo de 30 (trinta) dias após o recebimento definitivo da entrega e instalação da solução.

6.3.3 Permitir a possibilidade de treinamento presencial (handson), direto com o fabricante com a mesma quantidade de horas e a mesma qualidade do curso certificado integral com reconhecimento do fabricante e dispensando despesas com alimentação e hospedagem que serão de inteira responsabilidade da CONTRATANTE.

6.3.4 O treinamento oficial do fabricante deverá ser ministrado virtualmente pelo fabricante, de segunda a sexta-feira, das 8:00 às 17:00, de modo que os alunos possam praticar e obter

6.3.5 conhecimentos. Não serão aceitos treinamentos gravados, todos deverão ser ao vivo em tempo real com técnicos formalmente oficializados do fabricante.

6.3.6 A Contratada deverá emitir para o servidor participante, sem ônus e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento oficial do fabricante, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia desse certificado deverá acompanhar a nota fiscal para o devido pagamento.

6.3.7 Todo o material didático oferecido pela Contratada para realização do treinamento deverá ser oficial do fabricante da solução, ser de primeiro uso, atualizados e deverão estar em inglês e português.

6.3.8 O resultado da Avaliação de Instrutor/Tutor será utilizado como critério de aceitação do treinamento oficial do fabricante, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 6 (seis) dos 10 (dez) itens avaliados.

6.3.9 Caso o resultado da Avaliação de Instrutor/Tutor seja considerado “não proveitoso”, o treinamento oficial do fabricante fornecido será considerado não aceito.

6.3.10 Na hipótese de não aceitação, a Contratada deve oferecer outro treinamento oficial do fabricante, com a mesma carga horária, com outro instrutor, sem qualquer ônus:

6.3.11 Na hipótese de o resultado do segundo treinamento oficial do fabricante ser “não proveitoso”, o objeto será considerado não aceito, caracterizando inexecução parcial da obrigação, aplicando-se as sanções previstas contratualmente.

6.3.12 O novo treinamento oficial do fabricante deverá ser realizado no prazo de 30 (trinta) dias, contados da não aceitação, considerando-se os critérios estabelecidos nesse item.

6.4 Item 04 – Serviço de Suporte do Fabricante 24/7

6.4.1 Deverá fornecer suporte 24 horas por dia, 7 da semana de forma irrestrita, direcionado aos serviços de segurança cibernética contratados.

6.4.2 O suporte deverá ser disponibilizado e permitir contato via e-mail, telefone ou chat direto com especialistas do fabricante das soluções, sem intermédio de distribuidores e sem automação (robô).

6.4.3 Em caso de necessidade de substituição do NG Firewall, seja por mal funcionamento de hardware ou software, o suporte deverá prover um equipamento reserva com SLA de no máximo 4hrs úteis/balcão.

6.4.4 Todas as atualizações de hardware ou de software das soluções são por conta do fabricante e caso seja necessário mediante chamado técnico, o fabricante deve intervir remotamente para prestar o suporte ao usuário final.

6.4.5 O suporte do fabricante deverá manter um backup em nuvem atualizado, no caso de locação de Firewall UTM NGFW, com todas as configurações do equipamento para uso posterior

7 – PROVA DE CONCEITO

7.1 Constatado o atendimento pleno das condições de menor preço e de habilitação, essa será declarada provisoriamente vencedora do certame.

7.2 A sessão será suspensa para a apresentação da prova de conceito, que acontecerá até o 5º (quinto) dia útil após a abertura dos envelopes, sendo ela a partir das 09hrs00min.

7.3 Serão nesta etapa, validadas as funcionalidades contidas nos itens 6.1 à 6.1.80, pelos integrantes da Comissão Técnica nomeada pela Secretaria de Modernização, Tecnologia e Inovação, através da demonstração da solução ofertada, os integrantes da comissão irão observar o atendimento às especificações pela solução ofertada, por meio da simples conferência do atendimento ou não às funcionalidades

7.4 As demonstrações serão sucessivas, observando-se a mesma ordem em que se encontram neste termo, devendo ser feitas em equipamentos da própria licitante, inclusive periféricos e, havendo necessidade, a Secretaria de Modernização e comunicação disponibilizará apenas o espaço para apresentação e acesso à internet.

7.5 A apresentação de cada sistema deverá ser feita em até 05 (cinco) horas, procedimento este que será acompanhado pelo servidor responsável do setor correspondente, devidamente designado para apoio durante a sessão, podendo também ser assistido pelas demais licitantes, desde que não causem tumulto ou mantenham comportamento inadequado durante as demonstrações.

7.6 Não deverão ser feitos questionamentos durante as demonstrações, para que possa ser devidamente cumprido o prazo especificado para a apresentação, porém a licitante classificada em primeiro lugar deverá usar este termo como um checklist, demonstrando item a item.

7.7 Terminada a demonstração do sistema, a Secretaria de Modernização, Tecnologia e Inovação, por meio do servidor responsável pelo setor correspondente, manifestar-se-á pela sua aprovação ou reprovação, sendo que, nesse último caso, deverá especificar as funcionalidades que entendeu não terem sido atendidas, ouvindo também eventuais apontamentos por parte das demais licitantes, que poderão se manifestar na ata ou incluir à ata um anexo constando os tópicos que entendeu oportuno se manifestar quanto aos desatendimentos.

7.8 Caso as demonstrações não possam ser finalizadas no mesmo dia, poderá ser dada continuidade no dia seguinte, lavrando-se em Ata as ocorrências até o momento da paralisação.

7.9 Se a participante deixar de contemplar algum item exigido para as demonstrações do sistema, será desclassificada, refazendo-se todos os procedimentos para a segunda colocada, e assim sucessivamente, até a apuração de uma proponente que atenda todos os pré-requisitos do Edital e deste Anexo.

7.10 Será juntada aos autos as manifestações sobre o atendimento ou não das especificações contidas no Edital, sendo que o prazo para a interposição de recurso terá início apenas após a decisão acerca do procedimento.

7.11 Verificado o atendimento das especificações do objeto e aprovada a demonstração da prova de conceito, a proponente será declarada vencedora definitiva.

8 – CONDIÇÕES DE HABILITAÇÃO

8.1 HABILITAÇÃO JURÍDICO

8.1.1 Registro comercial, no caso de empresa individual.

8.1.2 Ato constitutivo, estatuto ou contrato social consolidado, devidamente registrado, em se tratando de sociedade empresária ou cooperativa, devendo o estatuto, no caso das cooperativas, estar, na forma prevista nos artigos 27 e 28 da Lei Federal nº 12.690 de 19/07/2012 e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores.

8.1.3 Sendo o licitante Microempreendedor Individual, apresentar o CCMEI (Certificado do Cadastro do Microempreendedor Individual) expedido através do site portal do empreendedor: http://www.portaldoempreendedor.gov.br.

8.1.4 Inscrição no Registro Civil de Pessoas Jurídicas do ato constitutivo acompanhada dos nomes e endereço dos diretores em exercício, no caso de sociedades simples.

8.1.5 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.

8.2 REGULARIDADE FISCAL

8.2.1 Cadastro Nacional de Pessoa Jurídica (CNPJ).

8.2.2 Certidão conjunta de Tributos Federais e Dívida Ativa da União, nos termos da Portaria MF n° 358/14, de 05 de setembro de 2014.

8.2.3 Certidão de regularidade de débito com a(s) Fazenda(s) Estadual e/ou Municipal, da sede ou do domicílio do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame.

8.2.4 A prova de regularidade perante a Fazenda Estadual se dará por meio da Certidão Negativa de Débitos inscritos em Dívida Ativa, cujo prazo da expedição, para efeito de validade, deverá ser de até 180 (cento e oitenta) dias anteriores à data designada para a entrega dos envelopes, se outro prazo de validade não lhe constar expressamente.

8.2.5 A prova de regularidade perante a Fazenda Municipal se dará por meio da certidão negativa de débitos referentes a tributos mobiliários municipais.

8.2.6 Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço, mediante a apresentação em original ou cópia autenticada do "CRF"- Certificado de Regularidade Fiscal expedido pela Caixa Econômica Federal, dentro de seu prazo de validade.

8.2.7 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas “CNDT”, obtida em “http://www.tst.jus.br/certidao”, em atendimento a Lei 12.440/11, conforme o inc. V do art. 29 da Lei Federal nº 8.666/93.

9 - FORMA DE ENTREGA OU EXECUÇÃO DOS SERVIÇOS / FORMA DE PAGAMENTO

9.1 Os equipamentos deverão ser entregues dentro do horário de atendimento do Paço Municipal (08:00/17:00h), sendo que, o transporte e descarregamento no exato local indicado pela contratante ficam sob responsabilidade da contratada.

9.2 A entrega poderá ser fracionada ou em sua totalidade, mas deverá ser efetuada

somente mediante ordem de fornecimento.

9.3 Os pagamentos serão realizados através de boleto bancário com vencimento em até 30 (trinta) dias após emissão da Nota Fiscal.

9.4 No ato da entrega os produtos serão homologados pela Secretaria Municipal de Modernização e Comunicação.

9.5 Os produtos/serviços deverão ser entregues dentro do prazo de 15 dias corridos a contar da data da Ordem de Serviço/Pedido de Compra.

9.6 Os produtos ofertados ao objeto do certame deverão estar acondicionados unitariamente e devidamente identificados.

10 - LOCAL DE ENTREGA DOS PRODUTOS OU EXECUÇÃO DOS SERVIÇOS

Os equipamentos deverão ser entregues nos locais e datas de acordo ao cronograma expedido pela Secretaria de Modernização, Tecnologia e Inovação, no ato da emissão da ordem de serviço, localizada no Paço Municipal, situado à Praça José Rodrigues do Nascimento, 30 – Água Fria – Cajamar/SP, das 08:00h às 12:00h e das 13:00h às 17:00h, exceto aos feriados.

11 - PRAZO DE ENTREGA / VIGÊNCIA DO CONTRATO

11.1 Em caso, de Ata de registro de preço o contrato terá vigência de 12 (doze) meses, sendo vedada sua prorrogação.

11.2 Os produtos deverão ser entregues dentro do prazo de 30 dias corridos após a data da ordem de serviço/pedido de compra.

12 - VALIDADE DO PRODUTO OU GARANTIA DOS SERVIÇOS

12.1 Produtos de fabricação nacional deverão possuir garantia igual ou superior a 12 meses, quando não descritos em seus itens.

12.2 *Produtos de fabricação não nacional deverão possuir garantia igual ou superior a 12 meses, quando não descritos em seus itens e ficando o fornecedor responsável pela garantia do mesmo.*

13 - VISITA TÉCNICA / SUPORTE

13.1 O equipamento fornecido deverá contar com o suporte telefônico especializado da própria fabricante.

13.2 Deverá ser fornecido um telefone do tipo 0800 da fabricante para eventuais questionamentos.

13.3 Em casos, que venham ser necessários a troca do produto, a empresa responsável pelo fornecimento, deverá efetuar a troca e (ou) interagir para que a troca seja rápida, não gerando ônus para a Prefeitura Municipal.

13.4 Em caso de serviços, os interessados poderão visitar os locais de execução dos serviços até o dia anterior ao previsto para a entrega das propostas. A visita deverá ser agendada previamente junto à Secretaria Municipal de Modernização, Tecnologia e Informação, através do telefone (11) 4446-0011, ocasião em que será fornecido o Atestado de Visita em nome da empresa, indicando o responsável da licitante interessada em participar da Licitação.

13.5 Em caso de locação, sempre que necessário suporte aos equipamentos, a Secretaria de Modernização, Tecnologia e Informação, solicitará reparo pelo sistema de chamados fornecido pela própria empresa, indicando os locais em que estão os equipamentos a serem reparados, sejam eles em qualquer logradouro pertencente a departamentos da CONTRATANTE, bem como, horário e responsável/telefone por seu acompanhamento.

14 – AMOSTRA DOS PRODUTOS

Não será necessária a apresentação de amostras. Entende-se ainda que a vedação de amostra não trará prejuízos à competitividade no certame uma vez que se trata de uma solução.

15 – OBRIGAÇÃO DA CONTRATADA E DA CONTRATANTE

15.1 *A empresa CONTRATADA fornecerá equipamentos equivalente ou superior à configuração descrita neste termo.*

15.2 Será de responsabilidade da CONTRATADA, fornece um produto que esteja em linha de produção pelo fabricante.

15.3 Deverá seguir as recomendações INMETRO, caso se aplique à categoria.

15.4 Os Itens/Produtos de fabricação nacional deverão atendar as Normas Técnicas

Brasileiras e Regulamentações, nos quais se apliquem à categoria do produto solicitado.

15.5 O equipamento deverá seguir a categoria de uso (quando houver). Estando ela descrita no item, deverá por sua vez, coincidir com a categorização dos produtos da fabricante. Atendo assim, as necessidades descritas.

15.6 A empresa licitante deverá apresentar em sua proposta declaração formal, sob as penalidades cabíveis, quanto à disponibilidade dos equipamentos destinados à prestação dos serviços objeto da presente licitação.

15.7 A CONTRATADA somente irá fornecer os produtos, quando devidamente autorizados CONTRATANTE, fornecendo apenas equipamentos novos, sem uso anterior, em seu último estágio de revisão tecnológica, de software e hardware.

15.8 Os equipamentos deverão ser distribuídos e instalados, em até 10 dias úteis e, de acordo com a programação e necessidade nos locais estabelecidos pela CONTRATANTE.

15.9 Os licitantes deverão apresentar, ainda, dentro do ENVELOPE 01, catálogo técnico do fabricante, com a devida indicação da marca e modelo, que comprove todas as funcionalidades e características dos equipamentos solicitados no descritivo deste edital.

15.10 Agilizar a imediata correção das falhas apontadas pelo CONTRATANTE, concernente a execução do presente contrato;

15.11 Responsabilizar-se pelos encargos sociais, trabalhistas, previdenciários, fiscais, e comerciais resultantes da execução do contrato.

15.12 Declarar estar em dia com as obrigações trabalhistas, previdenciárias e fundiárias.

15.14 A CONTRATADA deverá manter, durante a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação, qualificação e condições de assinatura do contrato exigidas por ocasião da licitação que precedeu este ajuste, obrigando-se, ainda, a comunicar a unidade requisitante, toda e qualquer alteração dos dados cadastrais, para atualização, podendo a Administração requerer a sua comprovação, a qualquer tempo, durante a vigência do contrato.

16 – PENALIDADES

16.1 Multas para aquisição de produtos:

16.1.1 Pela inexecução total da obrigação objeto da licitação será aplicada multa equivalente a 20% (vinte por cento) do valor da Autorização de Fornecimento.

16.1.2 Pela inexecução parcial do ajuste será aplicada multa equivalente a 10% (dez por cento) do valor da Autorização de Fornecimento.

16.1.3 O atraso na entrega do objeto sujeitará a empresa vencedora à multa de mora de 0,5% (cinco décimos percentuais) do valor da Autorização de Fornecimento por dia de

atraso, até o 15° (décimo quinto) dia, após o que, poderá ser considerada inexecução total ou parcial do ajuste, conforme o momento da autorização de fornecimento.

16.1.4 O descumprimento do prazo de 24 (vinte e quatro) horas para reposição dos produtos entregues em desacordo com as especificações contidas neste Edital, para entrega da quantidade faltante de mercadoria solicitada pela Administração e para substituição da Nota Fiscal emitida com falhas, conforme previsto nos devidos itens deste Edital, acarretará a aplicação de multa diária equivalente a 1% (um por cento) do valor da Autorização de Fornecimento, até o limite de 15 (quinze) dias, quando será considerada a inexecução parcial. Considerar-se-á inexecução total do ajuste o atraso na entrega dos produtos por prazo igual ou superior a 30 (trinta) dias ou a reincidência da inexecução parcial do ajuste.

16.1.5 A não observância das quantidades solicitadas pela Administração na Autorização de Fornecimento sujeitará a empresa vencedora a multa no valor de 10% (dez por cento) do valor da Autorização de Fornecimento, sem prejuízo das demais sanções aplicáveis.

16.1.6 O fornecimento do objeto em desacordo com as especificações constantes do edital ou em níveis de qualidade inferior ao especificado no presente edital, sujeitará a empresa vencedora a multa de 10% (dez por cento) do valor total da Autorização de Fornecimento, sem prejuízo da substituição do objeto e demais sanções aplicáveis.

16.1.7 Para aplicação das penalidades descritas acima, será instaurado procedimento administrativo específico, sendo assegurado o direito ao contraditório e ampla defesa, com todos os meios a eles inerentes.

16.1.8. As multas são independentes e não eximem a empresa vencedora da plena execução do objeto contratado.

17 - DISPOSIÇÕES GERAIS/ INFORMAÇÕES COMPLEMENTARES

17.1. As propostas deverão ser apresentadas contendo obrigatoriamente a marca e o modelo do produto ofertado.

17.2. Os produtos ofertados ao objeto do certame deverão estar acondicionados unitariamente e devidamente identificados.

Cajamar/SP, 22 de junho de 2022.

André Luiz de Andrade Monteiro
Secretário Municipal de Modernização Tecnologia e Inovação