TERMO DE REFERÊNCIA COM FUNDAMENTO NA LEI FEDERAL Nº 14.133/2021

Órgão Requerente	**Secretaria de Administração e Finanças**
Responsável	**Luiz Carlos Previlato**
E-mail	**prefeituraquata@quata.sp.gov.br**

1- Definição do objeto:
Solicitamos abertura de processo de dispensa de licitação para fornecimento de licenças de software antivírus, incluindo suporte técnico e a implementação inicial, conforme exposto abaixo:

ITEM	CÓDIGO	PRODUTO / DESCRIÇÃO	UNID	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	598.004.021	CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE 215 LICENÇAS DE SOFTWARE ANTIVÍRUS, INCLUINDO SUPORTE TÉCNICO E ATUALIZAÇÕES (por um período de 12 meses)	MÊS	12	R$ 2.000,00	R$ 24.000,00
2	598.004.022	IMPLEMENTAÇÃO DO SOFTWARE ANTIVÍRUS INCLUINDO CAPACITAÇÃO E CONFIGURAÇÃO INICIAL	SV	1	R$ 8.400,00	R$ 8.400,00

1.2. Classificação do objeto:
Licenças de software antivírus.

1.3. Critério de Julgamento:
Menor preço global, devido o serviço de implementação estar atrelado às licenças de antivírus.

1.4. Justificativa para dispensa dos documentos solicitados:
É dispensado projeto básico por se tratar de licenças de software antivírus.
Análise de risco: A ausência de uma solução de antivírus corporativo pago pode deixar a rede suscetível à contaminação por vírus, malwares e outras ameaças cibernéticas. Esses incidentes podem resultar na criptografia de dados críticos, invasão de bases de dados, perda permanente de informações importantes, vazamento de dados sensíveis e até na interrupção total das atividades administrativas e operacionais do município. Redes distribuídas da prefeitura tornam-se ainda mais vulneráveis quando não há proteção centralizada, facilitando o acesso indevido por cibercriminosos. Soluções gratuitas de antivírus, em geral, não oferecem recursos avançados necessários para ambientes institucionais, como gerenciamento centralizado, proteção contra ransomware, análise comportamental, controle de dispositivos e resposta a incidentes. Além disso, a legislação de proteção de dados pessoais exige que os agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger as informações contra acessos não autorizados e incidentes de segurança. Nesse contexto, a ausência de solução adequada de antivírus configura uma falha relevante de segurança. Dessa forma, a adoção de uma solução profissional de proteção digital reduz significativamente a exposição a riscos, fortalece a integridade dos sistemas institucionais e contribui para a continuidade e confiabilidade dos serviços públicos.

1.5. Valor total:
O valor total estimado para execução do objeto descrito acima é de aproximadamente R$ 32.400,00 (trinta e dois mil e quatrocentos reais), considerando os valores obtidos na pesquisa de mercado, em empresas desse segmento localizadas no estado, via e-mail e telefone; além de considerar pesquisa em sites eletrônicos de antivirus, levando em conta o valor cobrado por assinatura/máquina.

1.6. Registro de Preços: ( ) SIM (x) NÃO
Dispensa de Licitação

2- Justificativa:
A aquisição das licenças de antivírus é essencial para assegurar a proteção dos computadores e servidores do Município de Quatá - SP, prevenindo contaminações por vírus, malwares e demais ameaças cibernéticas que

possam comprometer o sigilo, a integridade e a disponibilidade das informações institucionais. Diante do crescente volume de uso de e-mails, navegação na internet e circulação de dados, torna-se indispensável a adoção de uma solução de segurança capaz de mitigar riscos e garantir a continuidade dos serviços. A contratação das licenças proporciona maior proteção à infraestrutura tecnológica, evitando incidentes que possam impactar o funcionamento das atividades administrativas. Assim, a aquisição das licenças de antivírus configura-se como medida imprescindível para manter a confiabilidade, integridade e disponibilidade das informações e assegurar a continuidade das operações da Prefeitura Municipal de Quatá. A contratação de 215 licenças de software antivírus, com suporte pelo período de 12 meses, é necessária para atender integralmente o parque computacional da Prefeitura Municipal de Quatá-SP, abrangendo computadores, notebooks, terminais de atendimento e servidores utilizados pelos diversos setores administrativos.

3-Dotação orçamentária (Lei de responsabilidade fiscal LC101/00 art. 16 em especial)

FICHA	FUNÇÃO PROGRAMÁTICA	FONTE
058	Manutenção Unid. Tecnologia da informação (Serviço)	Recurso Próprio

3.1. Origem do recurso:
Recurso Próprio

4-Condições de habilitação:
Empresa deve estar apta para contratação pública, com CNPJ ativo e possuir CNAE compatível com o produto/serviço solicitado. Deverá ser apresentado Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, que comprove o fornecimento dos serviços ofertados, devendo estar explícito os tipos de serviço fornecidos.

5-Condições de execução do objeto:
O software antivírus deve possuir central única de gerenciamento; as configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de dispositivos e controle de aplicações deverão ser realizadas através da mesma central.
O produto deverá possuir no mínimo os seguintes módulos e funções:
Prover segurança para estações de trabalho, notebooks, servidores, sejam em ambientes físicos ou virtualizados:

- ✓ Possuir console central única de gerenciamento na nuvem (cloud) das configurações do Antivírus, AntiSpiware, Firewall, Detecção de intrusão, Controle de Dispositivos e Controle de Aplicações;
- ✓ O produto deverá ter a capacidade de remoção do software antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
- ✓ O produto deverá possuir no mínimo os seguintes módulos:
  - ■ Módulo para estações físicas, laptops e servidores;
  - ■ Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
- ✓ Utilizar o conceito de heurística;
- ✓ Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
- ✓ Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
- ✓ Oferecer inventário de softwares;
- ✓ Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado da execução do mesmo no ambiente de produção;
- ✓ Oferecer proteção por base de assinaturas.

Console de gerenciamento:

- ✓ Instalação e configuração

- ✓ Deve ser fornecido como um appliance virtual ou executável para instalação em servidores ou Console com gerenciamento em nuvem (cloud);
- ✓ Deverá suportar no mínimo os seguintes Hypervisors: Microsoft Hyper-V ou sistemas virtualizados;
- ✓ Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
- ✓ Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais;
- ✓ O mecanismo de varredura deverá estar disponível para download separadamente;
- ✓ A solução deverá permitir a inclusão de um módulo de balanceamento para casos em vários servidores terem a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
- ✓ Deve ser totalmente em português.

Características Gerais:

- ✓ Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;
- ✓ Permitir que o administrador escolha qual pacote será atualizado;
- ✓ As notificações dever ser destacadas como item não lido, enviar e-mail para o administrador;
- ✓ No mínimo enviar notificações com as seguintes frases:
  - ■ Problemas com licenças,
  - ■ Alertas de Surto de Vírus,
  - ■ Máquinas desatualizadas,
  - ■ Eventos de Antimalware;
- ✓ Painel para monitoramento baseado em “portlets” para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- ✓ Inventário de Rede;
- ✓ Possuir no mínimo as integrações abaixo: Múltiplos domínios Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
- ✓ Possuir a possibilidade de definição de sincronização com o Active Diretory em horas;
- ✓ Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
- ✓ Descoberta de rede para máquinas em grupo de trabalho definidos pelo administrador;
- ✓ Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP e MAC;
- ✓ Possibilitar a instalação remota e desinstalação remota do antivírus;
- ✓ Possibilitar a configuração de pacotes de instalação do produto antivírus;
- ✓ Possuir tarefas remotas e configuráveis de Scan;
- ✓ Possuir tarefa de reinicialização remota de estação de trabalho ou servidor;
- ✓ Assinar políticas para no mínimo os níveis: computador, máquina virtual ou possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política de Assinada, último status de malware;

Politicas:

- ✓ Modelo único para todos os equipamentos, seja físico ou virtual;
- ✓ Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
- ✓ Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

Relatórios:

- ✓ Relatório para cada serviço de segurança;
- ✓ Facilidade usar e visualização simplificada;
- ✓ Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

- ✓ Filtros de agendamento de relatório;
- ✓ Arquivo com todas as instâncias de relatórios agendados;
- ✓ Possibilitar exportar os relatórios nos formatos .pdf e/ou .csv.;
- ✓ Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução;

Quarentena:
- ✓ Restauração remota, com configuração de localidade e deleção;
- ✓ Criação e exclusão para arquivos restaurados;

Usuários:
- ✓ Administração baseada em regras;
- ✓ Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador – Gerente dos componentes da solução, Administrador de Rede – Gerente dos serviços de segurança;
- ✓ Deverá ser possível customizar um tipo de usuário;
- ✓ Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;
- ✓ Logs de Utilização;
- ✓ Registrar as ações do usuário no console de gerenciamento;
- ✓ Detalhar cada ação do usuário;
- ✓ Permitir busca complexa baseada em ações do usuário, intervalo de tempo;

Controle de Usuário
- ✓ Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso a internet, Bloqueio de acesso a aplicações definidas pelo administrador;

Certificado de Segurança:
- ✓ Deverá prover o acesso via HTTPS;
- ✓ Deverá permitir a importação de certificados digitais;
- ✓ O gerenciamento e a comunicação com dispositivos móveis, deverão ser feito de forma segura utilizando certificados digitais.

Proteção para estações de trabalho e servidores físicos:
- ✓ Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Híbrido, Scan Central;
- ✓ Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso à internet e instalar o antivírus sem o módulo de firewall;
- ✓ Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64 bits, Windows 7 32 e 64 Bits;
- ✓ Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2022, Windows Server 2022 Core, Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2;
- ✓ Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubunto Server 14.04 LTS ou superior, Red Hat Enterprise Linus / Cent OS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior; Amazon Linux AMI 2016.09 ou superior;

Gerenciamento e instalação remota:
- ✓ Deverá permitir ao administrador customizar a instalação;
- ✓ A instalação deverá ser possível com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerência web;

- ✓ Deverá gerar um relatório com as estações instaladas e as faltantes da instalação;
- ✓ A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;
- ✓ Através da console, o administrador poderá enviar uma política única para configurar o antivírus;
- ✓ O console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente se for para 32 ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- ✓ O Agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado;

Proteção para Estações e Servidores Virtuais:

- ✓ O agente deverá ser dedicado e preparado para ambientes virtualizados e incluir no mínimo as seguintes funcionalidades: Interface simples de administração (WEB) com console para administração de todos os servidores virtuais instalados, Scan distribuído para balanceamento de recursos de CPU em máquinas virtuais com o mesmo hypervisor;
- ✓ Deverá fornecer segurança para a imagem, mesmo que ela não esteja ligada (off-line);
- ✓ A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters
- ✓ da VMWare;
- ✓ Deverá proteger em tempo real e agendado as máquinas virtuais;
- ✓ O scan não deverá impactar o desempenho do ambiente virtualizado;
- ✓ Instalação remota da console de gerenciamento;

Detecção e Remoção:

- ✓ O Antivírus deverá realizar a detecção do vírus, spyware, adwares, malwares e aplicativos potencialmente indesejados (APIs) em tempo real;
- ✓ Deverá realizar scan baseado em assinatura e heurística, ambos configuráveis;
- ✓ Realizar scan em mídias removíveis, arquivos, diretórios, discos locais e unidades de rede;
- ✓ Possibilitar ao administrador configurar o horário de scan;
- ✓ Os eventos de ameaças detectados deverão ser enviados para o servidor de gerenciamento;

Requisitos de atualização:

- ✓ O administrador deverá escolher a periodicidade da atualização dos arquivos de assinaturas (ex. 1 hora, 2 horas, 6 horas);
- ✓ Deverá permitir que as estações, após duas tentativas de atualização com o servidor de gerenciamento, consultem o fabricante do antivírus par atualização dos arquivos de assinaturas;
- ✓ A atualização deverá ser incremental e deverá ser armazenada para eventuais problemas de conexão;
- ✓ O software deverá permitir o download de atualizações offline;
- ✓ A atualização deverá ser enviada para as máquinas off-line;

Controle de Aplicações:

- ✓ Possibilitar o bloqueio de aplicações baseado em perfil;
- ✓ Aplicação e verificação de assinatura digital e hash de aplicação para inclusão ou exclusão de execução;

Controle de Dispositivo:

- ✓ Possibilitar o bloqueio de dispositivos;
- ✓ Suporte a, no mínimo, bloqueio dos seguintes dispositivos: USB, Firewire, SD, etc;
- ✓ Possibilitar o desbloqueio temporário do dispositivo por senha;

Prova de Conceito;

- ✓ Deverá fornecer manual técnico de instalação e configuração em português;

- ✓ Permitir motor de varredura local, no servidor de rede ou em nuvem a fim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo scaneada;
- ✓ Proteção para caixa de e-mail;
- ✓ Fornecer proteção para ambiente Exchange;
- ✓ Oferecer tecnologia para proteção contra spam;
- ✓ Oferecer análise comportamental e proteção para zero-day;
- ✓ Oferecer proteção contra vírus e tentativas de phishing;

Criptografia;

- ✓ Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de com módulo de Criptografia presente na mesma Console do Antivírus;
- ✓ Deverá utilizar quando necessário serviços de criptografia através de agentes nativos da estação de trabalho baseado em Windows (BitLocker) ou Mac (File Vault);
- ✓ Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- ✓ Deverá ser compatível com: macOS Big Sur (11.x) ou superior;

Proteção Avançada;

- ✓ Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques em arquivos e malware sofisticado, devendo ser detectado e bloqueados antes de serem executados;
- ✓ Detectar e parar, bloquear e interromper malwares sem arquivos;
- ✓ Parar os ataques com base em macros e scripts. Analisar scripts, como PowerShell, WMI, intérpretes de Javascript, etc, bem como adicionar técnica de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos;

Reparo e Resposta automatizada a ameaças;

- ✓ Quando uma ameaça é detectada, a ferramenta deve neutraliza-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes;
- ✓ Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional;
- ✓ Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente;
- ✓ Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedem kits de exploração, além de bloquear tráfego suspeito na web. Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos;

Proteção para caixa de e-mail:

- ✓ Fornecer proteção para ambiente Exchange
- ✓ Oferecer tecnologia para proteção contra spam;
- ✓ Oferecer análise comportamental e proteção para zero-day;
- ✓ Oferecer proteção contra vírus e tentativas de phishing;

Machine Learning;

- ✓ As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados;
- ✓ A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosos devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos, ações evasivas e conexões a centro de comando e controle;

Sandbox

- ✓ Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso" o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas;

Antiexploit Avançado

- ✓ Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja: Flash ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (returnoriented programming) etc;

Inspetor de Processo

- ✓ O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativa de ocultar o tipo de processo, executar código no espaço de outro processo (sequestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem, etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware;

Detecção e Resposta – EDR

- ✓ Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades XEDR para detectar ataques avançados em vários terminais em infraestruturas hibridas (estações de trabalho ou servidores executando vários sistemas operativos);
- ✓ Deverá analisar continuamente os riscos, usando centenas de fatores para descobrir e priorizar as melhores configurações para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamento dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login e sites, gerenciamento de senhas inadequadas, uso de dispositivos USBs comprometidos, infecções recorrentes, etc.;

Do Treinamento

- ✓ O treinamento objetiva a transmissão dos conhecimentos necessários para que equipe técnica da CONTRATANTE possa administrar e operar a solução contratada, e treinar os usuários finais, e deverá atender os seguintes requisitos:
  - ■ O treinamento será realizado por meio de turma online nas dependências do CONTRATANTE, à distância com o uso de recursos audiovisuais;
  - ■ O treinamento deverá abordar as informações necessárias aos administradores desde as operações básicas até as mais avançadas.

- Toda e qualquer atualização de funções e ou adição de novos módulos na solução, deverá ser feito novo treinamento da equipe técnica da CONTRATANTE, para transmissão dos conhecimentos;
- Os horários e datas dos treinamentos serão definidos pela equipe técnica do CONTRATANTE e comunicado à CONTRATADA com antecedência mínima de 10 (dez) dias consecutivos;

Funções Gerais

- ✓ Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
- ✓ Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;
- ✓ Deverá fazer scan em tempo real automático;
- ✓ Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
- ✓ Escaneamento de comportamento heurístico;
- ✓ Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como: Discos Externos, Pen-Drivers,
- ✓ Deverá permitir a escolha e configuração de pastas a serem escaneada;
- ✓ Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
- ✓ Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
- ✓ O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
- ✓ Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser
- ✓ instalado/desinstalado nas estações de trabalho;
- ✓ O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
- ✓ Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
- ✓ Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- ✓ Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- ✓ Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- ✓ Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

Requisitos mínimos suportados pelo Sistema:

- ✓ Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, 8, 10 e superior.
- ✓ Sistemas Operacionais Servidores: Windows Server 2019 e superior , e Linux.

Posicionamento de mercado

- ✓ O fabricante/desenvolvedor da solução de proteção de endpoints, deverá estar presente no quadrante do Gartner mais recente, de forma que possa ser adquirida uma solução mais confiável, madura e robustas do mercado, contando com a prestação de serviços qualificados, potencializando o sucesso desta contratação.
- ✓ Vale ressaltar que a utilização do quadrante do Gartner, é prática comum entre as contratações públicas de TIC e que a adoção deste requisito, não fere os princípios da isonomia e da competitividade, visto que a maioria dos principais fabricantes/desenvolvedores constam no último quadrante em vigência, no momento da escrita deste Termo.
- ✓ Sendo assim, o fabricante/desenvolvedor desta solução deverá constar no quadrante para EPP (plataformas de proteção de endpoint) do Gartner mais recente, em qualquer categoria, seja de líderes, visionários, competidores de nicho ou desafiadores.

5.1 – Prazo e forma de entrega/execução:

A contratação deverá iniciar mediante comum acordo entre o Setor de TI com a empresa, que será após a formalização do contrato, com vigência prevista de 12 meses, podendo ser prorrogada conforme necessidade

da Administração. A implementação do software antivírus, incluindo capacitação e configuração inicial, ocorrerá no início da vigência,definida em comum acordo, enquanto o suporte e a manutenção serão prestados continuamente ao longo de todo o período contratual, de acordo com as demandas do Setor de Administração e Finanças e do Setor de Tecnologia da Informação.
A central de gestão do software antivírus da contratada, objeto desta contratação, deverá estar disponível 24 (vinte e quatro) horas por dia 7 (sete) dias da semana, durante o período de vigência do contrato, salvaguardados os casos de interrupções programadas. Os serviços deverão ser prestados de forma ininterrupta. Na hipótese de ocorrência de interrupções total de operação do serviço, as falhas deverão ser corrigidas e o serviço restabelecido em no máximo 8 (oito) horas úteis. A CONTRATADA deverá garantir suporte técnico, seja próprio ou do fabricante, sempre que necessário, quando reportado incidentes ou requisições pelo CONTRATANTE. A CONTRATADA, deverá disponibilizar um canal digital de suporte técnico para que os incidentes e requisições sejam devidamente registrados. As interrupções programadas nos serviços de gestão centralizada deverão ser comunicadas à CONTRATANTE com antecedência mínima de 3 (três) dias. A quebra ou violação do sigilo de dados, a qualquer momento, ensejará a Rescisão Unilateral do CONTRATO, sem prejuízo de outras sanções cabíveis, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.
As licenças serão recebidas, definitivamente, após aceite do fiscal do contrato ou Setor de TI, com base na validação do funcionamento. A CONTRATADA deverá fornecer todos os materiais, mão-de-obra, equipamentos, transporte necessários à execução dos serviços.
A entrega efetiva do serviço e a ativação das licenças deverão ser coordenadas com os técnicos do Departamento de Tecnologia da Informação. O agendamento prévio deverá ser realizado através do e-mail ti@quata.sp.gov.br ou pelo telefone (18) 3366-1008. A vigência da licença terá início a partir da ativação no ambiente tecnológico da Prefeitura Municipal de Quatá, mediante validação e aprovação do fiscal do contrato. Os serviços poderão ser rejeitados caso estejam em desacordo com as especificações, devendo a contratada realizar as correções necessárias. Eventuais penalidades serão aplicadas, se for o caso, conforme previsto na Lei nº 14.133/2021. A contratante se compromete a cumprir as disposições previstas no Termo de Referência, fornecer as informações necessárias para a execução do objeto, designar servidores responsáveis pelo recebimento e fiscalização, garantir os recursos orçamentários e acompanhar a execução contratual.

5.2 – Local de entrega/execução, responsável pelo recebimento do objeto:
A entrega das licenças de software antivírus, bem como os serviços de implementação e capacitação, ocorrerão de forma remota ou presencial, conforme necessidade do Setor de Tecnologia da Informação da Prefeitura Municipal de Quatá. O setor de T.I. poderá solicitar capacitação presencial sempre que julgar necessário, devendo a contratada atender às convocações dentro dos prazos acordados. O recebimento provisório será realizado no ato da entrega, junto à nota fiscal, pelos responsáveis pelo acompanhamento e fiscalização do contrato — Ana Paula dos S. Braatz Vieira e Rodrigo da Silva Costa — que farão a verificação preliminar da conformidade com o Termo de Referência. Caso sejam identificadas inconsistências, o serviço poderá ser rejeitado total ou parcialmente, devendo a contratada realizar a substituição/correção no prazo de até 5 (cinco) dias úteis. O recebimento definitivo ocorrerá em até 5 (cinco) dias úteis após análise completa da documentação e validação da conformidade técnica, podendo este prazo ser prorrogado de forma justificada. O recebimento, provisório ou definitivo, não exime a contratada de suas responsabilidades legais e contratuais relacionadas à execução do objeto. No caso de visitas presenciais, o endereço será: Rua Carlos Bleinroth N.º 94 - na entrada da cidade de Quatá-SP, CEP: 19780-025. Esclarecimentos adicionais poderão ser solicitados ao setor responsável durante o horário de atendimento (das 07:00h às 11:00h e das 13:00h às 17:00h), em dias úteis, obedecendo ao calendário municipal. Os responsáveis pelo recebimento e fiscalização serão Ana Paula dos S. Braatz Vieira e Rodrigo da Silva Costa - Analistas de Tecnologia e Comunicação (T.I.C).

5.3 – Condições de garantia e assistência técnica:
A empresa deve garantir o pleno funcionamento do software antivírus, garantir a disponibilidade do mesmo 24 (vinte e quatro) horas por dia 7 (sete) dias da semana, durante o período de vigência do contrato, salvaguardados os casos de interrupções programadas.

5.4 – Prazo de vigência da contratação:
Vigência do contrato de 12 meses, podendo ser prorrogado por igual período.

5.5- Demais informações necessárias para a execução do objeto:
No caso de prorrogação do contrato, o item 2 (implementação, pago de forma única após a instalação) não será cobrado novamente, pois o software já estará implementado, o serviço só será continuado, devendo ser cobrado somente as mensalidades.
A Prefeitura de Quatá poderá recusar o recebimento do objeto que não atenda as normas e os padrões mínimos exigidos e aplicados ao mesmo, respondendo a empresa vencedora INTEGRALMENTE pelo custo de suas substituições tantas vezes quantas forem necessárias. A empresa vencedora se responsabilizará por todos os custos, diretos e indiretos causados por incidentes e apurados na hipótese da incidência do previsto no Edital.

6-Obrigações da contratada:
-Fornecer o objeto de acordo com as especificações e quantitativos em conformidade com as condições deste instrumento, obrigando-se a substituir aquele(s) não achado(s) conforme(s) pela CONTRATANTE;
-Responder, integralmente, por perdas e danos que vier a causar a esta Prefeitura ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de seus prepostos, independentemente de outras cominações legais a que estiver sujeita;
-Fornecer o serviço e adotar todas as medidas preventivas no sentido de se minimizar incidentes ou danos que venham a comprometer a qualidade do serviço fornecido;
-Manter, pessoal e equipamentos suficientes para o atendimento;
-Assumir inteira responsabilidade quanto à qualidade do fornecimento;
-Fornecer o objeto obedecendo às quantidades requisitadas, qualidade, horários, prazos e locais estabelecidos para a prestação dos serviços;
-Cumprir todas as demais cláusulas do contrato;
-Prestar os serviços e cumprir integralmente as obrigações relacionadas com a contratação descritas neste Termo de Referência e Contrato;
-Fornecer mão de obra especializada para a execução dos serviços;
-Prestar todos os esclarecimentos solicitados pelo CONTRATANTE, atendendo prontamente a todas as reclamações;
-Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, os serviços em que forem verificados vícios, defeitos ou incorreções;
-Registrar as ocorrências havidas durante a execução do Contrato/Termo, dando plena ciência ao CONTRATANTE, bem como respondendo integralmente por sua omissão;
-Disponibilizar para o CONTRATANTE um atendimento personalizado e imediato, com fornecimento de números de telefone, e-mail ou outra forma de comunicação para abertura de chamados;
-Providenciar a imediata correção das deficiências apontadas pelo CONTRATANTE;
-Responder, integralmente, por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, quando esses tenham sido ocasionados por seus empregados durante a entrega do serviço, independentemente de outras cominações contratuais ou legais a que estiver sujeita;
-Comunicar ao CONTRATANTE, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;
-Apresentar os documentos de cobrança, nota(s) fiscal(is) com a descrição completa dos serviços.
-Manter, durante toda a execução contratual, compatibilidade com mas obrigações assumidas;
-Manter sigilo de informações às quais porventura venha a ter acesso;
-Realizar a implementação do software antivírus, incluindo capacitação e configuração inicial;
-Prestar suporte e a manutenção continuamente ao longo do período contratual;
-A contratada deverá possuir técnico certificado pelo Fabricante da solução para comprovar qualificação para execução do serviço durante todo período contratual;

-A contratada deverá atender prontamente todas as solicitações, esclarecimentos e orientações emitidas pelo Setor de T.I e seus representantes, conforme as obrigações previstas no contrato vigente.
-A CONTRATADA deverá fornecer todos os materiais, mão-de-obra, equipamentos, transporte necessários à execução dos serviços;

7-Gestão e Fiscalização:
Gestão: Luiz Carlos Previlato - Secretário de Administração e Finanças
Fiscalização: Ana Paula dos S. Braatz Vieira / Rodrigo da Silva Costa - Analista de Tecnologia e Comunicação (T.I.C)

8- Outras informações:
O pagamento será realizado no prazo de até 30 (trinta) dias contados a partir do recebimento da nota fiscal eletrônica de serviços, por meio de ordem bancária, para crédito em banco, agência e conta corrente jurídica indicado pela CONTRATADA.
- contabilidade.nf@quata.sp.gov.br
- prefeitura@quata.sp.gov.br
- ti@quata.sp.gov.br
- Tel: (18) 3366-1008

Quatá/SP, 05 de Janeiro de 2026.

Luiz Carlos Previlato
Secretário de Administração e Finanças

Ana Paula dos S. Braatz Vieira / Rodrigo da Silva Costa
Analista de Tecnologia e Comunicação (T.I.C)

Evandro Alves
Escriturário/Elaborador TR