Proc. Administrativo 2- 639/2024

De: Jozué W. - TI

Para: GP - Gabinete do Prefeito

Data: 19/07/2024 às 15:11:07

Setores envolvidos:

GP, TI, SEAF

Processo Licitatório - Solução Antivírus

Boa tarde!

Segue documentação para assinatura, aquisição de Solução Antivírus.

–

Jozué Wuicik
Departamento de Informática

Anexos:
Termo_de_Referencia_Antivirus.pdf

xanxere.sc.gov.br
+55 49 3441-8500
Rua José de Miranda Ramos, 455, Centro,
Xanxerê - Santa Catarina, CEP 89820-000

TERMO DE REFERÊNCIA

Unidade Requisitante: Secretaria de Administração e Finanças

Ordenador da despesa: Carlos Alberto Peretti

(01) Objeto

Aquisição de **Licenças Antivírus para** estações de trabalho e servidores, com segurança avançada baseada em Inteligência Artificial (IA) e Aprendizado de Máquina (Machine Learning) de próxima geração, incluindo suporte técnico e atualizações pelo período de 36 (trinta e seis) meses, **sendo que a ferramenta contratada deve ser 15 licenças para implantação em Windows server 2008/2012/2016 e superior, 125 para estações Windows 7,8,10,11 totalizando 140 licenças.**

(02) Motivação/Justificativa

A contratação proposta é essencial para garantir a segurança e a proteção dos dados produzidos e armazenados nos servidores do município de Xanxerê. Além disso, visa minimizar e prevenir a contaminação dos serviços e sistemas informatizados por programas ou atividades digitais maliciosas, assegurando o nível adequado e desejado de proteção de dados e informações do Município.

A aquisição desta solução permitirá ao departamento de informática do município manter os níveis de segurança exigidos para a proteção das informações que trafegam na rede e implementar políticas necessárias para garantir que essas informações sejam acessadas e manipuladas apenas por pessoas autorizadas. A otimização da infraestrutura de segurança dos dados armazenados na instituição também proporcionará maior confiabilidade nas informações trafegadas e armazenadas nas estações de trabalho e nos diversos sistemas corporativos do Município.

(03) Especificações técnicas:

Contratação de empresa para fornecimento de licenças de software de antivírus e suporte pelo período de 3 anos

xanxere.sc.gov.br
+55 49 3441-8500
Rua José de Miranda Ramos, 455, Centro,
Xanxerê - Santa Catarina, CEP 89820-000

1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.

1.1. Possuir console 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 console;

1.2. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

1.3. O produto deverá possuir no mínimo os seguintes módulos:

1.4. Console de Gerenciamento fornecendo funcionalidades de gestão;

1.5. Módulos para estações físicas, laptops e servidores;

1.6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

1.7. Utilizar o conceito de heurística;

1.8. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);

1.9. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;

1.10. Oferecer inventário de softwares;

1.11. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;

1.12. Oferecer proteção por base de assinaturas.

2. Console de Gerenciamento

2.1. Instalação e configuração

2.2. Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).

2.3. Deverá suportar no mínimo os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box;

2.4. Microsoft Hyper-V, Red Hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;

2.5. Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;

2.6. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;

2.7. O mecanismo de varredura deverá estar disponível para download separadamente;

2.8. A solução deverá permitir a inclusão de um módulo de balanceamento para casos em vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);

2.9. Deve ser totalmente em idioma português.

3. Características Gerais

3.1. Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;

3.2. Permitir que o administrador escolha qual o pacote será atualizado;

3.3. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;

3.4. No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware;

3.5. Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;

3.6. Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;

3.7. Inventário da Rede

3.8. Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;

3.9. Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

3.10. Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;

3.11. Descoberta de rede para máquinas em grupo de trabalho;

3.12. Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;

3.13. Possibilitar a instalação remota e desinstalação remota do antivírus;

3.14. Possibilitar a configuração de pacotes de instalação do produto de antivírus;

3.15. Possuir tarefas remotas e configuráveis de Scan;

3.16. Possuir tarefa de reinicialização remota de estação ou servidor;

3.17. 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 Assinada, último status de malware.

xanxere.sc.gov.br
+55 49 3441-8500
Rua José de Miranda Ramos, 455, Centro,
Xanxerê - Santa Catarina, CEP 89820-000

4. Políticas

4.1. Modelo único para todos os equipamentos, seja físico ou virtual;

4.2. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

4.3. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

5. Relatórios

5.1. Relatório para cada serviço de segurança;

5.2. Facilidade de usar e visualização simplificada;

5.3. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

5.4. Filtros de agendamento de relatórios;

5.5. Arquivo com todas as instâncias de relatório agendados;

5.6. Exportar o relatório nos formatos “.pdf” e/ou “.csv”;

5.7. Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

6. Quarentena

6.1. Restauração remota, com configuração de localidade e deleção;

6.2. Criação e exclusão para arquivos restaurados.

7. Usuários

7.1. Administração baseada em regras;

7.2. Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;

7.3. Relatório - Monitora e cria relatórios;

7.4. Deverá ser possível customizar um tipo de usuário;

7.5. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;

7.6. Logs de utilização;

7.7. Registrar as ações do usuário na console de gerenciamento;

7.8. Detalhar cada ação do usuário;

7.9. Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

8. Certificado de Segurança

8.1. Deverá prover o acesso via HTTPS;

8.2. Deverá permitir a importação de certificados digitais;

8.3. O gerenciamento e a comunicação com dispositivos móveis devem ser feitos de forma segura utilizando certificados digitais.

9. Proteção para Estações de Trabalho e Servidores Físicos

9.1. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;

9.2. Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso à internet; (Windows Workstation), Instalar o antivírus sem o módulo de firewall; (Windows Workstation);

9.3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 7 (32 e 64 Bits), Windows 8 (32 e 64 Bits), Windows 10 e 11 (32 e 64 Bits) ou versões mais recentes;

9.4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 ou versões mais recentes;

9.5. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Red Hat Enterprise Linux, Cent OS 5.6 ou superior, Ubuntu 10.04 LTS ou superior, SUSE Linux Enterprise Server 11 ou superior, OpenSUSE 11 ou superior, Fedora 15 ou superior, Debian 5.0 ou superior.

10. Gerenciamento e Instalação Remota

10.1. Deverá permitir ao administrador customizar a instalação;

10.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;

10.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

10.4. 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;

10.5. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;

10.6. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, edição, criação, logout, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

10.7. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado.

11. Proteção para Estações e Servidores Virtuais

11.1. Proteção de antivírus dedicado para ambientes virtuais;

11.2. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;

11.3. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;

11.4. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;

11.5. O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM.

12. Funções Gerais

12.1. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

12.2. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida.

13. Requisitos Mínimos suportados pelo Sistema.

13.1. Plataformas de Virtualização: VMware vSphere ESX 5.0 ou superior, VMware vCenter Server 4.1 ou superior, VMWare Tools 8.6.0, Citrix XenDesktop 5.0 ou superior, Xen Server 5.5 ou superior, Citrix VDI-in-a-Box 5, Microsoft Hyper-V Server 2008 R2, 2012, Oracle VM 3.0, Red Hat Enterprise Virtualization 3.0;

13.2. Sistemas Operacionais desktops (32 e 64 Bits): Windows 7 / 8 /10 e 11;

13.3. Sistemas Operacionais Servidores: Windows Server 2008/2008 R2, 2012/2012 R2 / 2016 / 2019 / 2022, Linux Red Hat Enterprise, CentOS 5.6 ou superior, Ubuntu 10.04 LTS ou superior, SUSE Linux Enterprise Server 11 ou superior, OpenSUSE 11 ou superior, Fedora 15 ou superior, Debian 5.0 ou superior.

14. Componentes e Funcionalidade do Antivírus Geral

14.1. Deverá fazer scan em tempo real automático;

14.2. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

14.3. Escaneamento de comportamento heurístico;

14.4. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como: CD/DVD, discos externos, pen-drivers. Deverá permitir a escolha e configuração de pastas a serem escaneadas;

14.5. 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;

14.6. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;

14.7. 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 nas estações de trabalho;

14.8. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;

14.9. O módulo de firewall deverá permitir configurar o modo invisível, a nível de rede local ou internet, nas estações de trabalho;

14.10. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

14.11. Deverá fazer a remoção automática de arquivos antigos, predefinidos pelo administrador;

14.12. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;

14.13. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;

14.14. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas.

15. Controle de Usuário

15.1. Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso à internet, bloqueio de acesso às aplicações definidas pelo administrador.

16. Controle do Dispositivo

16.1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

16.2. Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CD-ROM/DVD-ROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;

16.3. Deverá permitir regras de definição de bloqueio/desbloqueio;

16.4. Deverá permitir regras de exclusão.

17. Atualização

17.1. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;

17.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

17.3. Permitir atualizações de assinatura de hora em hora;

17.4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

18. Proteção para caixa de e-mail:

18.1. Fornecer proteção para ambiente Exchange;

18.2. Oferecer tecnologia para proteção contra spam;

18.3. Oferecer análise comportamental e proteção para zero-day;

18.4. Oferecer proteção contra vírus e tentativas de phishing.

19. Criptografia

19.1. Possibilidade de criptografia de disco através da console de gerenciamento, seja em nuvem ou on-premise, com módulo de criptografia presente na mesma console do antivírus;

19.2. Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);

19.3. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

19.4. Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.

20. **Proteção Avançada NGAV**

20.1. 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 sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados;

20.2. Detectar e parar, bloquear e interromper malwares sem arquivos;

20.3. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc., bem como adicionar técnicas 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;

20.4. Reparo e resposta automatizada a ameaças;

20.5. Quando uma ameaça é detectada, a ferramenta deve neutralizá-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;

20.6. Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional;

20.7. Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente;

20.8. 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;

20.9. Deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web;

20.10. Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.

21. Machine Learning

21.1. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados;

21.2. 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. Minimizando desta forma os falsos positivos, as ações evasivas e as conexões aos centros de comando e controle.

22. Sandbox

22.1. 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. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

23. Antiexploit Avançado

23.1. 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 *(return - oriented programming),* etc.

24. Inspetor de processo

24.1. 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 tentativas 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.;

24.2. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas;

24.3. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

25. **Detecção e Resposta - EDR**

25.1. Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho, servidores ou containers executando vários sistemas operativos);

25.2. Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento;

25.3. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de dispositivos USB(s) comprometidos, infecções recorrentes, etc.

26. Obrigações da Contratada

26.1. Será de responsabilidade da CONTRATADA o serviço de implementação, configuração e treinamento da solução.

(04) Prazo, local e condições de entrega ou execução:

15 (quinze) dias após assinatura do contrato, na Prefeitura Municipal de Xanxerê – Departamento de Informática.

(05) Condições de garantia

O licitante deverá prestar assistência técnica por telefone e acesso remoto, quando necessário, durante o período de vigência contrato, sendo que os prazos serão contados a partir da data de emissão do Termo de Recebimento Definitivo de Bens.

Não obstante, também com relação ao cumprimento da garantia, a empresa contratada fica sujeita às disposições contidas no respectivo Contrato.

A CONTRATADA deverá arcar com todos os custos e despesas inerentes à prestação do serviço de garantia acima citado, tais como deslocamentos, alimentação, hospedagem, fretes, etc.

Durante o período de vigência contratual, o fornecedor ficará obrigado a efetuar, às suas expensas, possíveis correções no software para o perfeito funcionamento da solução, regularmente constatado.

Além da obrigação de prestação de garantia, a CONTRATADA também se obriga a responder num prazo máximo de 02 (duas) horas, contados a partir do momento do registro, os atendimentos à distância - remotos ou telefônicos.

A CONTRATADA deverá solucionar o problema apontado no chamado técnico, no prazo máximo de 02 (dois) dias úteis, contados a partir da data e hora de protocolo do registro, realizado pelo servidor do Município.

Na hipótese de subcontratar a assistência técnica para a prestação do serviço, a CONTRATADA deverá entregar à CONTRATANTE cópia autenticada ou via original do pertinente instrumento particular de contrato firmado entre ela (CONTRATADA) e a empresa terceirizada (com firmas devidamente reconhecidas em cartório), sob pena de rescisão unilateral do presente Termo Contratual, sem prejuízo das sanções dispostas nos artigos 86 e 87 da Lei Federal nº 8.666/93.

A CONTRATADA deverá fornecer relatórios de serviços executados, assumir todos os possíveis danos, tanto nas dependências físicas, quanto bens materiais, causados a CONTRATANTE, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança quando da execução dos serviços;

Fica de responsabilidade da CONTRATADA o serviço de implementação, configuração e treinamento da solução.

(06) Responsável pelo recebimento e fiscal de contrato

Anderson Orso
Telefone: 3441-8516
ti@xanxere.sc.gov.br

(07) Condições e prazos de pagamento:

Conforme Decreto n° 005/2024

(08) Dotação Orçamentária

Red. 15

Elemento: 3999

(09) Obrigações da contratante

Efetuar pagamento conforme cronograma;

Fiscalizar a execução do objeto.

(10) Obrigações da contratada

Prestar os serviços de forma continua;

Realizar suporte técnico quando necessário.

(11) Qualificação técnica:

Atestado de Capacidade Técnica.

Documento emitido por empresa, entidade pública ou profissional habilitado, que comprova a experiência e a qualificação técnica de um profissional ou da empresa na execução dos serviços ou atividades exigidas.

(12) Critério de avaliação das propostas

Menor preço.

(13) Valores referenciais de mercado

Valores baseados no mercado atual.

Buscas realizadas na plataforma compras.gov.br retornou somente processos suspensos.

ARCEGO Representações Comerciais – Valor: 26.390,00

SystemUp Solução em Tecnologia – Valor 29.898,60

Outros Termos/Processos (Processo Administrativo nº 14/2023 – Conselho Federal de Química) - Valor: 16.800,00

(14) Estimativa de Custo

R$ 24.362,86

(15) Prazo de Vigência do Contrato:

36 meses.

(16) Resultados esperados:

Fornecer segurança cibernética nos dados da prefeitura;
Proteger a integridade dos arquivos e comunicações internas;
Suporte técnico.

(17) Responsável por informações sobre o objeto:
Anderson Orso – 3441-8516 – 7:30 às 11:30 – 13:00 às 17:00.

Data: 17/07/2024

_____ Ciente:_____

Carlos Alberto Peretti — Oscar Martarello

Assinatura do Secretário — Prefeito Municipal

_____

Anderson Orso

Assinatura do Fiscal

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: A976-6413-BD5B-A8F4

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

ANDERSON ORSO (CPF 043.XXX.XXX-22) em 19/07/2024 15:27:03 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

CARLOS ALBERTO PERETTI (CPF 008.XXX.XXX-74) em 22/07/2024 09:09:16 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

OSCAR MARTARELLO (CPF 461.XXX.XXX-15) em 24/07/2024 10:57:36 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://prefxanxere.1doc.com.br/verificacao/A976-6413-BD5B-A8F4