Estudo Técnico Preliminar 181/2024

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

SOLUÇÃO ANTIVÍRUS

Todo o ambiente corporativo sendo ele governamental ou não, necessita implementar uma solução de antivírus para proteger seus ativos de TI contra ameaças cibernéticas, ou seja, software projetado para detectar, prevenir e remover malware, incluindo vírus, worms, trojans, spyware, adware e outras formas de software malicioso.

A principal função de um antivírus é proteger computadores e dispositivos contra ameaças que podem comprometer a segurança dos dados e a integridade do sistema.

Ainda importante ressaltar o vencimento da licença atual Nº do Edital: PREGÃO ELETRÔNICO Nº 0007/2021

3. Área requisitante

Área Requisitante	Responsável
Secretaria de Administração e Finanças - Departamento de Informática	Carlos Alberto Peretti - Anderson Orso

4. Necessidades de Negócio

Proteção contra malwares que possam comprometer as estações de trabalho.

Proteção contra malwares que possam comprometer o uso dos servidores.

Garantir disponibilidade aos serviços internos de TI Equipamentos com garantia técnica e suporte técnico.

Proteção contra vazamento de informações e perda de dados.

Atualização e modernização das soluções de segurança. Reduzindo o risco de indisponibilidade na rede.

Deverá fornecer Console de Gerenciamento para controle e operacionalização, além de controle de políticas, para cada tipo de módulo de segurança contratado.

Deverá permitir a instalação das licenças ou agentes em servidores, estações de trabalho e máquinas virtualizadas, via console de gerenciamento, com opção de remoção de soluções antivírus previamente instalada.

Deverá possuir painel de controles dashboard com acompanhamento e monitoramento em tempo real do status de cada endpoint.

As licenças fornecidas devem ser por subscrição e deverão permanecer ativas na vigência do contrato.

5. Necessidades Tecnológicas

Detecção de malware: A solução precisa ter a capacidade de identificar e bloquear diferentes tipos de malware, como vírus, worms, trojans, ransomware e outros softwares maliciosos. Isso pode envolver a utilização de assinaturas de malware, análise heurística, detecção de comportamento malicioso e aprendizado de máquina.

Atualizações de definições: É importante que a solução seja atualizada regularmente com as últimas definições de malware. Isso garante que ela possa reconhecer e combater as ameaças mais recentes.

Proteção de Endpoint e servidores: Soluções de proteção de servidores devem fornecer recursos como detecção e prevenção de intrusões, firewall de host, controle de acesso a aplicativos e serviços, além de auditoria e registro de eventos para monitorar atividades suspeitas e proteger os servidores contra-ataques.

Proteção de armazenamento: Soluções de proteção de armazenamento (storage) devem garantir a segurança dos dados armazenados. Isso pode incluir criptografia de dados em repouso, detecção de intrusões, controle de acesso baseado em função, backups e recuperação de dados, além de auditoria de eventos relacionados ao armazenamento.

Integração com plataformas e sistemas: É importante que as soluções de segurança possam ser integradas com as plataformas e sistemas existentes na infraestrutura de TI, como sistemas operacionais, servidores de e-mail, firewalls de rede, switches e roteadores. A integração permite uma maior visibilidade e controle sobre as ameaças e atividades maliciosas.

Gerenciamento centralizado: Uma necessidade importante é a capacidade de gerenciar todas as soluções de segurança a partir de uma única interface centralizada. Isso facilita a configuração, monitoramento e geração de relatórios, além de permitir uma resposta mais rápida a ameaças e incidentes de segurança.

Relatórios e auditoria: A solução de segurança deve oferecer recursos de geração de relatórios e auditoria para acompanhar a eficácia das medidas de proteção implementadas, identificar áreas de melhoria e atender aos requisitos de conformidade regulatória. Deve ser fácil de configurar e gerenciar.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

A transferência de informações técnicas será realizada por meio de um treinamento, que ocorrerá imediatamente após a assinatura do contrato de prestação de serviços. Este treinamento será destinado a, no mínimo, dois colaboradores da contratante.

7. Estimativa da demanda - quantidade de bens e serviços

Este estudo técnico tem como objetivo a contratação de uma solução de antivírus para estações de trabalho, servidores que compõe o ambiente administrativo da Prefeitura de Xanxerê.

UNIDADE	Justificativa	Quantidade
Centro Administrativo	Servidores, Desktop e notebooks	140

8. Levantamento de soluções

	Identificação de Soluções
01	**Antivírus Tradicional** Software instalado localmente em computadores e dispositivos, que oferece proteção direta e imediata.
02	**Antivírus na Nuvem** Soluções que utilizam processamento em nuvem para detectar ameaças, reduzindo a carga sobre o dispositivo do usuário e oferecendo proteção atualizada em tempo real.
03	**Renovação de licenciamento da solução atual de antivírus** Essa alternativa consiste na renovação da última licença de antivírus adquirida pelo Município, permitindo a atualização tecnológica. Isso aumentará o nível de segurança e reduzirá falhas tanto de segurança quanto técnicas.

04	**Soluções Corporativas/ Contratação de nova solução de antivírus** Essa alternativa consiste na aquisição de uma nova solução de antivírus, possibilitando atualização tecnológica de modo a aumentar a nível de segurança e reduzir falhas de segurança e técnicas. Ferramentas de antivírus projetadas para empresas, oferecendo gerenciamento centralizado, proteção de servidores e dispositivos móveis, além de políticas de segurança personalizadas.

9. Análise comparativa de soluções

Solução 1: Um antivírus tradicional é um software projetado para detectar, prevenir e remover malwares, como vírus, worms, trojans e spyware, de um sistema informático. Aqui estão alguns pontos principais sobre antivírus tradicionais:

1. **Baseado em Assinaturas**: Eles utilizam um banco de dados de assinaturas de malwares conhecidos. O software compara os arquivos no sistema com essas assinaturas para identificar possíveis ameaças.
2. **Escaneamento Regular**: Os antivírus tradicionais realizam escaneamentos periódicos do sistema, analisando arquivos e programas para detectar atividades suspeitas.
3. **Proteção em Tempo Real**: Além dos escaneamentos regulares, eles monitoram o sistema em tempo real para bloquear malwares à medida que são detectados.
4. **Atualizações Frequentes**: Para se manter eficaz, o banco de dados de assinaturas de malware precisa ser atualizado regularmente com novas definições de vírus.
5. **Remoção de Malware**: Quando uma ameaça é detectada, o antivírus oferece opções para quarentena, remoção ou limpeza dos arquivos infectados.
6. **Recursos Adicionais**: Alguns antivírus tradicionais também incluem firewalls, proteção contra phishing e ferramentas para segurança na navegação na internet.

Apesar de sua eficácia contra malwares conhecidos, os antivírus tradicionais podem ser limitados na detecção de ameaças novas e desconhecidas, especialmente aquelas que usam técnicas avançadas para evitar a detecção. Por isso, muitas soluções de segurança modernas combinam métodos tradicionais com técnicas mais avançadas, como análise comportamental e aprendizado de máquina.

Solução 02: Um antivírus na nuvem é uma solução de segurança que utiliza a tecnologia de computação em nuvem para detectar, analisar e mitigar ameaças cibernéticas. Aqui estão os principais aspectos de um antivírus na nuvem:

1. **Análise Baseada na Nuvem**: Em vez de depender exclusivamente de um banco de dados local de assinaturas de malwares, os antivírus na nuvem enviam informações sobre arquivos suspeitos para servidores remotos onde a análise é realizada. Isso permite uma detecção mais rápida e precisa de novas ameaças.

2. **Atualizações em Tempo Real**: Como a base de dados de ameaças está na nuvem, ela pode ser atualizada continuamente e em tempo real. Isso garante que o software de antivírus esteja sempre equipado com as informações mais recentes sobre ameaças.
3. **Redução do Uso de Recursos Locais**: Com a análise e o armazenamento de dados ocorrendo na nuvem, o impacto no desempenho do dispositivo do usuário é reduzido. Isso é especialmente benéfico para dispositivos com recursos limitados.
4. **Detecção de Ameaças Avançadas**: Os antivírus na nuvem podem utilizar técnicas avançadas, como aprendizado de máquina e análise comportamental, para identificar ameaças novas e desconhecidas com mais eficácia.
5. **Escalabilidade**: A infraestrutura baseada na nuvem pode facilmente escalar para lidar com grandes volumes de dados e aumentar a capacidade de processamento conforme necessário.
6. **Gerenciamento Centralizado**: Empresas podem gerenciar a segurança de todos os seus dispositivos a partir de um painel de controle centralizado na nuvem, facilitando a implementação de políticas de segurança e monitoramento de ameaças.
7. **Colaboração Coletiva**: As soluções de antivírus na nuvem frequentemente agregam dados de ameaças de todos os usuários, criando uma base de dados coletiva que melhora a detecção e resposta a novas ameaças para todos os clientes.

Embora os antivírus na nuvem ofereçam várias vantagens, eles também dependem de uma conexão de internet ativa para funcionar plenamente, o que pode ser uma limitação em ambientes com conectividade limitada ou intermitente.

Solução 03: Embora essa solução proporcione um avanço tecnológico significativo ao utilizar versões de antivírus mais atualizadas e integradas com novas tecnologias, o custo operacional e de renovação é substancialmente elevado.

Diante desse cenário, do ponto de vista da eficiência e da economicidade, a alternativa em questão não atende plenamente às necessidades de negócio elencadas e, portanto, é considerada inviável.

Solução 04: A aquisição de uma nova licença de antivírus, que atenda aos requisitos de negócio e tecnológicos estabelecidos neste ETP, permitirá a atualização de estações de trabalho e servidores, melhorando significativamente o nível de segurança e reduzindo o número de falhas de segurança.

Além de utilizar uma base de dados de vacinas atualizada regularmente, a ferramenta se comunicará com os clientes por meio de um agente instalado, possibilitando o gerenciamento centralizado através do software apropriado.

A qualidade do produto, a segurança e o suporte técnico durante o prazo de vigência do contrato são fatores que tornam essa solução particularmente atrativa para o serviço público, especialmente considerando o elevado grau de confidencialidade das informações.

Um antivírus corporativo é uma solução de segurança projetada especificamente para proteger redes e dispositivos de uma organização contra malwares, ataques cibernéticos e outras ameaças digitais. Aqui estão os principais aspectos de um antivírus corporativo:

1. **Proteção Abrangente**: Oferece proteção não apenas para desktops e laptops, mas também para servidores, dispositivos móveis e outros endpoints dentro da rede corporativa.
2. **Gerenciamento Centralizado**: Fornece uma console de administração centralizada que permite aos administradores de TI gerenciar a segurança de todos os dispositivos da rede a partir de um único ponto. Isso inclui a aplicação de políticas de segurança, monitoramento de ameaças e a implementação de atualizações.
3. **Escalabilidade**: Projetado para escalar conforme a organização cresce, permitindo a fácil adição de novos dispositivos e usuários à rede protegida.
4. **Recursos Avançados de Segurança**: Além das funcionalidades básicas de um antivírus, as soluções corporativas frequentemente incluem:
    - **Firewall Integrado**: Protege contra acessos não autorizados à rede.
    - **Proteção contra Phishing**: Bloqueia tentativas de phishing e fraudes online.
    - **Detecção e Resposta a Ameaças (EDR)**: Ferramentas para detectar e responder rapidamente a ameaças avançadas.
    - **Controle de Dispositivos**: Gerencia e restringe o uso de dispositivos externos como pendrives.
    - **Proteção de Dados**: Inclui recursos para prevenção de perda de dados (DLP).
5. **Automação e Inteligência Artificial**: Utiliza algoritmos de aprendizado de máquina e inteligência artificial para detectar padrões anômalos e novas ameaças, melhorando a capacidade de resposta a ataques sofisticados.
6. **Relatórios e Auditorias**: Gera relatórios detalhados sobre incidentes de segurança, conformidade e desempenho do sistema, ajudando na tomada de decisões e em auditorias de segurança.
7. **Suporte e Serviços**: Frequentemente vem com suporte técnico dedicado e serviços adicionais, como assistência na configuração, resposta a incidentes e consultoria em segurança.
8. **Integração com Outras Ferramentas**: Integra-se com outras ferramentas de segurança e gerenciamento de TI, como sistemas de gerenciamento de informações e eventos de segurança (SIEM), para uma abordagem mais holística à cibersegurança.

Os antivírus corporativos são essenciais para proteger os dados sensíveis das empresas, garantir a continuidade dos negócios e cumprir regulamentos e normas de segurança. Diante do exposto, esta solução é considerada viável para Contratação.

10. Registro de soluções consideradas inviáveis

Conforme a análise individual das soluções da sessão anterior, as soluções: **SOLUÇÃO 01, 02 e 03** não são consideradas as mais vantajosas no atual cenário da instituição, quando comparada com a **SOLUÇÃO 04**.

11. Análise comparativa de custos (TCO)

Esta análise levará em conta não apenas o custo inicial de aquisição, mas também os custos operacionais ao longo do tempo, incluindo manutenção, atualizações e suporte técnico. Dessa forma, será possível garantir que a escolha da solução seja a mais econômica e eficaz a longo prazo, proporcionando um investimento que traga benefícios sustentáveis e contínuos para a segurança e proteção dos dados municipais.

Pregão/ processo	Órgão publico	Fornecedor	CNPJ	Valor da Proposta
Processo ADM - Nº 14/2023 PREGÃO ELETRÔNICO SRP N° 80/2022	SERVIÇO PÚBLICO FEDERAL -CONSELHO FEDERAL DE QUÍMICA - HOSPITAL DAS FORÇAS ARMADAS, MINISTÉRIO DA DEFESA /			16.800,00
PROPOSTA COMERCIAL Nº: 49V1/2024	Cotação de Mercado	A R C E G O Representações Comerciais	01.418.445/0001-59	26.390,00
Orçamento N° 2020	Cotação de Mercado	SYSTEMUP - Soluções em Tecnologia	12.027.844/0001-05	29.898,60

A tabela acima foi construída considerando critérios técnicos e quantitativos semelhantes ao cenário existente hoje.

Pregão/ processo	Órgão publico	Fornecedor	licenças		Treinamento e suporte		CNPJ

				Valor da Proposta /licença		**Valor da Proposta Treinamento /Suporte**	
Processo ADM - Nº 14 /2023 PREGÃO ELETRÔNICO SRP N° 80 /2022	SERVIÇO PÚBLICO FEDERAL - CONSELHO FEDERAL DE QUÍMICA - HOSPITAL DAS FORÇAS ARMADAS, MINISTÉRIO DA DEFESA /		sim	R$ 16.800,00	não	--	--
PROPOSTA COMERCIAL Nº: 49V1/2024	Cotação de Mercado 01	ARCEGO Representações Comerciais	sim	R$ 20.790,00	sim	R$ 5.600,00	01.418.445/0001-59
Orçamento N° 2020	Cotação de Mercado 02	SYSTEMUP - Soluções em Tecnologia	sim	R$ 25.898,60	sim	R$ 4.000,00	12.027.844/0001-05

Valor unitário das licenças/ média	Total 140 licenças	Implantação, treinamento e suporte	Valor total
166,74	23.344,30	4.800,00	**28.144,30**

A tabela acima foi construída considerando critérios de licenças e treinamentos/ implantação. Valor 1 - consiste em um processo de 2023, onde os valores possuem licenças e não contempla treinamento (valores defasados). Valor 2 – utilizado para mesurar valores exatos e economicidade ao Município. Valor 3 - utilizado para mesurar valores exatos e economicidade ao Município.

Deste modo, foi utilizado para média somente o valor 2 e 3, os dois valores possuem pacote completo de licenciamento, implantação e treinamento.

Descrição da Solução	Ano 1	Ano 2	Ano 3	Total
Aquisição de licenciamento Antivírus, incluindo suporte técnico e atualizações pelo período de 36 (trinta e seis) meses.	**R$ 9.381,43**	**R$ 9.381,43**	**R$ 9.381,43**	**R$ 28.144,3**

Tabela a cima, valor médio baseado em cotação de mercado.

12. Descrição da solução de TIC a ser contratada

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 mínimos 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 modulo 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.

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 Sever 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, Windows 10

13.3. Sistemas Operacionais Servidores: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, 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, pendrives. Deverá permitir a escolha e configuração de pastas a serem escaneada;

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

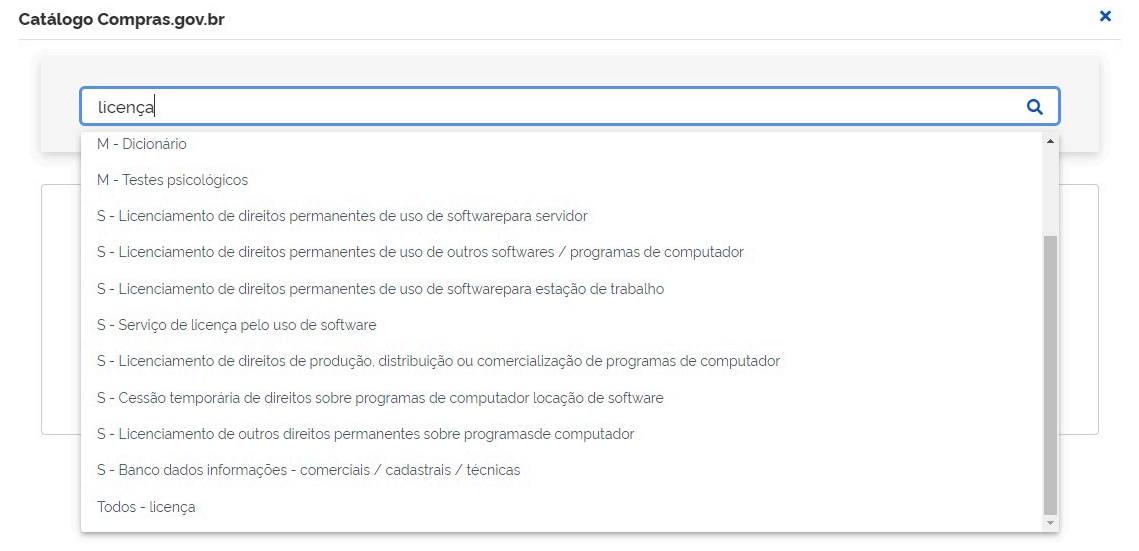
26.1. Será de responsabilidade da CONTRATADA o serviço de implementação, configuração e treinamento da solução.

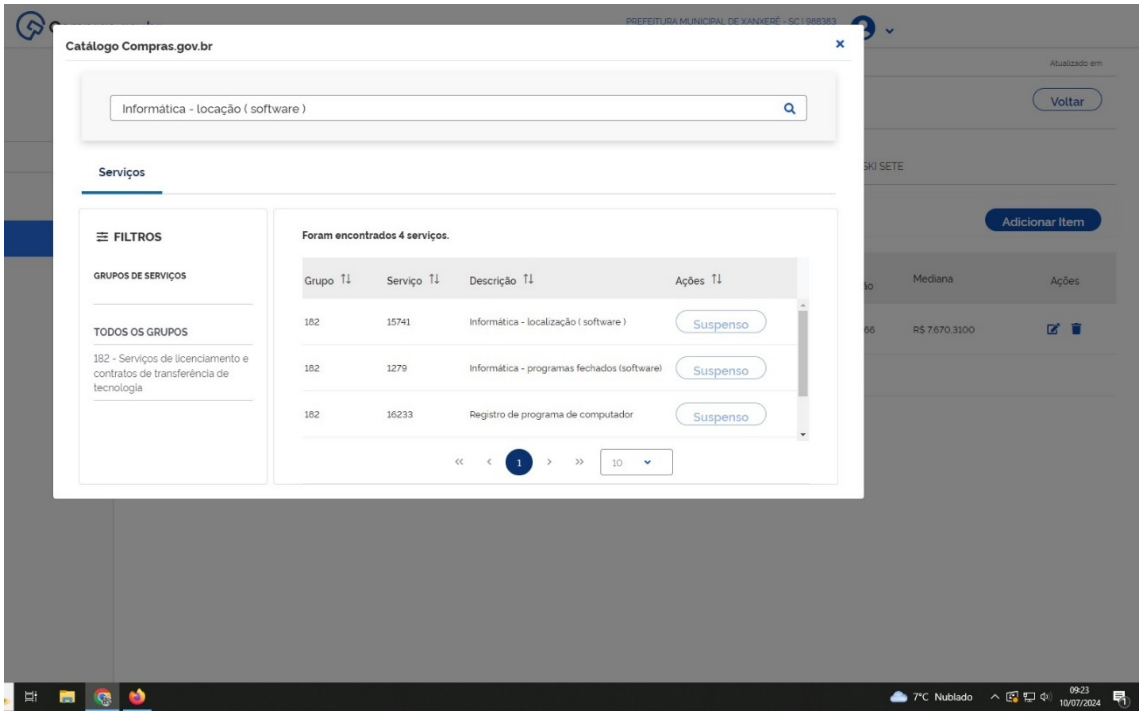
13. Estimativa de custo total da contratação

Valor (R$): 28.144,30

Valor (R$): 28.144,30 referentes a 140 licenças, implantação, suporte e treinamento (validade 36 meses).

De acordo com a pesquisa realizada nos processos de licitação da administração pública (compras.gov.br) não foi encontrado nenhum processo ativo para itens de informática (locação de software) ou licenciamento da ferramenta antivírus. Somente processos suspensos.





Seguimos na busca de contratos de outras repartições públicas contratando o mesmo objeto: Termo-de-referencia-Adesao-Ata-Antivirus.pdf (cfq.org.br). A contratação é do ano de 2023 e está desatualizada - considerando atualizações de preço baseadas em dólar. Feita a pesquisa de preço no mercado, considerando os itens compatíveis com a contratação pretendida, o valor global estimado para a contratação é de aproximadamente R$ **28.144,30**.

Pregão/Processo	Órgão publico	Fornecedor	CNPJ	Valor da Proposta
Processo ADM - Nº 14 /2023 PREGÃO ELETRÔNICO SRP N° 80 /2022	SERVIÇO PÚBLICO FEDERAL -CONSELHO FEDERAL DE QUÍMICA - HOSPITAL DAS FORÇAS ARMADAS, MINISTÉRIO DA DEFESA /			16.800,00
PROPOSTA COMERCIAL Nº: 49V1/2024	Cotação de Mercado	ARCEGO Representações Comerciais	01.418.445/0001-59	26.390,00
Orçamento N° 2020	Cotação de Mercado	SYSTEMUP - Soluções em Tecnologia	12.027.844/0001-05	29.898,60

			Média	**28.144,30**

14. Justificativa técnica da escolha da solução

Após analisar as soluções mencionadas no item 8, 'LEVANTAMENTO DE SOLUÇÕES', concluiu-se que todas elas cumprem os requisitos técnicos necessários para atender às necessidades do órgão. Desta forma, será escolhida a solução mais vantajosa para a Administração Pública e que atenda todos os requisitos solicitados.

Com esta contratação a Prefeitura de Xanxerê pretende alcançar os seguintes benefícios: Prover níveis adequados de segurança à rede de dados. Assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações. Aumento da eficiência contra as vulnerabilidades, segurança, proteção e autenticidade de dados sensíveis da organização. Possibilitar a identificação e o rastreamento das tentativas de invasão à rede. Proteção, autenticidade e acessibilidade as informações. Resolução remota de incidentes de segurança. Atualização tecnológica dos recursos humanos envolvidos na área de segurança (treinamentos). Implementação de regras e políticas de segurança no que se refere ao uso da rede de dados. Filtrar conteúdo, com a capacidade de analisar em tempo real o acesso à internet, permitido ou bloqueando sites de acordo com a categoria e permitir a emissão de relatório de acesso, evitando o anonimato na rede e assegurando a boa utilização da internet.

15. Justificativa econômica da escolha da solução

A ausência da solução em questão pode levar a eventos catastróficos com impactos negativos incalculáveis para os dados do município. Assim, sua contratação se justifica economicamente, uma vez que reduzirá custos inesperados relacionados à mitigação de riscos. Além disso, a solução proposta é amplamente reconhecida como a melhor alternativa disponível no mercado para as demandas atuais. Essa escolha também se justifica economicamente pela alta concorrência entre fornecedores, o que pode reduzir os valores de referência e gerar economia para a administração.

16. Benefícios a serem alcançados com a contratação

Prevenção de Eventos Catastróficos: A ausência desta solução pode levar a eventos catastróficos com impactos negativos incalculáveis para os dados do município. A implementação da solução ajudará a evitar tais eventos.

Redução de Custos: A contratação se justifica economicamente, pois permitirá a redução de custos inesperados relacionados à mitigação de riscos, resultando em uma gestão financeira mais eficiente.

Melhor Alternativa de Mercado: A solução proposta é amplamente reconhecida como a melhor alternativa disponível no mercado para atender às demandas atuais, garantindo a eficácia e a qualidade do serviço.

Concorrência e Economia: A escolha também se justifica pela alta concorrência entre fornecedores, o que pode levar à redução dos valores de referência e, consequentemente, gerar economia para a administração.

Segurança e Confiabilidade: Implementar a solução aumenta a segurança e a confiabilidade dos dados do município, protegendo informações críticas contra possíveis falhas ou ataques.

Eficiência Operacional: A solução proporcionará uma maior eficiência operacional, permitindo uma gestão mais ágil e eficaz dos recursos e processos municipais.

17. Providências a serem Adotadas

O Departamento de informatica adotará a forma de repasse de conhecimento entre os integrantes da equipe que gerenciará a solução contratada. O repasse de conhecimento se dará na forma de capacitação ou treinamento na solução e seus recursos. A referida atividade de treinamento deverá ser capaz de dotar aos participantes a capacidade de instalar, operar e manter todos os módulos e recursos da solução fornecida pela contratada. Serão capacitados 2 (dois) integrantes da equipe responsável pelo gerenciamento da solução contratada. Juntamente com o repasse de conhecimento, a TI deverá realizar o armazenamento da documentação dos produtos contratados em ambiente digital.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A solução proposta é viável e justificável sob diversos aspectos, destacando-se:

A implementação desta solução é crucial para evitar eventos catastróficos que poderiam causar impactos negativos incalculáveis aos dados do município. A contratação é economicamente justificável, pois contribuirá para a redução de custos inesperados associados à mitigação de riscos. Esta solução é reconhecida no mercado como a melhor alternativa para as demandas atuais. A proposta é amplamente aceita como a mais eficaz e de maior qualidade disponível no mercado, garantindo que as necessidades do município sejam atendidas de forma otimizada. A solução proporcionará maior eficiência operacional, permitindo uma gestão mais ágil e eficaz dos recursos e processos municipais.

Com base nesses pontos, declaramos a viabilidade da contratação da solução proposta, ressaltando sua importância e os benefícios significativos que trará para a administração municipal.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ANDERSON ORSO

Equipe de apoio

DANIEL STRADA

Agente de contratação

Assinou eletronicamente em 29/07/2024 às 10:07:24.

LUIZA BABINSKI SETE

Agente de contratação

Assinou eletronicamente em 29/07/2024 às 10:03:53.