TERMO DE REFERÊNCIA

PROCESSO ADMINISTRATIVO Nº 65/2024.

Fundação das Artes de São Caetano do Sul

Necessidade da Administração: Contratação por dispensa de licitação, de empresa para o fornecimento de licença por 12 meses, de software de antivírus para utilização nos computadores e servidores da Fundação das Artes de São Caetano do Sul (sede) e Unidade Santa Paula, conforme especificações deste Termo.

1. DO OBJETO

Contratação de empresa para fornecimento de 76 licenças, de software de antivírus.

Descrição detalhada:

Fornecimento por 12 meses do serviço de hospedagem profissional com 100 domínios e 40 caixas postais de 2Gb., armazenamento de informações em um banco de dados MS SQL e 10 caixas postais adicionais.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

A aquisição das licenças de antivírus tem o objetivo prevenir a contaminação por vírus, malwares e suas variantes bem como ameaças cibernéticas distintas nos computadores da Fundação das Artes e Unidades que podem colocar em risco o sigilo, a integridade e disponibilidade das informações.

Com o grande volume de utilização e com o crescimento da utilização de e-mails e acesso a páginas de internet a aquisição de um software de antivírus é necessária para fornecer um mínimo de segurança à infraestrutura de rede de computadores da FASCS.

As aquisições propõem uma maior proteção aos computadores e servidores, resguardando problemas que podem prejudicar os serviços da FASCS.

Assim, a aquisição das licenças de antivírus é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades da Fundação das Artes de São Caetano do Sul e Unidade Santa Paula.

3. DESCRIÇÃO DA SOLUÇÃO.

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

- 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;

- O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pelo console de gerenciamento;
- O produto deverá possuir no mínimo os seguintes módulos:

✓ Console de Gerenciamento fornecendo funcionalidades de gestão;
✓ Módulos 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 antes 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 Windows ou Console com Gerenciamento na nuvem (Cloud).
- Deverá suportar no mínimo os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box;
- Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
- Deverá ser fornecido com base de dados embutido no Console em Nuvem, sem a necessidade de baixar para máquina do administrador do Console;
- Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
- O mecanismo de varredura deverá estar disponível para download separadamente;
- 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);
- 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 o pacote será atualizado;
- As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;

- No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
- Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações:

✓ Nome; Tipo de relatório; Alvo do relatório;

- Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- Inventário da Rede
- Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;
- Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
- Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
- Descoberta de rede para máquinas em grupo de trabalho;
- Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
- Possibilitar a instalação remota e desinstalação remota do antivírus;
- Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- Possuir tarefas remotas e configuráveis de Scan;
- Possuir tarefa de reinicialização remota de estação 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 Assinada, ultimo status de malware;

Políticas

- 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 à 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 de usar e visualização simplificada;
- Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
- Filtros de agendamento de relatórios;
- Arquivo com todas as instâncias de relatório agendados;
- Exportar o relatório 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;
- Relatório - Monitora e cria relatórios;
- 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, intervalos de tempo;

Certificado de Segurança
- Deverá prover o acesso via HTTPS;
- Deverá permitir a importação de certificados digitais;
- O gerenciamento e a comunicação com dispositivos móveis deve 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 Hibrido, Scan Central;
- Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; (Windows Workstation), Instalar o antivírus sem o módulo de firewall; (Windows Workstation)
- Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.
- Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2012R2, Windows Server 2012, Windows Server 2008 R2.
- 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;

Gerenciamento e Instalação Remota

- Deverá permitir ao administrador customizar a instalação;
- 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;
- Deverá ser possível ter 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;
- A 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 ser for para 32 bits 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

- Proteção de antivírus dedicado para ambientes virtuais;
- Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;
- O 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 Linux;
- O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

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;

Requisitos Mínimos suportados pelo Sistema.

- 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
- Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10

- 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.

Componentes e Funcionalidade do Antivírus Geral

- 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:

✓ CD/DVD, 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;

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;

Controle do Dispositivo

- Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;

- Deverá permitir regras de definição de bloqueio/desbloqueio;
- Deverá permitir regras de exclusão;

Atualização

- Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
- Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- Permitir atualizações de assinatura de hora em hora;
- 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.

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 Criptografia presente na mesma Console do Antivirus.
- Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);
- Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra

Proteção Avançada NGAV

- 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.
- 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 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.

- Reparo e resposta automatizada a ameaças
- 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.

- 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. Projetado desde o início para
- 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 hospedam kits de exploração, além de bloquear tráfego suspeito na web.
- Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.

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 maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros 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. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecem 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 ecanismos 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 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. 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.

4. DOS REQUISITOS PARA CONTRATAÇÃO.

Das obrigações da contratada:

A Contratada se responsabiliza pelo pleno atendimento ao que o objeto deste Termo de Referência requer, e execução de todo o processo pertinente ao objeto deste projeto, sendo que a entrega bem como a forma de fazer o acompanhamento e controle ficará a cargo do Departamento de Compras da Fundação das Artes em atendimento às características especificadas acima.

5. EXECUÇÃO DO OBJETO.

O prazo para o início da execução dos serviços, a princípio, será de 1 dia após envio da Ordem de Serviço para a Contratada;

6. GESTÃO DO CONTRATO.

A gestão e a fiscalização do objeto contratado serão realizadas conforme o disposto no Decreto Municipal 11.914 de 12 de abril de 2023, nos termos da Lei Federal nº 14.133/2021.

Acompanhar e registrar as ocorrências relativas à execução contratual, informando a unidade responsável por sua gestão e ao gestor do contrato designados, aquelas que podem resultar na execução dos serviços e obras ou na entrega de material de forma diversa do objeto contratual, tomando as providências necessárias a regularização, por parte da contratada, das faltas ou defeitos observados;

Recepcionar da contratada, devidamente protocolados, os documentos necessários ao pagamento, previstos no termo de contrato e das normas de SEFAZ que disciplina os procedimentos

para a liquidação e pagamento, conferindo e remetendo à unidade responsável pela gestão de contrato, e ao gestor contratual designado;

Verificar se o prazo de entrega, as quantidades e a qualidade dos serviços, das obras ou do material encontram-se de acordo com o estabelecido no instrumento contratual, atestar a respectiva nota fiscal ou fatura e remetendo a unidade responsável pela gestão de contratos, e ao gestor designado;

Manifestar-se formalmente, quando consultado, sobre a prorrogação, rescisão ou qualquer outra providência que deva ser tomada com relação ao contrato que fiscaliza;

Consultar a unidade demandante dos serviços, obras ou materiais sobre a necessidade de acréscimos ou supressões no objeto do contrato, se detectar algo que possa sugerir a adoção de tais providências;

Propor medidas que visem a melhoria contínua da execução do contrato;

Exercer qualquer outra incumbência que lhe seja atribuída por força de previsão normativa.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO.

As medições para efeito do pagamento serão realizadas de acordo com os seguintes procedimentos:

Após a conferência dos quantitativos e valores apresentados, bem como da documentação exigida, a Fiscalização atestará a medição, comunicando a CONTRATADA, no prazo de 3 (três) dias contados do recebimento do relatório, o valor aprovado, e autorizará a emissão da correspondente fatura, a ser apresentada no primeiro dia subsequente à comunicação dos valores aprovados.

As Notas Fiscais/Faturas deverão ser emitidas pela CONTRATADA, contra o CONTRATANTE, e apresentadas para a Fiscalização.

A Fiscalização emitirá o Atestado de Realização dos Serviços em até 3 (três) dias contados a partir do recebimento da(s) Nota(s) Fiscal(is)/Fatura(s).

Os pagamentos serão efetuados em até 10 (dez) dias úteis contados da data de emissão dos Atestados de Realização dos Serviços, em conta corrente da CONTRATADA, em conformidade com os serviços executados, mediante a apresentação dos originais da nota fiscal/fatura.

O recebimento provisório ou definitivo dos serviços não exime a CONTRATADA de sua responsabilidade civil pela solidez e pela segurança do serviço, nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

O prazo para recebimento provisório será de até 15 (quinze) dias corridos, contados da comunicação escrita pela CONTRATADA, mediante termo circunstanciado assinado pelas partes, na forma expressa pela alínea 'a', inciso I, artigo 140, da lei Federal 14.133/21.

O recebimento definitivo dar–se–á por servidor ou Comissão designada pela Administração, mediante termo circunstanciado, assinado pelas partes, após o decurso de prazo de vistoria de até 90 (noventa) dias corridos, que comprove a adequação do objeto às condições contratuais, na forma expressa na alínea 'b', da legislação supra.

O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

8. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR.

Os critérios de aceitabilidade de preços serão:

- Valor Global estimado pela Fundação das Artes será de até: R$ 4.000,00.

O critério de julgamento da proposta é o menor preço global.

9. ESTIMATIVA DE PREÇOS

O custo estimado da contratação será tornado público apenas e imediatamente após o encerramento do envio das propostas.

10. ADEQUAÇÃO ORÇAMENTÁRIA

3.3.90.39.00 – Outros Serviços de Terceiros – Pessoa Jurídica.

São Caetano do Sul, 15 de abril de 2024.

José Carlos Rufato Junior
Chefe de Compras e Licitações
Fundação das Artes de São Caetano do Sul