ANEXO I

TERMO DE REFERÊNCIA

O presente Termo de Referência tem por objeto etabelecer critérios para a contratação de empresa especializada em serviços técnicos de solução e segurança de proteção de dados e gerenciamento de ativos de Tecnologia da Informação/TI, em nuvem, adotada na Prefeitura Municipal de Portão/RS, incluindo a instalação, configuração e treinamento, com o critério de JULGAMENTO das propostas MENOR PREÇO GLOBAL.

JUSTIFICATIVA PARA CONTRATAÇÃO

Atualmente o Município possui apenas um ponto de armazenamento de backup que se encontra no mesmo prédio da Prefeitura, onde os dados estão armazenados, também não possui solução de antivírus e proteção contra sequestros de dados e malwares em geral ou solução para gerenciamento das atualizações e inventário de hardware e software. Isso contraria as boas práticas de segurança que recomendam a replicação dos dados em outro ambiente físico, pois em caso de acidentes ou catastrofes os mesmos estariam protegidos. Além de um amplo gerenciamento dos recursos de tecnologia do Munícipio.

Sendo assim, faz-se necessária a aquisição do serviço para garantir a continuidade do negócio, alacançando os seguintes objetivos:
- Flexibilidade da solução de backup;
- Rapidez na implantação da solução;
- Facilidade na recuperação dos dados.
- Ampla proteção contra crimes cibernéticos;
- Controle dos endereços eletrônicos (sites) acessados pelos servidores.
- Manutenção e monitoramento da integridade dos equipamentos de informática.

1. PRAZO, LOCAL E FORMA DE ENTREGA.

Os serviços serão executados no prédio da Prefeitura Municipal, na Rua 9 de Outubro, 229, centro, e o telefone para contato com os responsáveis do setor de Tecnologia da Informção/TI é (51) 3500-4200, nos ramais 230 ou 281.

A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.

É responsabilidade da CONTRATADA monitorar eletronicamente a solução 24x7x365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.

A solução proposta deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações.

Em casos de paralisações dos serviços deve a CONTRATADA iniciar a correção do problema em até 4 horas corridas.

O sistema da CONTRATADA será responsável por operar as tarefas de backup de acordo com as solicitações realizadas pelo setor de Tecnologia da Informação/TI do Município.

A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup, e em casos de falha, a CONTRATADA deverá notificar eletronicamente o setor de Tecnologia da Informação/TI do Município, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

Em casos de impossibilidade técnica da resolução do erro, a CONTRATADA deve abrir chamado juntamente com o setor de Tecnologia da Informação/TI do Município para que o erro possa ser solucionado.

O Município terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup ou proteção sem qualquer custo adicional.

A CONTRATADA deverá enviar semanalmente relatório estatístico das rotinas de backup, proteção e gestão.

A CONTRATADA deverá fornecer suporte técnico 8x5 e um número de plantão fora do horário comercial, em língua portuguesa, para sanar dúvidas quanto à solução, sua configuração ou quaisquer outros assuntos relacionados à solução.

O suporte técnico deverá ter os seguintes canais de atendimento:
- Suporte Telefônico;
- e-mail;
- Sistema online de chamados;
- Chat.

A CONTRATADA terá o prazo de até 30 dias, contados da assinatura do Contrato, para disponibilização dos serviços ao Município.

Antes do início do projeto deverá ser convocada pela CONTRATADA, reunião com a equipe técnica do setor de Tecnologia da Informação/TI do Município. Serão apresentados os aspectos de concepção do projeto, incluindo rotinas, configurações, políticas, bem como plano de execução dos serviços, detalhando responsáveis, prazos e fases. Novas reuniões poderão ser convocadas por ambas as partes de modo a definir pormenores da solução e eliminar pendências.

Planejamento e descrição dos serviços (ETAPAS)

Planejamento dos serviços a serem executados, visando definir:
- Escopo dos serviços
- Equipe envolvida na execução dos serviços
- Cronograma inicial de implementação da solução;
- Objetivo final dos serviços

Acompanhamento da execução dos serviços.

Execução dos serviços

Implementação da solução:
- Um especialista da CONTRATADA deverá planejar todas as atividades necessárias e agendar a realização dos serviços em horários mutuamente acordados com o Município.
- Os serviços ocorrerão durante o horário comercial.

A CONTRATADA deverá disponibilizar checklist de backup, para que o Município preencha o mesmo com os servidores, serviços, bancos, diretórios, storages, agendamentos, prioridades e outras informações pertinentes à configuração das tarefas e rotinas de backup.

Implantação do Serviço

Testes de verificação da instalação, conectividade e redundância de conectividade

Documentação da instalação em relatório de instalação

Configuração das tarefas e rotinas de backup e proteção

A CONTRATADA deverá realizar reunião para demonstração do mapa de rotinas que foi criado a partir do checklist gerado pelo Município.

Em casos de alteração das rotinas ou divergência de entendimentos, o mapa de rotinas será alterado.
Implementação do mapa de rotinas na solução.

Execução inicial, de cada tarefa, acompanhada por técnico responsável da CONTRATADA.

Ao término da execução inicial, a CONTRATADA deve submeter seu resultado à aprovação do setor de Tecnologia da Informação/TI do Município.

Sessão de orientação ao cliente.

Fornecer orientação à equipe técnica do setor der Tecnologia da Informação/TI do Município, em horário combinado, antes da conclusão do serviço, durante o horário de expediente;

2. VIGÊNCIA

O prazo de vigência da contratação será de 12 meses, contados da assinatura do Contrato, podendo ser prorrogado por igual período até o limite de 60 meses, após a verificação das reais necessidades e vantagens para o Município para sua continuidade.

3. DA QUANTIDADE E VALOR ESTIMADO

As quantidades e valores estimados a serem contratados seguem no quadro abaixo:

Item	Descrição	Qtd	Un	R$/Un	R$/Total
1	Contratação de serviços técnicos de solução e segurança de proteção de dados, em nuvem (cloud computing), com armazenamento em datacenter, incluindo suporte e treinamento e segurança. Composto por 1 (um) servidor físico totalizando uma massa de 10TB de dados.	12	mês	6.000,00	72.000,00
2	Solução de proteção para servidores e estações de trabalho. Totalizando uma massa de 5 licenças de antivírus, com antiransomware nativo e EDR.	12	mês	178,00	2.100,00

- Conforme descrito no quadro acima, o valor anual estimado será de **R$74.100,00** (Setenta e quatro mil e cem reais).

4. DESCRIÇÃO DO SERVIÇO

A solução de backup deverá prover:

A Solução deve proteger o ambiente atual do Município, que é composto por 1 (um) Servidor físico File server com uma massa de dados de 10TB.

A solução deverá ser entregue como serviço e todos os dados deverão ser armazenados em Datacenter externo ao Ambiente do Município.

A solução proposta deverá dispor de console/portal para gerência e execução de backup e restauração de dados em nuvem.

A Solução deve ter garantia de atualizações durante o período do contrato sem ônus financeiro para o Município.

O software deverá oferecer funcionalidade completa de backup e restauração através de gerência centralizada.

O software de backup deverá ser capaz de enviar alertas através de correio eletrônico com o objetivo de reportar eventos ocorridos na operação e configuração do software.

O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup, com opção de gerar relatórios online ou enviar os mesmos por e-mail.

O software deverá ser capaz de emitir relatórios com informações completas sobre os jobs executados e porcentagem de sucesso de backups e restaurações.

O sistema deve prover quantidade ilimitada de restaurações, durante a vigência deste contrato.

O tráfego de dados de internet deve ser ilimitado, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

O Município deve garantir o acesso à internet como cliente da solução.

A solução proposta deverá possibilitar comunicação criptografada e protegida para transferência de dados (HTTPS, VPN ou outros).

A solução proposta deverá permitir a criptografia dos dados na armazenagem e na transmissão dos dados.

O agente (cliente) deve ter um suporte nativo para os seguintes bancos de dados:
- MySQL
- Microsoft SQL Server
- ORACLE

A solução deverá possuir forma de criar scripts de comando para backup de outros bancos de dados além dos cidados acima.

Os agentes (clientes) devem possuir suporte do fabricante durante todo o período do contrato, permitindo assim, atualizações constantes dos agentes e da solução como um todo.

Os agentes (clientes) devem poder ser instalados nativamente nas seguintes plataformas de sistemas operacionais e plataformas de virtualização:
- VMware,
- Hyper-V,
- Windows Server
- Linux

O sistema deve ser capaz de gerar relatórios acerca da realização e/ou não realização das rotinas de backup.

Os relatórios devem poder ser acessados ou gerados das seguintes formas:
- Por e-mail; e
- Via web.

A solução deve permitir que as cópias de segurança ocorram simultaneamente, de forma a otimizar as janelas de backup.

As tarefas de restauração também devem ocorrer de forma simultânea, seja durante as tarefas de backup ou de restauração.

Dos recursos da solução

- Deve permitir replicação de um mesmo dado da origem para vários destinos.
- Deve permitir replicação criptografada.
- Deve possuir proteção antimaware contra ataque de ransomware nativa na ferramenta, com configurações para alertar, bloquear ou até mesmo reverter uma ataque de ransoware utilizando cache da máquina.
- A solução de backup deverá possuir tecnologia de desduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.
- Deverá possuir backup sintético, ou seja, criar uma imagem a partir dos backups incrementais já armazenados no backup
- Deverá suportar política de disaster recovery para prevenir perda de dados e uma restauração mais rápida e segura.
- Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental.
- A solução deverá ter a possibilidade de validar continuamente de forma automática a integridade lógica dos dados, armazenados no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade.
- Possibilitar predefinir arquivos, pastas ou tipos de arquivos que não devem fazer parte dos backups mesmo quando backup da VM toda;
- Deverá possuir interface de administração GUI.
- Deverá permitir executar múltiplos processos de backup em paralelo e otimizar a restauração de arquivos individuais.
- O sistema de armazenamento de backup deverá ser escalável conforme a necessidade do Município.
- Backup sintético otimizado (funcionalidade que permite criar uma imagem full, a partir dos backups incrementais, sem movimentação de dados);
- Deverá prover o envio de alertas e relatórios através de email, de modo automático, manual ou programado.
- Deverá suportar software de replicação remota do próprio FABRICANTE;
- Deve ter capacidade de restauração de dados granular, a partir de dispositivos de armazenamento em discos, sendo possível a recuperação de um simples arquivo, uma base de dados, ou até mesmo uma completa recuperação do servidor, suportar backup e restore de máquina virtual VMware, Hyper-V, XenServer, com Sistemas Operacionais Windows e Linux, suportando backup “de guest” (agente instalado na máquina virtual) e backup “de imagem” com restore individual de arquivos e diretórios. O restore granular de arquivos a partir do backup da imagem deve ser realizado prefencialmente sem necessidade de instalação de agentes na máquina virtual. Para Banco de Dados sendo eles Oracle, SQL Server, MySQL, MariaDB com instalação de agente.
- A solução de backup a ser ofertada deverá atender integralmente os requisitos especificados neste Termo de Referência, devendo ser fornecida com todas as licenças que forem necessárias para entrega funcional da solução proposta onde o licenciamento deverá possuir capacidade ilimitada de retenções.
- Deverá permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.
- Deverá possuir a capacidade de reiniciar backups a partir do ponto de falha, após a ocorrência da mesma.
- Deverá possuir mecanismo de atualização de clientes e agentes de backup de forma remota, através da interface de gerenciamento.
- O suporte e atualização da solução de backup será válido durante todo o período contratado.
- Deverá ter compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System).
- Deverá possuir correções e atualizações adicionais disponíveis para o funcionamento do produto no Sistema Operacional alvo.
- Deverá possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.
- Deverá permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos personalisáveis.
- Deverá permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de

retenção das imagens.

- Deverá permitir a realização do backup completo de servidor para recuperação de desastres.
- Deverá permitir restaurar o backup de recuperação de desastres para hardware diferente do original.
- Deverá ser capaz de recuperar dados para servidores diferentes do equipamento de origem.
- Deverá permitir integração do controle de acesso com sistemas de diretório Active Directory.
- A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais Linux e Windows bem como operações de recuperação bare metal de forma nativa sem software de Terceiros.
- Para servidores Windows, deverá ser possível a recuperação das imagens de recuperação de desastres em um hardware ou em ambiente virtual.
- Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção.
- Deverá possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia., tanto no tráfego quanto em repouso com senha personalizável na segunda opção.
- Deverá possuir mecanismo de auditoria, permitindo a emissão de relatórios.
- Deverá possuir capacidade de resumo de tarefas de backup com falha, retomando a partir do momento da falha.
- Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente.
- Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 (trinta) dias.
- Deverá suportar o uso da funcionalidade CBT (ChangeBlockTracking) para as operações de backup.
- Deverá permitir o descobrimento automático das máquinas virtuais nos ambientes VMWare e Hyper-V.
- Deverá permitir restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do seu repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantânea.
- Deverá prover otimização do backup e recursos, permitindo que somente blocos utilizados sejam copiados no processo de backup.
- Deverá possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais.
- Deverá possuir capacidade de realizar backup de máquinas virtuais em estado online ou off-line.
- Deverá possuir a capacidade de realizar backup On-Host e Off-host das máquinas virtuais Windows.
- Deverá possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial.
- Deverá suportar ambientes configurados com Cluster Shared Volumes.
- Deve implementar backup utilizando Microsoft Volume Shadow Copy Service (VSS).
- Os mesmos agentes de backup deverão possuir recurso de acesso remoto aos computadores permitindo assim uma maior facilitade ao suporte;
- Deverá possuir opção para mapeando de dados no backup, com relatório que mostre de acordo com as extensões configuradas se existem dados relevantes fora do plano de backup, se assim contrato em licença adicional.
- Os mesmos agentes (client) de backup deverão realizar inventário de hardware que serão acessados e auditados pela equipe do setor de Tecnologia da Informação/TI do Município, sem custo adicional.
- A solução deverá possuir recursos básicos de segurança como ant-malware e avaliação de vulnerabilidade sistemas operacionais e aplicativos visto que 60% dos vazamentos de dados estão relacionados a falhas em aplicativos;
- O acesso ao portal de gestão deverá possibilitar acesso com autenticação muliplofator via aplicativos de autenticação, sms ou e-mail.

A solução de antivírus deverá prover:

- A solução deverá possuir recursos básicos de segurança como anti-malware e avaliação de vulnerabilidade sistemas operacionais e aplicativos visto que 60% dos vazamentos de dados estão relacionados a falhas em aplicativos;
- A solução deverá possuir recurso de detecção e resposta de endpoint (EDR) fazendo a identificação de rastreio de como o virus entrou na rede, e quais arquivos foram afetados pelo malware.
- Possuir console central único de gerenciamento. As configurações do Antivírus, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através do mesmo console;
- O produto deverá possuir no mínimo os seguintes módulos:

- Console de Gerenciamento fornecendo funcionalidades de gestão;
- Módulos para estações físicas, laptops e servidores e VMs;

- Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo os seguintes Hypervisors:

- VMWare vSphere;
- Citrix XenServer;
- 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 a instalação remota via console WEB de gerenciamento para ambientes de rede com ou sem domínio configurado.
- Licenciamento flexível ou seja permitir remover e adicionar licenças entre dispositivos de forma autonôma, sem precisar depender do suporte técnico;
- Arquitetura simples de atualização, com um simples clicar de botão todas as funções do antivírus.
- Descoberta de rede para máquinas em grupo de trabalho;
- Possuir busca em tempo real pelo menos com os seguintes filtros: Nome e Endereço IP;
- Possibilitar a instalação remota do antivírus;
- Através do console o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
- Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
- Deverá reportar o estado atual das máquinas no mínimo, protegida/desprotegida;
- O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado;
- Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- Possuir tarefas remotas e configuráveis de Scan;
- Filtro de sites malicosos com opção de notificar e bloquear o acesso do usuário, sendo possível gerar uma lista manual de sites bloqueados ou bloquea-los por categoria;
- Proteção antivírus e antimalware: Detecção de arquivos baseada em assinatura em nuvem em tempo real;
- Analisar arquivos baseados em intenligência artificial de pré-execução, Cyber Engine baseado em comportamento;
- Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit); exploração de memória, injeção de códigos e encaminhamento de privilégios.
- Detecção e interrupção de processos de criptomineração;
- Impedir alterações não autorizadas em registros, processos e aplicações com opção de proteção por senha se necessário.
- Oferecer proteção por base de assinaturas;
- Realizar proteção não só dos discos físicos, mas também de pastas recebidas e enviadas através de compartilhamento de rede;
- Possibilitar gerenciamento do Windows Defender ou Microsoft Security Essentials de forma centralizada na console web permitindo configurar proteção em tempo real, varreduras, exceções e demais

funcionalidades do mesmo;

- Possuir alternativa para que o usuário escolha qual ação será tomada em cada item de proteção, por exemplo, se quer ser apenas notificado, que o processo seja interrompido ou revertido;
- Antiransomware baseado em Inteligência Artifical, capaz de dectar e reverter processos de criptografia e sequestro de dados;
- Opção de acesso remoto as máquinas com agentes instalados, podendo essa função ser adicionada individualmente ao antivírus nas estações de forma ilimitada;
- Inventário de hardware para proteção e acompanhando das modificações realizadas nos computadores, permitindo uma proteção completa do patrimônio de informática, essa função também deve poder ser instalada separadamente ao antivírus de forma ilimitada;
- Possuir opção de bloqueio do uso de protas USB e FireWire por dispositivos removíveis, bloqueio do uso de impressões, acesso a área de transferência, dispositivos móveis, capturas de tela, bluetooth e unidades mapeadas;
- Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos;
- O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:

- Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;
- Módulos para estações físicas, notebooks e servidores;
- Módulo para ambientes virtualizados;
- Utilizar o conceito de heurística para combate e ações contra possíveis malwares;
- Oferecer tecnologia onde a solução identifique vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
- Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware;
- Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução dele no ambiente de produção;
- Oferecer proteção por base de assinaturas.

- CONSOLE DE GERENCIAMENTO
- Instalação e configuração
- Permitir instalação remota via console WEB de gerenciamento.
- Deve ser totalmente em português.
- Funcionalidades Gerais
- Licenciamento flexível;
- 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;
- A console de gerenciamento deverá incluir sessão de log com as seguintes informações:
- Login;
- Edição;
- Criação;
- Log-out;
- Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução;
- Permitir que o administrador escolha qual o pacote será atualizado;
- As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail;
- No mínimo enviar notificações para as seguintes ocorrências:
- Problemas com licenças;
- Alertas de surto de vírus;
- Máquinas desatualizadas;

- Eventos de antimalware;
- Deverá prover o acesso via HTTPS;
- Possuir no mínimo as integrações abaixo:
- Múltiplos domínios do Active Directory;
- Descoberta de rede para máquinas em grupo de trabalho;
- Possuir busca em tempo real pelo menos com os seguintes filtros:
- Nome;
- Sistema Operacional;
- Endereço IP;
- Possibilitar a instalação remota e desinstalação remota do antivírus;
- Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- Assinar políticas para no mínimo os níveis:

- Computador;
- Máquina Virtual;
- Grupo de Endpoints;

- Possuir a propriedade detalhada de objetos gerenciados para:

- Nome;
- IP;
- Sistema Operacional;
- Grupo;
- Política Assinada;
- Último status de malware.

Políticas

- Modelo único para todos os equipamentos, sejam físicos ou virtuais;
- Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
- Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
- Deverá permitir quantidade ilimitada de políticas cadastradas.

Relatórios

- Deverá apresentar as seguintes funcionalidades:
- Relatório para cada serviço de segurança;
- Facilidade de usar e visualização simplificada;
- Dashboard de relatórios configuravel, para selecionar quais relatórios devem ser exibidos.

Administração de Usuários:

- Deverá apresentas no mínimo as seguintes funcionalidades:
- Administração baseada em regras;
- Deverá ser possível customizar um tipo de usuário:
- Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento;
- Registrar as ações do usuário na console de gerenciamento;
- Detalhar cada ação do usuário;
- Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

SEGURANÇA PARA ESTAÇÕES E SERVIDORES

- Proteção para ambientes físicos;
- Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac;
- Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

- Windows 10 64Bits;
- Windows 8.1 64Bits;
- Windows 8 64Bits;
- Windows 7 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:

- Ubuntu 14.04 LTS ou superior;
- Red Hat Enterprise Linux / CentOS 6 ou superior;
- SUSE Linux Enterprise Server 11 SP4 ou superior;
- OpenSUSE Leap 42.x;
- Fedora 25 ou superior;
- Debian 8.0 ou superior;
- Oracle Linux 6.3 ou superior.

- Proteção para ambientes virtuais
- Para plataforma de virtualização com VMWare, deverá:
- A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
- Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac;
- Possuir opção de bloqueio do uso de protas USB e FireWire por dispositivos removíveis, bloqueio do uso de impressões, acesso a área de transferência, dispositivos móveis, capturas de tela, bluetooth e unidades mapeadas.
- Realizar proteção não só dos discos físicos, mas também de pastas recebidas e enviadas através de compartilhamento de rede.
- Detecção e interrupção de processos de criptomineração.
- Filtro de sites malicosos com opção de notificar e bloquear o acesso do usuário, sendo possível gerar uma lista manual de sites bloqueados ou bloquea-los por categoria.
- Instalação e Configuração Remota
- Deverá permitir ao administrador customizar a instalação;
- Deverá permitir a instalação customizada do antivírus com no mínimo:
- Instalar o antivírus sem o controle de acesso a internet;
- 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 uma visualização com as estações instaladas e as faltantes da instalação;
- 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 a distribuição em um agente separado.

Funções Gerais

- Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;
- Deverá permitir a configuração do scan do antivírus do cliente como:
- Scan local;
- Scan hibrido (local\remoto);
- Scan remoto;
- Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida;
- Deverá fazer scan em tempo real e automático;
- Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja,

por tamanho ou por tipo de extensão;

- Deverá possuir escaneamento baseado em análise heurística;
- Deverá permitir a escolha e configuração de pastas a serem scaneadas;
- 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;
- Antiexploit disponível para servidores e estações de trabalho baseado em Machine Learning para proteger contra vulnerabilidades de softwares;
- Deve possuir módulo de mitigação de Ransomware para detecção e recuperação de possíveis arquivos criptografados;
- Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;
- Deve possuir módulo de proteção contra ataques de rede que fornece uma camada de segurança a mais que detecta e executa ações contra ataques de rede projetados para obter acesso em endpoints através de técnicas específicas, tais como: ataques de força bruta, explorações de rede, ladrões de senha, movimentação lateral, etc...
- Inventário de hardware para proteção e acompanhando das modificações realizadas nos computadores, permitindo uma proteção completa do patrimônio de informática, essa função também deve poder ser instalada separadamente ao antivírus de forma ilimitada;
- Opção de acesso remoto as máquinas com agentes instalados, podendo essa função ser adicionada individualmente ao antivírus nas estações de forma ilimitada;
- Possibilitar gerenciamento do Windows Defender ou Microsoft Security Essentials de forma centralizada na console web permitindo configurar proteção em tempo real, varreduras, exceções e demais funcionalidades do mesmo;
- Deverá ter os seguintes requisitos mínimos de sistema:

- Plataformas de Virtualização
- VMware vSphere ESX 5.0 ou superior;
- VMware vCenter Server 4.1 ou superior;
- 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 para Desktops;
- Windows 10 64Bits;
- Windows 8.1 64Bits;
- Windows 8 64Bits;
- Windows 7 64Bits;

- Sistemas Operacionais para Servidores:

- Windows Server 2012R2;
- Windows Server 2012;
- Windows Server 2008 R2;
- Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;
- 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.

Quarentena:

- Deverá permitir restauração remota, com configuração de localidade e deleção;
- Criação e exclusão para arquivos restaurados;
- 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 de assinaturas.

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;
- Unidades ópticas;
- Discos Externos;
- Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

- Discos Externos;
- USB (Pendrives, armazenamentos removíveis);
- Área de transferência;
- Capturas de tela;
- Unidades mapeadas;

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

Atualização:

- Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização;
- Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando ela estiver sendo escaneada.

Proteção Avançada:

- Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques 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.
- Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
- Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.
- Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na

web. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.

- Proteção inteligente e em tempo real, verificando constantemente os arquivos e programas abertos, mesmo que para leitura.
- Prevenção de exploração através de recusos de proteção de memória, proteção contra programação orientada por retorno ou técnica ROP, proteção contra encaminhamento de privilégios ou injeção de códigos.

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.

Possibilidade de integração Futura da solução de gerenciamento:

- Agendamento de atualizações e execução de backups pré-atualização.
- A ferramenta devera desmobilizar dentro da mesma solução um painel para gestão das atualizações de aplicativos como java, adoble, office e outros, como também gerenciar paches de atualizações do Windows de forma individual, agrupada ou bloquear atualizações específicas;
- Listar atualizações de correção de vulnerabilidades listadas pelo MITRE.
- Gerenciar quais atualizações deverão ser realizadas (apenas importantes, recomendadas...)
- Inventário de Hardware e Sofware com relatório de registro de alterações, com no mínimo as especificações:
- Nome do Computador;
- Marca/modelo;
- Informações do CPU;
- Velocidade do CPU;
- RAM (Mb);
- Armazenamento total;
- Espaço livre;
- IP externo da máquina;
- Endereço de MAC;
- Endereço de IP;
- Máscara de sub-rede;
- Sistema Operacional instalado na máquina;
- Aplicativos e softwares instalados no computador, com fabricante e versão insatalada.
- Controle de dispositivos, com bloqueio da área de transferência, impressoras, removíveis e portas USB.
- Verificação da integridade do HD, com dashboard indicativo da “saúde” do componente.
- Solução de acesso remoto básico para quantidade ilimitade de computadores e avançado conforme licenças solicitadas no objeto.
- Possibilidade de excução de scripts em massa através das linguagens PowerShell e Bash para atualização, configuração, instalação ou remoção de softwares, por exemplo.
- Repositório de Scripts para armazenar o histórico de scripts criados pela equipe de TI.
- Biblioteca de scripts pré-configurados, como no minímio 40 scripts ja configurados para uso imediato.
- Permitir o gerenciamento dos dispositivos através de grupos, de forma que facilite a localização de um dispositivo na lista de computadores onde a solução for instalada.
- Opção para gerar alertas automaticos de integridade, com no mínimo as opções:
- Alterações de hardware,
- Espaço livre de unidades de disco,
- Log de eventos do windows,
- Logons com falha,
- Softwares instalados/desinstalados ou atualizados,
- Status de atualização do S.O windows,

- Status do software antimalware,
- Status do firewall,
- Status do prcesso,
- Status do AutoRun,
- Status dos serviços do windows,
- Tamanho de pasta/arquivo,
- Taxa de transferência de dados no disco,
- Taxa de transferência de dados no disco por processo,
- Temperatura da CPU,
- Temperadtura da GPU,
- Uso de CPU por processo,
- Uso da memória RAM por processo,
- Uso da rede por processo,
- Uso geral da CPU,
- Uso geral da memória Ram,
- Uso geral da rede;
- Última reinicialização da estação de trabalho.
- Os alertas de alterações de hardware, espaço em disco, tamanho de pasta/arquivo e ultima reinicialização do sistema não deverão gerar custo adicional no licenciamento.
- Cada alerta deverá permitir uma personalização da sua severidade, no mínimo: Informativo, Aviso, Erro e Crítico.
- Permitir correção automática através de script remoto.
- Permitir reniciar a máquina, interrempor processo, interromper ou iniciar serviço do windows automaticamente atráves do alerta gerado.
- Possuir opção de plano recomendado, ja com pacote de alertas pré-configurado pra estações de trabalho.

Recursos adicionais, sem vinculo ao licencimento (poderão ser instalados em quantidade ilimitade de máquinas):

- Relatório de pontuação de segurança, com no mínimo os itens:Antimalware, backup, firewall, vpn, criptografia de disco e trafégo NTLM.
- Módulo de controle de dispositivo
- Inventário de Hardware com relatório de registro de alterações, com no mínimo as especificações:
- Nome do Computador;
- Marca/modelo;
- Informações do CPU;
- Velocidade do CPU;
- RAM (Mb);
- Armazenamento total;
- Espaço livre;
- IP externo da máquina;
- Endereço de MAC;
- Endereço de IP;
- Máscara de sub-rede;
- Antiransomware, como detecção e reversão de criptografia.
- Funções padrões do antimalware (proteção de pastas, proteção antimalware, detecção de mineração e quarentena), sem proteção em tempo real, apenas agendada.
- Avaliação e relatório de vulnerabilidades listados pela MITRE.
- Acesso remoto via RDP e HTML.
- Alertas automátcos de alteração do hardware, espaço em disco, tamanho de arquivos/pastas e ultima reinicialização da carga de trabalho.

5. HABILITAÇÃO TÉCNICA

A solução proposta deverá hospedar os dados em Datacenter que possua a certificação da NBR ISO/IEC 27001:2013 e estar localizado em território nacional, sendo que a comprovação deverá ser apresentada na habilitação;

6. OBRIGAÇÕES DA CONTRATADA

Além daquelas determinadas em Leis, Decretos, regulamento e demais dispositivos legais, nas obrigações da CONTRATADA, também incluem:
a) comunicar o Município por escrito, no prazo de 48 horas, quaisquer alterações, acontecimentos ou motivos de força maior que impeçam, mesmo que temporariamente, de garantir o fornecimento total ou parcial;
b) cumprir rigorosamente as solicitações e os prazos de entrega descrito neste termo;
c) assumir, os riscos e as despesas decorrentes da prestação dos serviços, bem como, os encargos sociais e trabalhistas necessários à perfeita execução do objeto do contrato;
d) responsabilizar-se por quaisquer acidentes que venham a ser vítimas seus empregados e/ou terceiros, decorrentes do fornecimento;
e) manter, durante todo o período de execução do contrato, as condições de habilitação jurídica, qualificação técnica, qualificação econômico-financeira e regularidade fiscal exigidas para a contratação, sob pena de suspensão do pagamento e/ou rescisão contratual;
f) apresentar na data de assinatura do contrato, nome, endereço e telefone de profissional da empresa para responder pela execução dos serviços;
g) não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o presente contrato, nem subcontratar a prestação a que esta obrigada;
h) utilizar pessoal uniformizado e identificado com crachá, para entrega do material contratado, sendo este de bom comportamento, podendo ser exigida a substituição, cujo comportamento ou capacidade o Município julgue impróprio ao desempenho dos serviços contratados;
i) não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o presente contrato.
j) manter uma cópia dos dados em um local remoto visando a segurança dos dados em caso de desatre;
k) assegurar a restauração dos dados de forma rápiada e segura;
l) melhoria na qualidade do backup dos dados;
m) replicação do backup em ambiente seguro;
n) ampliação da disponibilidade do backup dos dados (quando necessitar).

7. DO FATURAMENTO E PAGAMENTO

7.1 - O pagamento do valor mensal dos serviços prestados pela CONTRATADA será efetuado pelo Município no prazo de até 30 dias, após a conferência e comprovação de sua execução no período, obedecidas as especificações do **Termo de Referência - Anexo I** deste edital.

7.1.1 - A CONTRATADA emitirá a Nota Fiscal-e até o 5° dia útil do mê subsequente da prestação de serviços.

7.2 - A CONTRATADA apresentará a Nota Fiscal-e dos serviços prestados, na Prefeitura Municipal, na Rua 9 de Outubro, 229, centro, podendo enviá-la ainda, para o e-mail previamente fornecido pelo Município.

7.3 - Para o pagamento do serviço prestado, a CONTRATADA emitirá a Nota Fiscal-e em nome do Município, com obediência ao valor contratado, contendo ainda os dados para depósito bancário vinculado ao CNPJ tomador.

7.4 - Além da Nota Fiscal-e do serviço prestado, a CONTRATADA deverá apresentar sempre que solicitado, os seguintes documentos:

7.4.1 - Prova de regularidade junto a Fazenda Federal, Estadual e Municipal, relativa à sede ou domicílio do proponente, dentro de seu período de validade;

7.4.2 - Prova de regularidade junto ao Fundo de Garantia por Tempo de Serviço/FGTS, dentro de seu período de validade.

7.5 - Serão processadas as retenções previdenciárias nos termos da Lei que regula a matéria.

7.6 - Ocorrendo atraso no pagamento, o valor será corrigido monetariamente pelo Índice nacional de Preços ao Consumidor Amplo/IPCA-IBGE positivo do período, ou outro índice que vier a substituí-lo por Lei, e o Município compensará a detentora da Ata de Registro de Preços com juros de 0,5% ao mês, *pro rata.*

7.7 - Os recursos orçamentários necessários ao suporte das despesas aqui estabelecidas serão suportados com recurso provenientes da seguinte dotação orçamentária:
3750-333904009000000 – Hospedagem de sistemas – SEMAG.

8. DAS OBRIGAÇÕES DO MUNICÍPIO

a) Efetuar regularmente o pagamento, desde que obedecida às cláusulas e condições estabelecidas;
b) Acompanhar a execução dos serviços, podendo recusar qualquer destes, que não esteja de acordo com as normas ou descrições;
c) Sustar a execução de qualquer serviço que esteja sendo feito em desacordo com o Contrato, normas ou orientação formal.

Portão/RS, Março de 2024.

MATHEUS POLO KÖCKE
Diretor dos Serviços de Informática