PROCESSO DE DISPENSA DE LICITAÇÃO Nº 188/2025-

Manifestação de interesse

O **MUNICÍPIO DE TUPANCI DO SUL, TORNA PÚBLICO** que através do Processo de Dispensa de Licitação, pretende dispensar licitação para contratação de solução de proteção de ENDPOINT (antivírus), visa proteger dispositivos da prefeitura municipal de Tupanci do Sul/rs, bem como a contratação de empresa especializada para o fornecimento de serviço de e-mail corporativo, hospedado em servidor cloud dedicado.
As soluções devem proporcionar segurança, desempenho e escalabilidade adequados às necessidades da administração pública, com foco em proteção contra uma ampla gama de ameaças avançadas bem como o gerenciamento centralizado e alta disponibilidade e suporte técnico presencial 8/5 durante todo o período de 3 anos.
Conforme segue:

1. A instalação, configuração, manutenção e suporte técnico deverá se iniciar a partir da assinatura do contrato. Os serviços deverão ser prestados exclusivamente pela contratada, (ficando vedado a subcontratação de outra prestadora de serviço), na modalidade on-site (presencial) com tempo máximo de 1 (uma) hora para atendimento presencial, em todos os setores da Prefeitura Municipal de Tupanci do Sul/RS devendo ser realizada exclusivamente por técnicos especialistas.
2. Chamados técnicos poderão ser abertos em regime 8x5, via internet, chamada telefônica local ou discagem direta, caracterizando a abertura do chamado. Este momento será considerado o início para a contagem dos prazos estabelecidos;
3. Os chamados serão registrados pela Contratada e deverão estar disponíveis para acompanhamento pela equipe da Administração Municipal, contendo data e hora da chamada, o problema ocorrido, a solução, data e hora de conclusão;
4. Os atendimentos aos chamados obrigatoriamente deverão ser realizados por profissionais certificados e deverão ser realizados presencialmente sempre que solicitado pela Administração pública, sendo que a solução para o problema, caso seja atribuída aos equipamentos descritos, deverá ser alcançada em no máximo 24 (vinte e quatro) horas corridas após a abertura do chamado técnico;
5. Deverá a contratada apresentar ao CONTRATANTE a certificação do profissional que irá prestar o suporte, certificação esta que deverá estar vigente durante a vigência do contrato.
6. É vedado a subcontratação de outra empresa para realização dos trabalhos.

Item 1: Solução de Antivirus
2. Especificações Técnicas Mínimas

2. Requisitos Gerais

Tipo de Solução: Software de proteção de endpoints com capacidades de proteção

contra ameaças cibernéticas e gerenciamento de segurança.
Tipo de Licenciamento: Licença por usuário/dispositivo ou baseado em subscrição, conforme o número de endpoints a serem protegidos.
Modelo de Implementação: Solução baseada em nuvem com gerenciamento centralizado e possibilidade de integração com infraestrutura local se necessário.
Parceria com o Fabricante: A contratada deve ser parceira do fabricante da solução, o que indica que a contratada possui habilidades comprovadas com a solução.

3. Certificações Requeridas

A contratada deve possuir em seu quadro de funcionários, no mínimo um profissional com as seguintes certificações:
FCA - Fortinet Certified Associate in Cybersecurity: Necessária para confirmar que o fornecedor possui uma base sólida em segurança cibernética, essencial para a integração e suporte da solução de proteção com a infraestrutura de segurança existente da Fortinet.
Cloud Tech Professional: Exigida para garantir que o fornecedor tenha uma compreensão avançada das soluções de backup e recuperação em nuvem, essenciais para a proteção e recuperação de dados.
Cloud Tech Associate Disaster Recovery: Necessária para assegurar que o fornecedor pode implementar e gerenciar eficazmente as soluções de recuperação de desastres, garantindo a continuidade dos negócios em caso de falhas ou incidentes críticos.
Cloud Tech XDR: A certificação em XDR é fundamental para o profissional responsável pela contratação de soluções de antivírus, pois garante expertise em integrar e analisar dados de diversas fontes, como endpoints, redes, e-mails, servidores e aplicativos em nuvem. Essas integrações permitem uma resposta mais rápida e eficaz contra ameaças cibernéticas, assegurando a melhor escolha para proteger a administração pública.

4. Funcionalidades Principais

Proteção Contra Ameaças:
Antivírus e Antimalware: Detecção e remoção de vírus, malware, ransomware e outras ameaças cibernéticas.
Proteção em Tempo Real: Monitoramento contínuo de atividades suspeitas e bloqueio automático de ameaças.
Filtragem de Conteúdo Web: Bloqueio de sites maliciosos e controle de acesso à internet.
XDR (Extended Detection and Response): Capacidade de fornecer uma visão integrada de eventos de segurança e resposta a ameaças, correlacionando dados de múltiplas fontes (endpoints, rede, e-mail, etc.) para detectar e mitigar ameaças complexas e persistentes.
Detecção Comportamental Avançada:
Mecanismo de Detecção Baseado em Inteligência Artificial: Tecnologia que utiliza IA para identificar e prevenir malware, ransomware e ataques de dia zero através da análise comportamental dos endpoints e sistemas.
Prevenção de Ameaças Desconhecidas: Capacidade de detectar e bloquear ameaças que não são identificadas por assinaturas tradicionais, usando análise comportamental e heurística.
Gerenciamento de Patches:

Atualização Automática de Patches: Implementação automática de atualizações e patches de segurança para sistemas operacionais e aplicativos, garantindo que as vulnerabilidades sejam corrigidas prontamente.
Controle de Dispositivos:
Gerenciamento de Dispositivos Externos: Controle e monitoramento de dispositivos externos conectados aos endpoints, como USBs e dispositivos de armazenamento, para prevenir vazamentos de dados e introdução de malware.
Prevenção Contra Vazamento de Dados (DLP):
Recursos de DLP: Capacidade de implementar políticas de prevenção contra vazamento de dados para proteger informações sensíveis e evitar o envio não autorizado de dados fora da organização.

Isolamento de Endpoints:
Mecanismo de Isolamento: Possibilidade de configurar o isolamento dos endpoints na rede de forma manual ou automática. Isso inclui a capacidade de colocar um endpoint em quarentena ou restringir seu acesso à rede em resposta a comportamentos suspeitos ou confirmações de infecção, garantindo uma resposta rápida a incidentes e minimizando a propagação de ameaças.
Gerenciamento e Relatórios:
Console de Gerenciamento Centralizado: Interface intuitiva para administração e configuração de políticas de proteção em todos os endpoints.
Relatórios e Alertas: Geração de relatórios detalhados sobre status de proteção, eventos de segurança e atividades de segurança. Configuração de alertas para atividades suspeitas e falhas de segurança.
Integração com Ferramentas de Segurança Adicionais:
Integração com Perception-Point: Possibilidade de integrar a solução com a ferramenta de proteção de e-mail da Perception-Point (Advanced Email Security) para fornecer uma camada adicional de proteção contra ameaças de e-mail, como phishing e malware.
Conformidade e Segurança:
Gerenciamento de Patches: Reiterado, confirmando sua importância.
Conformidade com Regulamentações: Suporte a regulamentações de proteção de dados, como LGPD, GDPR, entre outros.
Suporte aos Sistemas/Aplicativos/Virtualizadores:
Compatibilidade: A solução deve suportar uma ampla gama de sistemas operacionais, aplicativos e hipervisores, garantindo que se adapte ao ambiente tecnológico existente.
Recuperação de Arquivos e Notificações de Ameaças:
Resposta a Incidentes de Antimalware: O software deve ser capaz de gerar alertas em tempo real quando um arquivo suspeito for detectado. Além disso, deve interromper imediatamente o processo relacionado ao arquivo malicioso e reverter quaisquer alterações feitas pelo arquivo utilizando o cache de serviços. Isso garante que o sistema seja restaurado ao seu estado seguro anterior à infecção.

Suporte e Atendimento:
Suporte Técnico: Disponibilidade de suporte técnico 8/5 para resolução de problemas e assistência técnica durante todo o período da licença da solução. Com tempo máximo admitido para atendimento presencial de 1 (uma) hora.
Canais de Contato: A contratada deverá oferecer vários canais de contato com a equipe de TI da prefeitura, incluindo um portal de chamados (helpdesk), e-mail e telefones. Esses canais devem estar disponíveis para garantir uma comunicação eficiente e rápida resolução de problemas.
Tempo do atendimento presencial: A empresa contratada deverá prestar suporte técnico de forma presencial, sempre que solicitada, em um prazo máximo de 1 hora, contados a abertura do chamado, sem custos adicionais a contratante. Esta exigência visa assegurar a eficiência e a qualidade do atendimento
O fornecedor deve realizar a instalação, configuração e teste do equipamento na sede da Prefeitura no máximo em 24 horas após a assinatura do contrato, de forma presencial e sem custos adicionais para administração pública.
Treinamento para a equipe técnica da Prefeitura sobre as funcionalidades e administração da solução.
Equipe Certificada: A contratada deve possuir em seu quadro de funcionários, no mínimo um profissional certificado pelo fabricante na categoria "Professional" para gerenciar e operar o equipamento.
Suporte às Demandas de Configuração: A contratada deverá atender todas as demandas de configuração relacionadas ao equipamento solicitadas pela Prefeitura

Quantidade até 50 unidades, nós equipamentos definidos pela administração
Valor unitário R$ 358,00;
Prazo da vigência 3 anos;

Com orçamento proposto de até R$ 17.900,00 (dezessete e novecentos reais) .

Desta forma, de acordo com as disposições do § 3º do art. 75 da Lei Federal nº 14.133, manifesta o interesse da Administração Municipal em obter propostas adicionais de eventuais interessados em até três dias úteis desta publicação.

Os interessados devem enviar as documentação e propostas juntamente:

a) Atestado de Capacidade Técnica emitida por pessoa jurídica de direito público, firmando que o licitante prestou ou presta Serviço de licenciamento de antivírus, e que cumpriu/cumpre com as obrigações assumidas, fornecido por no mínimo 01 (uma) instituição;

b) A empresa licitante deverá possuir em seu quadro funcional no mínimo 1 (um) profissional com formação em Segurança da Informação (junto com comprovante de

especialização de nível superior na área - no mínimo pós-graduação), que será o responsável técnico pelos serviços contratados;

c) 1 (um) profissional com formação em CyberSecurity (junto com comprovante de especialização de nível superior na área - no mínimo pós-graduação);

c) Prova de vínculo dos profissionais, com a empresa licitante, caso não possua vínculo societário, deverá apresentar a Carteira de Trabalho e Previdência Social (CTPS) com o devido registro do empregado.

d) A licitante deverá indicar um responsável técnico dos serviços, de segurança virtual, devendo conter no mínimo: treinamentos em: CompTIA Security + 2, CCNA Cisco Cyberops 2, Gestão de Identidade e Acesso, Sistemas de Detecção e Prevenção de Intrusão, comprovando sua qualificação através de Certificado e/ou atestado de conclusão de cursos relacionados acima.

Documentação deve ser, devidamente formalizadas e assinadas, para o e-mail : licita@tupancidosul.rs.gov.br –informações 54-984226449- www.tupancidosul.rs.gov.br –

Tupanci do Sul/RS, 14 de outubro de 2025

FERNANDO LUIS FAVRETTO,
PREFEITO MUNICIPAL.