

DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA - DFD

1. PREENCHIMENTO PELA ÁREA REQUISITANTE

Área requisitante	INFORMÁTICA
Responsável pela demanda	REGINALDO DO CARMO TOLEDO
Matrícula	2264
E-mail	reginaldotoledo@saae.sp.gov.br
Telefone	1938349449

2. IDENTIFICAÇÃO DA DEMANDA

Item	Descrição	Unid.	Quantidade
26.0263	SOFTWARE ANTIVIRUS PARA ESTACAO E SERVIDOR - LICENÇA 3 ANOS software de antivírus instalado na nuvem do fornecedor com as seguintes especificações técnicas: Detecção e resposta de terminal integrado; análise de causa raiz (com suporte para histórico de 90 dias); ação de resposta remota (shell de comando remoto e quarentena); etiquetagem de técnicas MITR; avisos de atividades suspeitas; análise de ameaças do sandbox em nuvem; aprendizagem de máquina HyperDetect customizável; aprendizagem de máquina no dispositivo baseada em 80.000 características de malware; proteção de memória de exploit ativa; bloqueio de comportamento de processo malicioso; management console para instalação, configuração, atualização, desinstalação e parametrização, com opção de 1, 2 ou 3 anos de licença.	SV	320

Obs.:

3. JUSTIFICATIVA

O uso de software antivírus é uma medida essencial para garantir a integridade, confidencialidade e disponibilidade dos dados armazenados em sistemas computacionais. Esses programas atuam como uma camada de proteção lógica, monitorando, detectando e eliminando vírus e outras ameaças maliciosas que podem comprometer o funcionamento dos computadores e redes.

Vírus, malwares e outras formas de software malicioso são projetados para explorar vulnerabilidades em sistemas operacionais, aplicativos e até no comportamento dos usuários. Um antivírus atualizado é capaz de identificar

padrões de comportamento e assinaturas de ameaças conhecidas, neutralizando-as antes que possam causar danos como perda de dados, roubo de informações sensíveis ou o comprometimento do sistema.

Além disso, o software antivírus tem evoluído para incluir a detecção de ameaças zero-day e ransomware, que são cada vez mais sofisticados e representam riscos significativos para empresas e indivíduos. Ao bloquear essas ameaças, o antivírus contribui para a estabilidade e segurança do ambiente digital, permitindo o uso seguro de recursos online, proteção contra phishing e controle de acessos não autorizados.

Portanto, o antivírus é fundamental não apenas para a proteção individual de dispositivos, mas também para a segurança de redes inteiras, garantindo um ambiente digital confiável e resiliente frente ao crescente número de ameaças cibernéticas.

4. FINALIDADE

O **software essencial para proteção lógica dos computadores contra vírus** tem como finalidade principal garantir a segurança, integridade e desempenho adequado dos sistemas computacionais, protegendo-os contra uma ampla gama de ameaças virtuais, como vírus, malwares, trojans, spyware e ransomwares. Essas ameaças têm a capacidade de comprometer os dados armazenados nos computadores, roubar informações confidenciais, interromper operações críticas e até mesmo danificar fisicamente os equipamentos.

Um antivírus eficiente age de forma preventiva e proativa, identificando e neutralizando ameaças antes que causem danos significativos. Ele opera por meio de diferentes mecanismos, como a análise de comportamento de programas, o escaneamento de arquivos em busca de assinaturas de vírus conhecidos, além de proteger o sistema contra novos tipos de ataques (ameaças zero-day) através de atualizações frequentes e em tempo real.

Além de proteger os computadores de infecções por vírus, o software antivírus contribui para a segurança de redes corporativas ou pessoais, bloqueando tentativas de invasão, phishing e espionagem cibernética, que poderiam comprometer a privacidade e a confidencialidade dos dados. Em um contexto empresarial, essa proteção é ainda mais relevante, pois evita que dados críticos, como informações financeiras e documentos sigilosos, sejam acessados indevidamente ou corrompidos.

Portanto, a finalidade do software antivírus é oferecer uma barreira lógica e robusta contra o amplo espectro de ataques cibernéticos que circulam pela internet, garantindo que o ambiente computacional permaneça seguro, eficiente e sem interrupções, preservando a integridade tanto dos sistemas quanto dos dados que eles armazenam e processam.

5. PREVISÃO DE GASTOS

R\$ 34.500,00 pagamento único após a ativação do antivírus conforme prazos contratuais

6. REQUISITANTE

Nome	REGINALDO DO CARMO TOLEDO
CPF	180703908-08
Cargo	DIRETOR
E-mail	reginaldotoledo@saae.sp.gov.br
Telefone	1938349449

Por este instrumento declaro ter ciência das competências do integrante requisitante, bem como da minha indicação para exercer esse papel na equipe de planejamento da contratação.

Reginaldo do Carmo Toledo
Diretor de Informática
SAAE INDAIATUBA

7. PARTE TÉCNICA

Nome	PAULO SERGIO GRANATO
CPF	10271664827
Cargo	ADMINISTRADOR DE REDES
E-mail	paulo@granato@saae.sp.gov.br
Telefone	1938349469

Por este instrumento declaro ter ciência das competências do integrante técnico, bem como da minha indicação para exercer esse papel na equipe de planejamento da contratação.

Paulo Sérgio Granato
Administrador de Redes
Departamento de Informática

8. ENCAMINHAMENTO

Encaminhe-se à Superintendência para análise e deliberação sobre a pertinência da demanda e o prosseguimento da contratação.

Paulo Sérgio Granato
Administrador de Redes
Departamento de Informática

9. DECISÃO DA AUTORIDADE COMPETENTE

Aprovo a continuidade do procedimento destinado à contratação em tela, considerando a justificativa acima demonstrada e sua compatibilidade aos objetivos desta Administração.

Encaminhe-se à parte técnica para continuidade do procedimento para presente contratação.

Reginaldo do Carmo Toledo