FUNDAÇÃO PRÓ-LAR DE JACAREÍ
Autorização de Execução de Serviço

AS 000023/2024 - Emissão: 24/04/2024

1ª Via - comprador

Endereço: R. José Bonifácio, 37 - Centro, Jacareí - SP, 12327-190
CNPJ: 45.392.032/0001-18
TELEFONE: (12) 3951-6402

Fornecedor:	**AVANT SERVICES LTDA (3806977)**		**29.140.121/0001-10**
Endereço:	**RUA NEO ALVES MARTINS, 2939 - ZONA 01, CEP: 87013060, MARINGA - PR**		
e-Mail:	**CONTATO@AVANTSERVICES.COM.BR**	Contatos:	**(44) 3123-9450 |**
Conta Bancária:	**-**	Agência:	**-** C/C: **-**

Unidades atendidas

Unidade Adm.:	**Fundação Pró-Lar (0001)**
Centro Consumo:	**Diretoria Administrativa e Financeira (003)**
Solic.de Compra:	**000027/2024**

Processo de compra

Número:	**000017/2024**	Modalidade:	**DL - Dispensa de Licitação nº: 000015/2024**
Data:	**18/04/2024**	Artigo:	** Lei 14.133/2021, Art. 75, II*
Comprador:	**FP.ROMUALDO.FRO**		

Aquisição de Serviços licenças software antivírus profissional para proteção de computadores e rede da fundação Pró Lar para prevenção contra fraude de dados Hackers e acesso às informações relevantes por meio de vírus.
A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário a aquisição de uma Solução de Proteção para manter o padrão de proteção atual e reforçar a segurança digital do ambiente

Informação p/execução

Prazo de Execução:	**005 Dias**	Condições de pagamento:	**30 DIAS**
Local para execução do serviço:	**RUA JOSE BONIFÁCIO Nº 37 - CENTRO JACAREÍ**		

Empenho(s)

00313/2024 - Global	**Data:** 24/04/2024	UO: **0601 - PRESIDÊNCIA DA FUNDAÇÃO PRÓ-LAR DE JACAREÍ** UE: **060101 - GABINETE DA PRESIDÊNCIA DA FUNDAÇÃO PRÓ-LAR DE JACAREÍ** 00010 | 060101 | 04.482.0014.2203 | 01 | 110.0000 | 3.3.90.40.99	Valor utilizado: **5.412,00**

ITEM	CLASSIFICAÇÃO E DESCRIÇÃO DO ITEM	QUANTIDADE	VALORES	
			UNITÁRIO	TOTAL
0001	001.030 **SERVIÇO - AQUISIÇÃO DE SOFTWARES DE APLICAÇÃO** *ESPECIFICAÇÃO:* SERVIÇO DE LICENÇAS DE SOFTWARES Característica(s): especializado em licença de uso do software versão equivalente superior, com suporte e atualizações pelo período contratado de 2 anos (24 meses) Analítica de riscos integrada Analise continuamente os riscos de terminais para descobrir e priorizar as configurações incorretas e permitir ações de blindagem automática para remediar vulnerabilidades. Identifique ações e comportamentos de usuários que representam um risco de segurança para sua organização, incluindo fazer login em sites inseguros, gerenciamento de senhas inadequado e uso comprometido do USB. Prevenção e mitigação de ransomware Derrotar o ransomware requer entender todo o kill-chain cibernético e mapear as defesas para cada estágio do ataque. A prevenção e mitigação de ransomware está embutida no Console de Gerenciamento do GravityZone e consiste em: • cópias de backup automáticas e atualizadas à prova de adulteração de arquivos de usuário, sem usar cópias de sombra; • recursos de bloqueio e prevenção (Defesa de Ataques sem Arquivos; Defesa de Ataque de Rede; Antiexploit Avançado; Antimalware de Aprendizagem de Máquina); • múltiplas camadas de detecção (Inspeção de processos, monitoramento de registros,	40,0000	135,3000	5.412,00

AS 000023/2024 - Emissão: 24/04/2024

1ª Via - comprador

ITEM	CLASSIFICAÇÃO E DESCRIÇÃO DO ITEM	QUANTIDADE	VALORES	
			UNITÁRIO	TOTAL
	inspeção de código, Hyper Detect); - tecnologias de mitigação de risco do usuário e do sistema. Analítica de riscos humanos Ajuda a identificar ações e comportamentos do usuário que representam um risco de segurança para a organização, como o uso de páginas da web não criptografadas para fazer login em sites, um gerenciamento deficiente de senhas, uso de pendrives comprometidos na rede da organização, infecções recorrentes, etc. Ao colocar o elemento humano no meio da estratégia de gerenciamento e analítica de riscos, sua organização se torna ainda mais difícil de sofrer uma violação. Defesa em camadas As tecnologias sem assinatura, incluindo aprendizagem avançada de máquina em nuvem e local, análise comportamental, sandbox integrado e blindagem de dispositivos funcionam como proteção altamente eficaz e em camadas contra ameaças sofisticadas. Análise forense do ataque de ponta a ponta A análise forense e a visualização de ataques aumentam o nível de visibilidade do cenário de ameaças da sua organização e revelam o contexto mais amplo de ataques em terminais. Ele permite que você se concentre em ameaças específicas e tome medidas corretivas. Defesa de ataque em rede Detecte e evite ataques de vulnerabilidade de rede. A defesa contra ataques em rede bloqueia ataques de rede, incluindo força bruta, ladrões de senhas e movimento lateral antes que eles possam ser executados. A defesa contra ataques em rede é uma importante fonte de informações para correlações de incidentes de EDR. Sistemas Operacionais Suportados Windows 11 Windows 10 atualização de novembro de 2021 (21H2), Windows 10 atualização de maio de 2021 (21H1), Windows 10 atualização de outubro de 2020 (20H2), Windows 10 atualização de maio de 2020 (20H1), Windows 10 atualização de novembro de 2019 (19H2), Windows 10 atualização de maio de 2019 (19H1), Windows 10 atualização de outubro de 2018 (Redstone 5), Windows 10 atualização de abril de 2018 (Redstone 4), Windows 10 atualização para criadores de outono (Redstone 3), Windows 10 atualização para criadores (Redstone 2), Windows 10 atualização de aniversário (Redstone 1), Windows 10 atualização de novembro (Threshold 2), Windows 10 (RTM, versão 1507), Windows 8.1, Windows 8, Windows 7; Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 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, Amazon Linux AMI 2016.09 ou superior; macOS Monterey (12.x) macOS Big Sur (11.x), macOS Catalina (10.15), macOS Mojave (10.14), macOS High Sierra (10.13), macOS Sierra (10.12); Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7; Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2. Requisitos mínimos de hardware do Centro de Controle CPU T: 4 vCPU com 2 GHz cada Memória RAM mínima: 6 GB recomendado 40 GB de espaço livre em disco rígido Acesso à internet para atualizações e comunicação com terminais remotos e móveis. Requisitos de hardware de terminal Mínimo: CPU single core de 2,4 GHz recomendado: 1,86 GHz ou mais rápido CPU Intel Xeon multicore Memória: RAM livre mínima: 512 MB RAM gratuita recomendada: 1 GB de espaço em disco rígido: 1,5 GB de espaço livre no disco rígido. *UNIDADED DE MEDIDA:* UN			

FUNDAÇÃO PRÓ-LAR DE JACAREÍ
Autorização de Execução de Serviço

AS 000023/2024 - Emissão: 24/04/2024

1ª Via - comprador

ITEM	CLASSIFICAÇÃO E DESCRIÇÃO DO ITEM	QUANTIDADE	VALORES	
			UNITÁRIO	TOTAL
	GARANTIA: 24 MESES			
		TOTAL:		**5.412,00**

(cinco mil quatrocentos e doze reais)

1- O pagamento será efetuado através de crédito em Conta Corrente.
2- Fazer constar no corpo da Nota Fiscal os números desta AF e do Empenho, além da Condição de Pagamento.
3- As notas fiscais decorrentes desta autorização deverão ser emitidas em nome de FUNDAÇÃO PRÓ-LAR DE JACAREÍ, formato este correspondente a inscrição principal do Município no Cadastro Nacional da Pessoa Jurídica (CNPJ).
4- O não cumprimento das especificações e condições desta Autorização de Fornecimento fica sujeito as sanções previstas na Leis Federais 8.666/93 e 14.133/21 e Decreto Municipal 133/93;
5- Horário de entrega: de Segunda-feira a Sexta-Feira, das 8:00 h às 12:00 h e das 13:00 h às 17:00 h, no local indicado, com frete pago.

ALMOXARIFADO PRÓ-LAR
Horário de entrega: de Segunda-feira a Sexta-feira, das 08H00 às 12h00 e das 13h00 às 17h00;
6- A PARTIR DE 1º DE ABRIL DE 2.011, CONFORME LEGISLAÇÃO ESTADUAL VIGENTE, OS MATERIAIS/SERVIÇOS SUJEITOS A INCIDÊNCIA DE ICMS DEVERÃO SER ENTREGUES ATRAVÉS DE NOTA FISCAL ELETRÔNICA. NÃO SERÃO ACEITAS NOTAS FISCAIS MODELO 1 E MODELO 1A.
7 - Condição para recebimento de medicamentos/materiais hospitalares/odontológicos pelo Almoxarifado da Secretaria de Saúde: deverá conter impresso na embalagem os dados de identificação do produto, nome do fabricante, número do lote, data de validade e de fabricação, e armazenagem. No corpo da Nota Fiscal deve conter, além da identificação do produto, o número do lote e data de validade. No caso de medicamentos, as embalagens individuais devem conter inscritas, de forma destacada e não removível a frase: "PROIBIDA A VENDA PELO COMÉRCIO".
8 - DA ANTICORRUPÇÃO – Na execução do presente Contrato é vedado à Administração Municipal Direta e Indireta e à Contratada e/ou o empregado seu, e/ou o preposto seu, e/ou o gestor seu:
Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja, ou a terceira pessoa a ele relacionada;
Criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Contrato; Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;
Manipular ou fraudar o equilíbrio econômico-financeiro do presente Contrato; ou
De qualquer maneira fraudar o presente Contrato; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº12.846/2013 (conforme alterada), do Decreto nº8.420/2015 (conforme alterado) do U.S Foreign Corrupt Practices Act de 1977 (conforme alterado) ou de quaisquer outras leis ou regulamentos aplicáveis (“Leis Anticorrupção”), ainda que não relacionadas com o presente contrato.
O NÃO CUMPRIMENTO DESSA EXIGÊNCIA RESULTARÁ NA RECUSA/RECEBIMENTO DO MATERIAL/SERVIÇO.