FUNDAÇÃO PRÓ-LAR DE JACAREÍ
TxtTituloRelatorio

SC 00027/2024 (PC)

Solicitado em:	**18/04/2024**	Solicitante:	**ROMUALDO FROES RODRIGUES - FP.ROMUALDO.FRO**
Aprovado em:	**18/04/2024**	Aprovador:	**ROMUALDO FROES RODRIGUES - FP.ROMUALDO.FRO**
Unidade solicitante:	**Fundação Pró-Lar - (1)**		
Centro de consumo:	**Diretoria Administrativa e Financeira - (3)**		
Tipo de entrega:	**Única**	Prazo de entrega:	**5 Dias**

Justificativa

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

justifica-se pela necessidade de garantir a continuidade de proteção e segurança do ambiente de informática , principalmente considerando a existência e o aumento contínuo de softwares maliciosos como vírus, trojan, spyware, adware, worms e outros malwares. Uma solução corporativa de antivírus torna-se imprescindível para o bom funcionamento dos computadores e servidores de rede da Fundação Pró-Lar.

PEDIDO DE PRÉ-EMPENHO Nº: 28 **PRÉ-EMPENHO Nº: 160** **SITUAÇÃO DO PRÉ-EMPENHO: Aprovado**

TIPO DE EMPENHO: **Global** DESEMBOLSO: **1**
FICHA: **10**
UNIDADE ORÇAMENTARIA: **0601 - PRESIDÊNCIA DA FUNDAÇÃO PRÓ-LAR DE JACAREÍ**
UNIDADE EXECUTORA: **060101 - GABINETE DA PRESIDÊNCIA DA FUNDAÇÃO PRÓ-LAR DE JACAREÍ**
FUNCIONAL PROGRAMÁTICA: **04.482.0014.2203 - Manutenção dos serviços administrativos do Gabinete da Presidência**
CONTA: **3.3.90.40.00 - Serviços de Tecnologia da Informação e Comunicação - PJ**
ELEMENTO: **3.3.90.40.99 - Outros Serviços de Tecnologia da Informação e Comunicação - PJ**
FONTE DE RECURSO: **01 - Tesouro**
APLICAÇÃO: **110.0000**
FICHA DE CONTAS A PAGAR: **0 - 000000.000 - Contas a pagar**
CENTRO DE CUSTO: **FUNDAÇÃO PRÓ LAR**
TIPO DE DESPESA: **Serviços de tecnologia da informação**
ORDENADOR: **PRISCYLA APARECIDA DE CAMPOS FREIRE MATTOS**

ITEM	LIB.	CLASSIFICAÇÃO E DESCRIÇÃO DO *SERVIÇO*	QUANTIDADE	VALOR ESTIMADO UNITÁRIO	VALOR ESTIMADO 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);	40,0000	135,3000	5.412,00

• múltiplas camadas de detecção (Inspeção de processos, monitoramento de registros, 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

SC 00027/2024 (PC)

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 *LOCAL DE ENTREGA:* Rua José Bonifácio , 37 , Centro			
LIB. = Liberado		**TOTAL:**	**5.412,00**

SALDO DISPONÍVEL NA FICHA NA ELABORAÇÃO DO PRÉ-EMPENHO:	**33.800,10**
VALOR DO PRÉ-EMPENHO:	**5.412,00**
SALDO DISPONÍVEL NA FICHA APÓS A ELABORAÇÃO DO PRÉ-EMPENHO:	**28.388,10**

SC 00027/2024 (PC)

SOLICITANTE
ROMUALDO FROES RODRIGUES

APROVADOR
ROMUALDO FROES RODRIGUES

ORDENADOR
PRISCYLA APARECIDA DE CAMPOS FREIRE MATTOS

Controle Orçamentário - Financeiro:

Data:_____/_____/_____

Ass:_____

Controlador Orçamentário e Financeiro

Data:_____/_____/_____ ( ) Aprovado ( ) Não Aprovado

Francisco José Monteiro