REPÚBLICA DE MOÇAMBIQUE
MINISTÉRIO DA SAUDE
Departamento de Aquisições

Concurso por Cotações n° 58A000141/CC/Nº 0008/FG/2024 – Aquisição de Antivirus Para o MISAU Órgão Central

- Pedido de Cotação –

O Ministério da Saúde pretende adquirir Antivirus Para o MISAU Órgão Central. Assim, vimos pela presente solicitar a V. Excia a apresentar a melhor proposta técnica e financeira, de acordo com as especificações constantes nos Termos de Referência em anexo.

Entrega da Cotação
A proposta deverá ser apresentada até às **15Horas do dia 12 de Agosto de 2024**, a ser entregue em envelope fechado, contendo os documentos abaixo indicados, na Secretária do Departamento de Aquisições (DA), sita na Av. Eduardo Mondlane, n° 1008, R/C, cidade de Maputo, com a indicação no seu exterior do concorrente e do objecto de contratação.

Documentos de Qualificação:
- Certificado de Cadastro Único, correspondente a actividade objecto de contratação;
- Alvará compatível ao objecto de contratação.

Documentos que devem constar na cotação:
- Validade da Proposta: 90 dias, a contar da data de entrega da cotação;
- Condições de pagamento: não haverá adiantamento de pagamento;
- Critérios de Avaliação: Menor Preço Avaliado;
- Anexar 2 (dois) contratos em actividades similares.

O Concurso por Cotação será regido pelo Regulamento de Contratação de Empreitada de Obras Públicas, Fornecimento de Bens e Prestação de Serviços ao Estado, aprovado pelo Decreto n° 79/2022 de 30 de Dezembro.

Maputo, 06 de Agosto de 2024
Autoridade Competente

(Ilegível)

REPÚBLICA DE MOÇAMBIQUE

MINISTÉRIO DA SAÚDE

Termos de Referência para Aquisição de Antivirus Para o MISAU Órgão Central

O Ministério da Saúde, pretende contratar uma empresa para fornecimento de Antivirus para o MISAU Órgão Central. Pelo que, vimos pela presente solicitar a V. Excia a apresentação da proposta técnica e financeira de acordo com os Termos de Referência abaixo indicados.

Objectivo:

- ✓ Aquisição de equipamento e softwares licenciados.

Valor estimado:

- ✓ **700.000,00MT** (Setecentos mil meticais).

Nº Ordem	Designação do Objecto	Quantidade	Nº de Computadores
1	Licenças do tipo renovação da SOLUÇÃO ANTIVÍRUS ENDPOINT SECURITY FOR BUSINESS - SELECT	1	500
2	Licenças do tipo renovação da SOLUÇÃO ANTIVÍRUS ENDPOINT SECURITY FOR BUSINESS - SELECT	1	50
3	Antivirus internet security 3 in 1 + 1	30	N/A

Possibilidade de instalação do software em servidores, estações de trabalho e máquinas virtualizadas, via console de gerenciamento, com opção de remoção de soluções antivírus previamente instaladas;

Console Administrativa:

- Deve permitir administração centralizada por console única de gerenciamento;
- As configurações de antimalware, firewall e IDS deverão ser realizadas por meio da mesma console;
- A console administrativa poderá ser local (on-premise) ou baseada em nuvem;
- Deve haver uma única console de gerenciamento que concentre toda a administração da solução
- A console de gerenciamento deve permitir bloquear as configurações por senha nos endpoints, definindo permissões para que somente o administrador possa alterar as configurações;
- Capacidade de instalar remotamente a solução nos endpoints Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- Capacidade de instalar remotamente, diretamente ou por link, a solução de segurança em smartphones e tablets;
- Capacidade de gerenciar endpoints (Windows, Linux e Mac) protegidos pela solução;
- Capacidade de monitorar diferentes subnets de rede, grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede;
- Deve fornecer informações gerenciais dos endpoints;
- Deve permitir bloquear as configurações do antivírus instalado nos endpoints de maneira que o usuário não consiga alterá-las;
- Capacidade de configurar políticas móveis para que, quando um computador cliente estiver fora da estrutura de proteção da organização, possa atualizar-se via Internet;
- Deve possuir capacidade de exportação de dados para geração de relatórios, incluindo PDF.
- Capacidade de habilitar uma política caso ocorra uma epidemia na rede;

- Capacidade de realizar atualização incremental de vacinas nos endpoints;
- Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- Capacidade de realizar levantamento de hardware dos endpoints;
- Capacidade de realizar levantamento de aplicativos nos endpoints;

Proteção de Endpoints

- Compatibilidade com: Windows 10 e superior; Microsoft Windows Server 2012 x64 e superior; CentOS 7 e superior; Red Hat Enterprise Linux Server 7 e superior; OS X 10.10 e superior; sistemas Android
- Deve possuir as seguintes características:
- Proteção contra malware, incluindo vírus, trojans e worms; 4.6.2. Proteção contra ransomware;
- Proteção contra ameaças de dia zero (zero-day);
- Proteção Web, com verificação de sites e de downloads contra malwares, utilizando filtro URL;
- Proteção de e-mail;
- Firewall gerenciado, com filtragem de pacotes e de aplicativos;
- IDS (Intrusion Detection System);
- Proteção via EDR (Endpoint Detection and Response), capaz de identificar ameaças e comportamentos suspeitos;
- Autoproteção contra-ataques aos serviços/processos da solução de antivírus;
- Proteção baseada em tecnologia de machine learning;
- Gerenciamento de vulnerabilidade de sistemas operacionais;
- Capacidade de integração com sistemas SIEM externos;
- Capacidade de gerenciamento de patches de segurança;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade;
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;
- Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”;

- Capacidade de verificar objetos usando heurística;
- Capacidade de verificar tráfego SSL nos browsers mais utilizados no mercado;
- Possibilidade de adicionar sites da web em uma lista de exclusão;
- Capacidade de analisar as ações de cada aplicação em execução no endpoint, gravando as ações executadas e comparando-as com sequências características de atividades perigosas;
- Capacidade de analisar qualquer tentativa de edição, exclusão ou gravação do registro do Windows;
- Capacidade de analisar dispositivos externos de armazenamento externo removível;
- Capacidade de bloquear execução de aplicativo por blacklist ou por outro modo efetivo;
- Proteção da desinstalação por senha;
- Capacidade de desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com senha;
- Capacidade de pesquisar novos endpoints na rede e criar políticas de instalação da solução;
- Gerenciar o envio de alertas;
- Opção de criar contas com perfis de administração, funções e monitorização;
- Capacidade de exibir informação de utilização de recursos dos endpoint: CPU, memória, disco, entre outros;
- Capacidade de exibir informação sobre os softwares instalados nos endpoints;
- Deve possuir firewall para endpoints gerenciado a partir da console, com filtragem de pacotes e de aplicativos;
- Capacidade de efetuar instalação remota e imediata em equipamentos desprotegidos;
- O agente instalado na máquina cliente deverá ser único, de modo a atender todas as funcionalidades, não sendo permitido o uso de agentes simultâneos;
- Deve possuir criptografia de dados com gerenciamento centralizado;
- Capacidade de criptografar completamente o disco rígido de Endpoints Windows;
- Deve permitir que os administradores atribuam configurações de criptografia;

- Deve fornecer visibilidade global dos endpoints compatíveis com o recurso de criptografia.

Garantia Técnica

Os bens devem tem garantia técnica valida por 1 (um) ano,

Maputo, Agosto de 2024