ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa especializada para fornecimento de subscrição (assinatura) de licença para a solução antivírus corporativo, para atender as necessidades administrativas do Consórcio Intermunicipal de Saúde – CONIMS, de acordo com as condições e especificações constantes no Termo de Referência.

2. QUANTIDADES E ESPECIFICAÇÕES

Nº ITEM	CÓDIGO CONIMS	ESPECIFICAÇÃO/ DESCRITIVO	UNIDADE DE MEDIDA	QUANT.	VALOR UNITÁRIO
1	27010002	Contratação de empresa especializada para o fornecimento de licenças de software de antivírus e suporte pelo período de 3 anos.	UND	200	R$116,48
2	7202159056	Suporte técnico - Pago apenas no chamado quando solicitado	HORAS	60	R$180,00
VALOR TOTAL DO PROCESSO: R$ 34.096,00					

3. ESPECIFICAÇÕES TÉCNICAS

- 200 (duzentas) licenças sendo distribuídas da seguinte forma:
- 09 (nove) servidores internos;
- 191 (cento e noventa e um) computadores utilizados pelo CONIMS e suas unidades.

- A contratação será feita pelo período de 36 (trinta e seis) meses, levando em conta as premissas da administração pública, de maior eficiência, eficácia e economicidade, visto que contratando por esse período, consegue-se uma redução do valor por licença por estação de tratamento devido a fidelização, e o mesmo não terá reajuste durante a vigência contratual, conforme demanda do setor de tecnologia da informação.

3.1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.

3.2. Possuir console central única de gerenciamento. As configurações do Antivírus, Antispyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

3.3. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

3.4. Produto deverá possuir no mínimo os seguintes módulos:

3.5. Console de Gerenciamento fornecendo funcionalidades de gestão;

3.6. Módulos para estações físicas, laptops e servidores;

3.7. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

3.8. CONSOLE DE GERENCIAMENTO – INSTALAÇÃO E CONFIGURAÇÃO

3.8.1. Deverá ser fornecido com base de dados embutido;

3.8.2. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;

3.8.3. O mecanismo de varredura deverá estar disponível para download separadamente;

3.9. CARACTERÍSTICAS GERAIS

3.9.1. Licenciamento flexível;

3.9.2. Arquitetura simples de atualização, com um simples clicar de botão todas as funções e serviços devem ser atualizadas;

3.9.3. Permitir que o administrador escolha qual o pacote será atualizado;

3.9.4. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;

3.9.5. No mínimo enviar notificações:

1) Problemas com licenças;

2) Alertas de Surto de vírus;

3) Máquinas desatualizadas;

4) Eventos de antimalware;

3.10. PAINEL PARA MONITORAMENTO

3.10.1. Baseado em "portlets" configuráveis com no mínimo as seguintes especificações:

1) Nome;

2) Tipo de relatório;

3) Alvo do relatório;

4) Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;

3.11. INVENTÁRIO DA REDE

3.11.1. Possuir no mínimo as integrações abaixo:

1) Múltiplos domínios do Active Directory;

2) Múltiplos VMWare vCenters;

3) Múltiplos Citrix Xen Servers;

4) Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

5) Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;

6) Descoberta de rede para máquinas em grupo de trabalho;

3.11.2. Possuir busca em tempo real pelo menos com os seguintes filtros:

1) Nome;

2) Sistema Operacional;

3) Endereço IP;

4) Possibilitar a instalação remota e desinstalação remota do antivírus;

5) Possibilitar a configuração de pacotes de instalação do produto de antivírus;

6) Possuir tarefas remotas e configuráveis de Scan;

7) Possuir tarefa de reinicialização remota de estação ou servidor;

8) Assinar políticas para no mínimo os níveis:

9) Computador;

10) Máquina Virtual;

OU;

3.11.3. Possuir a propriedade detalhada de objetos gerenciados para:

1) Nome;

2) IP;

3) Sistema Operacional;

4) Grupo;

5) Política Assinada;

6) Último status de malware;

3.12. POLÍTICAS

3.12.1. Modelo único para todos os equipamentos, seja físico ou virtual;

3.12.2. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

3.12.3. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, criptografia, localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

3.13. RELATÓRIOS

3.13.1. Deverá apresentar as seguintes funcionalidades:

1) Relatório para cada serviço de segurança;

2) Facilidade de usar e visualização simplificada;

3) Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

4) Filtros de agendamento de relatórios;

5) Arquivo com todas as instâncias de relatório agendados;

6) Exportar o relatório nos formatos .pdf e/ou .csv;

3.14. QUARENTENA

3.14.1. Restauração remota, com configuração de localidade e deleção;

3.14.2. Criação e exclusão para arquivos restaurados;

3.15. USUÁRIOS

3.15.1. Deverá apresentas no mínimo as seguintes funcionalidades:

3.15.2. Administração baseada em regras;

3.15.3. Disponibilizar tipos de usuários pré-definidos como no mínimo:

3.15.3.1. Administrador – Gerente dos componentes da solução;

3.15. 3.2. Administrador de rede - Gerente dos serviços de segurança;

3.15.3.3. Relatório – Monitora e cria relatórios;

3.15.4. Deverá ser possível customizar um tipo de usuário:

3.15.5. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;

3.16. LOGS

3.16.1. Registrar as ações do usuário no console de gerenciamento;

3.16.2. Detalhar cada ação do usuário;

3.16.3. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

3.17. CERTIFICADO DE SEGURANÇA

3.17.1. Deverá prover o acesso via HTTPS;

3.17.2. Deverá permitir a importação de certificados digitais;

3.17.3. O gerenciamento e a comunicação com dispositivos móveis deverão ser feitos de forma segura utilizando certificados digitais;

3.18. PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS

3.18.1. Deverá apresentar no mínimo:

3.18.2. Deverá permitir a configuração do Scan do antivírus do cliente como:

3.18.3. Scan local;

3.18.4. Scan Hibrido;

3.18.5. Scan Central;

3.18.6. Deverá permitir a instalação customizada do antivírus com no mínimo:

1) Instalar o antivírus sem o controle de acesso à internet; (Windows Workstation)

2) Instalar o antivírus sem o módulo de firewall; (Windows Workstation)

3.18.7. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

1) Windows 10;

2) Windows 8.1;

3) Windows 8;

4) Windows 11;

3.18.8. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

1) Windows Server 2012 R2;

2) Windows Server 2012;

7) Windows Server 2016;

8) Windows Server 2019;

9) Windows Server 2022.

3.18.9. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:

1) Red Hat Enterprise Linux;

2) Cent OS 5.6 ou superior;

3) Ubuntu 10.04 LTS ou superior;

4) SUSE Linux Enterprise Sever 11 ou superior;

5) OpenSUSE 11 ou superior;

6) Fedora 15 ou superior;

7) Debian 5.0 ou superior;

3.19. GERENCIAMENTO E INSTALAÇÃO REMOTA

3.19.1. Deverá permitir ao administrador customizar a instalação;

3.19.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras:

1) Executar o pacote de antivírus diretamente na estação de trabalho

2) Instalar remotamente, distribuído via console de gerencia web;

3) Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

3.19.3. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:

1) Nome;

2) IP;

3) Sistema Operacional;

4) Política Aplicada;

5) Através da console o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;

3.19.4. A console de gerenciamento deverá incluir sessão de log com as seguintes informações:

1) Login;

2) Edição

3) Criação;

4) Log-out;

5) Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits**;**

6) Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

7) A agente utilizada na sincronização deve ser incluída no cliente do antivírus e não ser necessário à distribuição em um agente separado;

3.20. PROTEÇÃO PARA ESTAÇÕES E SERVIDORES VIRTUAIS

PROTEÇÃO DE ANTIVÍRUS DEDICADO PARA AMBIENTES VIRTUAIS

3.20.1. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;

3.20.2. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;

3.20.3. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;

3.20.4. O produto deverá oferecer agente para virtualização dos seguintes produtos:

1) Citrix Xen Server;

2) Microsoft Hyper-V;

3) Hat Virtualization;

4) KVM;

3.21. FUNÇÕES GERAIS

3.21.1. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

3.21.2. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

3.21.3. Requisitos Mínimos do Sistema

3.21.4..Plataformas de Virtualização

3.21.5. VMware vSphere ESX 5.0 ou superior;

3.21.6. VMware vCenter Server 4.1 ou superior;

3.21.7. VMWare Tools 8.6.0;

3.21.8..Citrix XenDesktop 5.0 ou superior;

3.21.9..Xen Server 5.5 ou superior;

3.21.10..Citrix VDI-in-a-Box 5;

3.21.11. Microsoft Hyper-V, 2012

3.21.12. Oracle VM 3.0;

3.21.13..Red Hat Enterprise Virtualization 3.0

3.21.14. Requisitos do Sistema

3.21.15. Sistemas Operacionais desktops:

1) Windows 8.1

2) Windows 8

3) Windows 10

4) Windows 11

3.21.16. Sistemas Operacionais Servidores:

1) Windows Server 2022

2) Windows Server 2019

3) Windows Server 2016

4) Windows Server 2012 R2

5) Windows Server 2012

6) Linux Red Hat Enterprise

7) CentOS 5.6 ou superior

8) Ubuntu 10.04 LTS ou superior

9) SUSE Linux Enterprise Server 11 ou superior

10) OpenSUSE 11 ou superior

11) Fedora 15 ou superior

12) Debian 5.0 ou superior

3.22. COMPONENTES E FUNCIONALIDADE DO ANTIVIRUS GERAL

3.22.1. Deverá fazer scan em tempo real automático;

3.22.2. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

3.22.3. Escaneamento de comportamento heurístico;

3.22.4. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

3.22.5. CD/DVD;

3.22.6. Discos Externos;

3.22.7. Pen-Drivers;

3.22.8. Deverá permitir a escolha e configuração de pastas a ser escaneada;

3.22.9. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:

3.22.10. Baseada em Assinaturas;

3.22.11. Baseada em Heuristica;

3.22.12. Baseada em monitoramento contínuo de processos;

3.22.13. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;

3.22.14. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;

3.22.15. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;

3.23. QUARENTENA

3.23.1. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

3.23.2. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;

3.23.3. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;

3.23.4. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;

3.23.5. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

3.24. CONTROLE DE USUÁRIO

3.24.1. Deverá ter módulo de controle de usuário integrando com as seguintes características:

3.24.2. Bloqueio de acesso à internet;

3.24.3. Bloqueio de acesso a aplicações definidas pelo administrador;

3.25. CONTROLE DO DISPOSITIVO

3.25.1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

3.25.2. Através do módulo de controle de dispositivo deverá ser possível controlar:

1) Bluetooth;
2) CDROM/DVDROM
3) IEEE 1284.4;
4) IEEE 1394;
5) Windows Portable;
6) Adaptadores de Rede;
7) Adaptadores de rede Wireless;
8) Discos Externos;
9) Deverá permitir regras de definição de bloqueio/desbloqueio;
10) Deverá permitir regras de exclusão;

3.26. ATUALIZAÇÃO

3.26.1. Após a atualização o administrador deverá ter a capacidade de adira uma reinicialização;

3.26.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

4. LOCAL E FORMA DA PRESTAÇÃO DE SERVIÇO

4.1.O endereço para a prestação dos serviços será na sede do CONIMS, à Rua Afonso Pena, 1902, Bairro Anchieta – Pato Branco/PR.

4.2. Os serviços deverão ser realizados nos horários de funcionamento do CONIMS (sendo o horário de funcionamento do administrativo, das 07:30 às 11:30 e das 13:00 às 17:00 de segunda à sexta-feira).

4.2.1. Os serviços serão realizados nos seguintes prazos:

A. Fornecimento dos sistemas: imediato, contado a partir da comunicação da ordem de compra/serviços à proponente vencedora/contratada;

B. Implantação (Configuração e habilitação do sistema para uso): 30 (trinta) dias corridos, contado a partir da data de conclusão de fornecimento das licenças de uso dos sistemas e suas instalações;

C. Todas as licenças que compõem a solução devem contar com manutenções corretivas, sem ônus adicional para esse CONIMS, durante o ciclo de vida do software indicado pelo fabricante, para o caso de vícios, defeitos ou falhas.

D. Os softwares a serem licenciados deverão possuir garantia de correção em relação a vícios, defeitos ou falhas durante o ciclo de vida do software indicado pelo fabricante.

E. Treinamento e acompanhamento operacional: 30 (trinta) dias corridos, contado a partir da data de conclusão da implantação do sistema;

F. Por atendimento via conexão remota: atendimento imediato, com prazo de diagnóstico e conclusão variável conforme complexidade da solicitação. O vencedor necessita disponibilizar canais de suporte por telefone, plataforma de atendimento/mensagem instantânea.

4.3. Caso não seja efetivada a execução dos serviços nos prazos acima mencionados, a contratada será NOTIFICADA para que, no prazo de 24 (vinte e quatro) horas, se manifeste a respeito; não o fazendo, proceder-se-á à abertura de processo administrativo para apuração e eventual aplicação das sanções previstas neste Termo de Referência e na Legislação.

5. DESCRIÇÃO DA CONTRATAÇÃO

5.1. Habilitar e contratar como fornecedor/prestador de serviços: **CBA INFORMATICA LTDA,** CNPJ sob nº 80.156.326/0001-41, para fornecimento de subscrição (assinatura) de licença para a solução antivírus corporativo, para atender as necessidades administrativas do Consórcio Intermunicipal de Saúde – CONIMS, de acordo com as condições e especificações constantes neste Termo de Referência.

6. RAZÃO DA ESCOLHA

6.1. A proponente acima apresentou o menor valor conforme cotações anexadas ao processo, estando com a documentação em situação regular.

6.2. A proponente está enquadrada como grande porte. Sendo sua proposta mais vantajosa a esta administração pública, tendo em vista a diferença de valor com as demais participantes deste certame, em conformidade com disposto no art. 49, incisos III e IV da Lei complementar n° 123/06, bem com, em consonância com o princípio da economicidade, que visa obtenção do resultado esperado com o menor custo possível.

7. DOTAÇÃO ORÇAMENTÁRIA

7.1. As despesas geradas em função do objeto ocorrerão por conta da dotação orçamentária:

01.001.10.122.0001.2.001.3.3.90.40.00.00.00.00 fontes 000 e 076.

8. Demais termos e condições estão dispostos na minuta do contrato, anexo V deste termo de referência.

Pato Branco-PR, 26 de março de 2024.

GUILHERME FRESSATO CARVALHO
ENCARREGADO DO SETOR DE TECNOLOGIA E INFORMAÇÃO

B | NoPaper

Data de criação do documento: 27/03/2024 às 16:02:01

Assinantes

✓ GUILHERME FRESSATO CARVALHO

Assinou em 01/04/2024 às 08:11:42 com o certificado avançado da Betha Sistemas

Eu, GUILHERME FRESSATO CARVALHO, estou ciente das normas descritas na Lei nº 14.063/2020, no que se refere a tipos de assinaturas consideradas como válidas para a prática de atos e interações pelos Entes Públicos.

Veracidade do documento

Documento assinado digitalmente.
Verifique a veracidade utilizando o QR Code ao lado ou acesse o site **verificador-assinaturas.plataforma.betha.cloud** e insira o código abaixo:

O9Y R15 6RQ Y7G