TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

O(a) Prefeito Municipal, OSVALDO JURCK, no uso das atribuições que lhe são conferidas pela legislação em vigor, especialmente sob Lei nº 10.520/02 e em face aos princípios ordenados através da Lei nº 8.666/93 e alterações posteriores, a vista do parecer conclusivo exarado pelo Pregoeiro e sua equipe de apoio, resolve:

01 - HOMOLOGAR E ADJUDICAR a presente Licitação nestes termos:

a) Processo Nr.: 166/2013
b) Licitação Nr.: 73/2013-PR
c) Modalidade: PREGÃO PRESENCIAL
d) Data Homologação: 22/10/2013
e) Data da Adjudicação: 22/10/2013 Sequência: 1
f) Objeto da Licitação contratação de empresa especializada em renovação de 250 Licenças de software de proteção corporativa contra vírus, trojans, worms, spywares, adwares e rootkits, para o período de 1 (um) ano, conforme especificação técnica, com serviço de migração da atual solução instalada e treinamento, para a Secretaria de Planejamento, Gestão e Finanças; Secretaria de Educação, Cultura, Esporte e Lazer; Secretaria de Obras e Serviços Urbanos; Secretaria de Saúde e Assistência Social; Secretaria de Agricultur

(em Reais R$)

g) Fornecedores e Itens Vencedores:	Unid.	Qtdade	Descto (%)	Preço Unitário	Total do Item

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

ABILIS TECNOLOGIA LTDA (12407)

1	Renovação de 250 Licenças de software de proteção corporativa contra vírus, trojans, worms, spywares, adwares e rootkits, para o período de 1 (um) ano. Anexo, especificação técnica. Serviço de migração da atual solução instalada e treinamento. Sendo: 8.□Características técnicas do serviço de manutenção do software de proteção corporativa contra vírus para estações de trabalho e servidores de rede: 8.1.□Apresentar abordagem em todo ciclo de vida do vírus; 8.2.□Permitir instalação e desinstalação da solução proposta em estações de trabalho e servidores nas plataformas Microsoft Windows 2000, XP, Server 2003, Vista, 7, 8 e Server 2008, nas arquiteturas 32 e 64bits sem requerer nenhum outro software ou agente previamente instalado e sem a necessidade de reinicialização da estação de trabalho; 8.3.□Permitir a instalação dos clientes em servidores da rede e em estações de trabalho de forma remota através do console de gerenciamento, através de login-script e group policy object (GPO). 8.4.□Instalação e atualização do software sem a intervenção do usuário. 8.5.□Possuir proteção contra remoção do módulo residente em memória e desinstalação do agente de antivírus através de senha específica. 8.6.□Proteção em tempo real contra vírus, trojans, worms, spywares, adwares e rootkits, integrado ao cliente antivírus, sem a necessidade de instalação de agentes ou pacotes adicionais; 8.7.□A solução proposta deverá ser de alta performance e de baixo consumo de recurso de hardware, não devendo ultrapassar a utilização de 128 MB de RAM em estado normal e com todos os módulos de proteção ativos; 8.8.□Geração de backup dos arquivos antes de iniciar o processo de remoção de vírus; 8.9.□Detecção e remoção de vírus de macro em tempo real; 8.10.□Deverá ter a capacidade de bloquear mídias removíveis que se conectem à estação de trabalho, pelo menos para plataformas Microsoft Windows 2000, XP, Server 2003, Vista, 7, 8 e Server 2008; 8.11.□Ferramenta integrada ao cliente antivírus que execute varredura no protocolo POP3 com suporte a Outlook Express, Microsoft Outlook, Windows Live Mail, NetScape e Mozilla Mail ou superior; 8.12.□Deverá detectar, analisar e reparar anexos em mensagens de e-mail dos clientes do Microsoft Exchange via Microsoft Outlook nos protocolos IMAP/POP3/SMTP/HTTP, prevenindo a entrada do vírus antes que o arquivo seja aberto; 8.13.□Ferramenta integrada ao cliente de antivírus que execute varredura no protocolo HTTP e HTTPS para proteção WEB; 8.14.□A solução deverá possibilitar a criação de lista de acesso à web, que contenha endereços de URL, adicionados manualmente, com acesso bloqueado; 8.15.□A solução deverá possibilitar habilitar bloqueio de acesso a listas de categorias de URL pré-programadas; 8.16.□O software deverá possibilitar a criação de lista com endereços URL que serão excluídos da varredura; 8.17.□O software deverá permitir informar e/ou marcar quais aplicativos utilizam acesso à internet para aumentar a segurança ao acesso dos mesmos à web; 8.18.□Permitir adicionar portas alternativas para o rastreamento HTTP e POP3; 8.19.□Permitir configuração de compatibilidade com o cliente de	UN	250	-	32,00	8.000,00

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

8.19. Permitir configuração de compatibilidade com o cliente de e-mail;
8.20. Possuir ferramenta para detecção e remoção de danos causados na estação de trabalho ou servidor por trojans;
8.21. Deverá possuir um repositório de quarentena, para onde são transferidos e armazenados automaticamente os arquivos infectados criptografados;
8.22. Deverá possuir uma opção para restaurar um arquivo em quarentena, sem requerer nenhum outro software e/ou utilitário;
8.23. Fornecer informações sobre características básicas do vírus detectado;
8.24. Bloquear automaticamente o acesso em websites que contenham códigos maliciosos;
8.25. Possuir método de rastreamento de arquivos compactados pelo menos nos formatos PKZIP, ZIP2EXE, LZEXE, ARJ, LZH, PKLITE e Microsoft Compress em pelo menos 15 níveis de compactação e/ou empacotamento;
8.26. Possibilitar a exclusão de arquivos e diretórios da verificação de vírus;
8.27. Emitir alerta ao usuário caso o cliente antivírus, ou as assinaturas de vírus, da sua estação ou servidor não esteja atualizada;
8.28. Não deverá ser necessário reiniciar as estações de trabalho e os servidores para habilitar a proteção do anti-vírus;
8.29. Detecção de atividade de trojans e recuperação de arquivos danificados por estes;
8.30. Detecção e remoção de vírus localizados em drives locais, diretórios e subdiretórios lógicos, programas executáveis, setores de BOOT e vírus de macro em arquivos de aplicativos da suíte Microsoft Office;
8.31. Deve detectar e remover vírus em unidades removíveis, como disquetes e dispositivos USB;
8.32. Deverá possuir facilidade de bloqueio através de senha das configurações do cliente, para que não possam ser alteradas pelos usuários;
8.33. Deve permitir a exclusão de varreduras para determinadas pastas, extensões de arquivo;
8.34. Deverá detectar, analisar e reparar arquivos contaminados por vírus quando acessados, modificados ou criados no disco ou rede, em tempo real;
8.35. Permitir a detecção de futuras ameaças em tempo real, através de análise de execução de código por intenções maliciosas através da tecnologia heurística;
8.36. Rastrear fluxo alternativo de dados (ADS) em sistemas NTFS;
8.37. Deverá remover os vírus de macro dos arquivos Microsoft Office, sem eliminação do conteúdo dos arquivos;
8.38. Possibilitar o rastreamento manual e agendado em todos os servidores da rede;
8.39. Ter a capacidade de detectar arquivos que possam ser potencialmente perigosos;
8.40. Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados, inclusive no prompt de comando, pelo Windows;
8.41. Rastreamento manual com interface Windows, personalizável, com opção de limpeza;
8.42. Rastreamento por linha de comando, parametrizável, com opção de limpeza;
8.43. Programação de rastreamentos automáticos do sistema com opções: todos os drives locais, drives específicos e pastas específicas;
8.44. Ter pelo menos três modos de ação ao detectar malware: apenas exibir alertas, limpar e excluir automaticamente;

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

8.45.□Gerar notificações de eventos de vírus através de alerta na rede NT (EventViewer);
8.46.□Possuir a capacidade de importar e exportar as configurações do cliente através da própria console do antivírus da estação;
8.47.□Possuir ferramentas próprias para realização de backup e restore do servidor de gerenciamento que permita restabelecer o completo funcionamento da solução no caso da ocorrência de um desastre.
8.48.□Descobrir automaticamente as estações da rede que não possuem o cliente instalado.
8.49.□Ter Firewall com:
8.49.1.□Suporte aos protocolos TCP, UDP e ICMP;
8.49.2.□Possibilidade de criar regras diferenciadas por aplicações, por portas locais ou remotas, por protocolos, por direção do tráfego e por endereços de origem ou destino;
8.49.3.□Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo;
9.□Características técnicas da atualização do software de proteção corporativa contra vírus:
9.1.□Atualização automática e incremental das assinaturas de vírus segundo política definida no ambiente de gerência através do protocolo HTTP;
9.2.□Permitir conexão através de serviço proxy padrão SOCKS para a atualização automática;
9.3.□Na atualização automática deverá permitir configuração: horária, diária, semanal, ou mensal em horários definidos;
9.4.□Ter suporte a agente de atualização para clientes móveis a partir do site do fabricante;
9.5.□Deverá permitir a distribuição centralizada de definições de vírus e atualizações dos produtos;
9.6.□Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo usuário;
9.7.□Permitir a utilização de FTP passivo;
9.8.□Uma estação deve poder atualizar qualquer outra estação;
9.9.□Atualizações de software antivírus, engines e lista de assinaturas de vírus automáticas e sem a necessidade de intervenção do administrador.
10.□Características técnicas do ambiente de gerenciamento da solução corporativa de sistema de segurança:
10.1.□Permitir a instalação do servidor de Gerenciamento na plataforma Microsoft Windows Server 2003, 7, 8 e Server 2008;
10.2.□A comunicação entre Cliente e o Servidor deverá ser no mínimo unidirecional (do cliente ao servidor), podendo ser parametrizado qual a frequência de tempo na qual o cliente irá se comunicar com servidor. Essa comunicação deverá ser via protocolo TCP, podendo ser definido qual porta de comunicação será utilizado, bem como poder implementar uma comunicação segura;
10.3.□Ter a possibilidade de utilizar banco de dados externos para armazenamento de toda informação pertinente ao Gerenciamento da solução, como logs, configurações, etc, para pelo menos Microsoft SQL
10.4.□Possibilidade de instalação de quantos servidores de gerenciamento forem necessários, sem limite de licença;
10.5.□A solução deverá suportar implementação baseado em hierarquia de Servidores, onde se possam instalar Servidores de Gerenciamento e atualização da Solução de Antivírus nos sites remotos, para realizar as atualizações de vacinas, motores de varreduras e gerenciamento dos clientes de antivírus instalados

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

varreduras e gerenciamento dos clientes de antivírus instalados no próprio site remoto, e os mesmos sendo apontado para o Servidor de Gerenciamento do Datacenter, onde irão replicar todos logs do site remoto para o Datacenter, bem como obedecer as políticas definidas a partir do Servidor da Solução de Antivírus instalada no Datacenter;
10.6. A configuração da replicação deverá permitir que um administrador possa definir quais as informações que serão transferidas automaticamente para servidores superiores a um intervalo predefinido;
10.7. A comunicação entre Servidor filho (Site Remoto) e o Servidor Pai (Datacenter) deverá ser no mínimo unidirecional (do Site Remoto ao Datacenter), podendo ser parametrizado qual a freqüência de tempo na qual o Servidor do Site Remoto irá se comunicar com o Servidor do Datacenter. Essa comunicação deverá ser via protocolo TCP, podendo ser definido qual porta de comunicação será utilizado, bem como poder implementar uma comunicação segura;
10.8.
10.9. Ser possível administrar todos os servidores da solução de antivírus, bem como visualizar todos os clientes de antivirus instalados nos sites remotos e datacenter, a partir da console de gerenciamento do datacenter;
10.10. Deverá permitir criar políticas de configuração para os clientes de antivírus, para no mínimo, nome da máquina, grupo, endereço IP e intervalo de IPs;
10.11. Deverá ter a capacidade de criar políticas de configuração em níveis hierárquicos; permitir a alteração das configurações nas estações clientes de maneira remota;
10.12. Permitir a atualização incremental das assinaturas de vírus nos clientes (estações e servidores), a partir de um único ponto da rede local;
10.13. Permitir a definição de políticas de atualização das assinaturas de vírus para os clientes (estações e servidores).. Estas atualizações devem ocorrer utilizando protocolo HTTP;
10.14. Realizar o agrupamento dos clientes (estações e servidores) de forma a facilitar a definição de políticas de gerenciamento;
10.15. Permitir a criação de tarefas de verificação de vírus em períodos de tempo pré-determinados;
10.16. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
10.17. Permitir a instalação remota do antivírus para os clientes (estações e servidores) para as plataformas Microsoft WindowsXP, Server 2003, Vista, 7, 8 e Server 2008;
10.18. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão a rede.
11. Características de relatórios:
11.1. Permitir a exportação dos relatórios gerenciais para o formato HTML e PDF.
11.2. Recursos do relatório e monitoramento deverão ser nativos do próprio console central de gerenciamento.
11.3. Possibilidade de gerar relatórios contendo a lista de hosts que possuam o produto instalado, contendo ainda informações como o nome do host, a versão do produto instalado, a versão e/ou a data da assinatura e status.
11.4. Possibilidade de gerar relatórios com informações como: hosts com maior incidência de infecção, malwares com maior ocorrência nos hosts, ataques de rede detectados e usuários dos hosts com maior incidência de infecção.
11.5. Possibilidade de agendamento da geração e envio por e-mail de relatórios.
12. Suporte do fabricante pelo período de 1 (um) ano;

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

12. Suporte do fabricante pelo período de 1 (um) ano.
12.1. As correções (patches) e atualizações do Software deverão ser disponibilizadas para download;
12.2. O fornecedor deverá prestar suporte 5 x 8 (cinco dias por semana, oito horas por dia), fornecido pelo fabricante da solução ou pela revenda do fabricante da solução, por telefone e e-mail, com tempo de resposta não superior a 4 (quatro) horas a partir da hora de registro da chamada técnica, sem limite da quantidade de ocorrências.
12.3. O acesso ao "Knowledge base" on-line, deverá estar disponíveis 24 (vinte e quatro) horas por dia, incluindo documentação de suporte e outros;
12.4. Solicitação de suporte técnico poderá ser aberto no próprio produto, junto ao fabricante.
13. Documentação obrigatória na entrega do objeto:
13.1. Prospectos e manuais eletrônicos em formato PDF, que descrevam e complementem as especificações técnicas, devendo destacar as tecnologias associadas a solução, bem como o modelo proposto.
14. Observações:
14.1. Para atendimento ao Windows 2000 poderá ser disponibilizada de software versão anterior compatível . As políticas disponibilizadas para o Windows 2000 deverão ser as mesmas utilizadas para versões posteriores.
INSTALAÇÃO:
A empresa ofertante do produto deverá realizar a migração da atual solução instalada na municipalidade ESET NOD32 Versão 4 (250 Licenças) para da solução de proteção corporativa ofertada, realizando a configuração de 01 servidor principal, 01 servidor secundário, 10 estações na rede local e 10 estações em rede remota comunicação unidirecional (do cliente ao servidor), de modo que as estações em rede remota sejam gerenciadas pelo servidor principal/secundário e as façam download das atualizações diretamente da fabricante da solução de proteção corporativa.
A configuração atual compõe-se de 04 (quatro) políticas essencialmente semelhantes, diferenciando-se na filtragem de navegação HTTP, ativo, não ativo, lista de URL bloqueadas, atualizações disponibilizadas no servidor principal/secundário ou fabricante da solução de proteção corporativa.
A empresa ofertante deverá oferecer treinamento completo da solução de proteção corporativa ofertada para o mínimo de 02 técnicos com carga horária mínima de 04h.
A configuração realizada pela empresa será acompanhada pela Diretoria de Informática e ao final a empresa deverá repassar todas as senhas utilizadas na configuração da solução de proteção corporativa.
O fornecedor deverá entregar uma documentação da instalação de forma que permita a sua reprodução por um profissional que possua conhecimento e experiência na solução contratada.

Total do Fornecedor: 8.000,00

Total Geral: 8.000,00

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO DE PROCESSO LICITATÓRIO

02 - Autorizar a emissão da(s) nota(s) de empenho correspondente(s).

Dotação(ões): 2.001.3.3.90.39.00.00.00.00 (5), 2.061.3.3.90.39.00.00.00.00 (13), 2.004.3.3.90.39.00.00.00.00 (43), 2.006.3.3.90.39.00.00.00.00 (55), 2.003.3.3.90.39.00.00.00.00 (64), 2.007.3.3.90.39.00.00.00.00 (72), 2.062.3.3.90.39.00.00.00.00 (81), 2.028.3.3.90.39.00.00.00.00 (92), 2.029.3.3.90.39.00.00.00.00 (103), 2.027.3.3.90.39.00.00.00.00 (114), 2.008.3.3.90.39.00.00.00.00 (132), 2.014.3.3.90.39.00.00.00.00 (176), 2.017.3.3.90.39.00.00.00.00 (199), 2.018.3.3.90.39.00.00.00.00 (230), 2.035.3.3.90.39.00.00.00.00 (252), 2.031.3.3.90.39.00.00.00.00 (313), 2.039.3.3.90.39.00.00.00.00 (335), 2.042.3.3.90.39.00.00.00.00 (356)

Schroeder, 22 de Outubro de 2013.

OSVALDO JURCK
PREFEITO MUNICIPAL

Ivandra de Souza
Pregoeiro(a)