	predominante do equipamento principal; c. Cabo de rede UTP CAT6, STP ou superior de 2 (dois) metros para conexão à placa de rede Ethernet. 12. Software e Documentação: a.Licença por unidade entregue, com todos os recursos, sendo na forma de assinatura ou subscrição, para garantir atualizações de segurança gratuitas durante todo o prazo de garantia estabelecida pelo fornecedor de hardware, para o sistema operacional Windows 7 Professional 64 bits ou superior; b.Sistema operacional Windows 8 Professional 64 bits em Português BR instalado e em pleno funcionamento, acompanhado de mídias de instalação e recuperação do sistema e de todos os seus drivers, além da documentação técnica em português necessária à instalação e operação do equipamento; c. Fornecer mídias externas (DVDs) contendo os drivers e o sistema operacional ou a imagem do disco rígido com o sistema operacional e drivers já instalados. 13. Outros Requisitos: a. O objeto bem como seus componentes/periféricos, deverão ser originais de fábrica, novos (sem uso, reforma ou recondicionamento); b. O objeto deverá ser entregue com cabos, adaptadores e conectores necessários ao perfeito funcionamento do mesmo; todos os objetos deverão ser idênticos entre si. c. Caso o componente/periférico não se encontre mais disponível no mercado, deve-se observar que o componente/periférico substituto deve ter, no mínimo, a mesma qualidade e especificação técnica do produto fora de linha; d. Apresentar prospecto (documentação técnica) com as características técnicas detalhadas do objeto, especificando marca, modelo, código do produto (partnumber) e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, possíveis expansões e “upgrades”, comprovando-os através de “folders” e demais literaturas técnicas editadas pelos fabricantes, sendo que a não apresentação não implicará na desclassificação da empresa. e. Serão aceitas cópias das especificações obtidas no sitio na internet do fabricante juntamente com o endereço do sitio; informar na proposta marca modelo e código do produto (partnumber) do objeto; f. Informar na proposta o sítio do fabricante na internet, onde deverá constar no sítio o objeto proposto, como modelo e código do produto (partnumber), com documentação técnica para constatação; 14. Garantia, Suporte, Exigências Comerciais E Qualificação Do Fornecedor: a. O equipamento proposto deverá possuir Garantia do Fabricante do Equipamento de no mínimo 03 (três) anos on-site;					
	VALOR TOTAL					R$ 200.000,00

ATA DE PREGÃO PRESENCIAL POR REGISTRO DE PREÇOS 121/2014
PROCESSO nº 0014416-7/2013
ADA Nº 19-14-0002093
PREGÃO PRESENCIAL SRP Nº. 1164/2013, CPL 04
CLÁUSULA PRIMEIRA - DO OBJETO
Aquisição de equipamentos de informática do tipo estações de trabalho, no-break, notebook e antivírus, no sentido de manter as atividades desta Secretaria de Estado de Saúde do Estado do
Acre, por um período previsto de 12 (doze) meses.
CLÁUSULA SEGUNDA – DO VALOR
O preço da Ata em epígrafe é R$ 105.000,00 (cento e cinco mil reais)
CLÁUSULA TERCEIRA – DA DOTAÇÃO ORÇAMENTARIA
Programa de Trabalho: 4133.0000, 4123.0000, 4124.0000, 4130.0000, 4131.0000, 4132.0000, 3185.0000, 4119.0000, 4121.0000, 4122.0000, 4134.0000, 4125.0000, 4126.0000, 4127.0000, 4128.0000, 4129.0000 e 3184.0000.
Elemento de Despesa: 33.90.39.0000 e 44.90.52.0000.
Fontes de Recursos: 100, 200, 400, 500 e 700.
CLAUSULA QUARTA – DA VIGÊNCIA
A presente Ata de Registro de Preços terá a validade de 12 (doze) meses, a contar da sua assinatura.
COMO GESTOR DE CONTRATO:
DIEGO CANIZIO LOPES.
COMO CO-GESTOR DE CONTRATO:
VITOR DE MATOS HALK
DATA DA ASSINATURA: 19/03/2014

ASSINAM: IRAILTON DE LIMA SOUSA pela Secretaria de Estado de Saúde e JOSE MURILO CIRINO NOGUEIRA JUNIOR representante da empresa JOSÉ MURILO CIRINO NOGUEIRA JUNIOR (ME).

ENCARTE I
Relação do(os) Fornecedor(es)/Preços Registrados por ocasião do Pregão Presencial para Registro de Preços Nº 1164/2013, CPL 04

EMPRESA: JOSÉ MURILO CIRINO NOGUEIRA JUNIOR (ME), Pessoa Jurídica de Direito Privado, inscrita no CNPJ nº. 05.250.796/0001-54, estabelecida a Avenida Rui Barbosa, nº 3373, Bairro Dionisio Torres, CEP: 60.115-222, Fortaleza – CE, Telefones: (85) 3224.9185 e 9146.7336, E-mail: diretoria@networksecure.com.br,

Item	Descrição	UND	Marca	Quant. para Registro	Valor Unit. Adjudicado	Valor Total R$
	Licença de antivírus 1. Servidor de Administração e Console Administrativa 1.1. Compatibilidade: 1.1.1. Microsoft Windows Server 2003 ou superior 1.1.2. Microsoft Windows Server 2003 x64 ou superior 1.1.3. Microsoft Windows Server 2008 1.1.4. Microsoft Windows Server 2008 Core 1.1.5. Microsoft Windows Server 2008 x64 SP1 1.1.6. Microsoft Windows Server 2008 R2 1.1.7. Microsoft Windows Server 2008 R2 Core 1.1.8. Microsoft Windows Server 2012 x64 1.1.9. Microsoft Windows Server 2012 x64 1.1.10. Microsoft Windows XP Professional SP2 ou superior 1.1.11. Microsoft Windows XP Professional x64 1.1.12. Microsoft Windows Vista SP1 1.1.13. Microsoft Windows Vista x64 SP1 1.1.14. Microsoft Windows Seven 1.1.15. Microsoft Windows Seven x64 1.2. Características: 1.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC; 1.2.2. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade 1.2.3. Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores; 1.2.4. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active					

04	Directory; 1.2.5. Capacidade de instalar remotamente a solução de segurança em smartphones Symbian, Windows Mobile, Blackberry e Android, utilizando estações como intermediadoras; 1.2.6. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus; 1.2.7. Capacidade de gerenciar smartphones (tanto Symbian quanto Windows Mobile, Blackberry e Android) protegidos pela solução antivírus; 1.2.8. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto; 1.2.9. Capacidade de atualizar os pacotes de instalação com as últimas vacinas, para que quando o pacote for utilizado em uma instalação já contenha as últimas vacinas lançadas; 1.2.10.Capacidade de fazer deployment (distribuição) remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes; 1.2.11.Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores 1.2.12. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas; 1.2.13.Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção; 1.2.14.Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção; 1.2.15.Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente; 1.2.16. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.; 1.2.17.Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos; 1.3. Deve fornecer as seguintes informações dos computadores: 1.3.1. Se o antivírus está instalado; 1.3.2. Se o antivírus está iniciado; 1.3.3. Se o antivírus está atualizado; 1.3.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo; 1.3.5. Minutos/horas desde a última atualização de vacinas 1.3.6. Data e horário da última verificação executada na máquina; 1.3.7. Versão do antivírus instalado na máquina; 1.3.8. Se for necessário reiniciar o computador para aplicar mudanças; 1.3.9. Data e horário de quando a máquina foi ligada; 1.3.10.Quantidade de vírus encontrados (contador) na máquina; 1.3.11.Nome do computador; 1.3.12.Domínio ou grupo de trabalho do computador; 1.3.13.Data e horário da última atualização de vacinas; 1.3.14. Sistema operacional com Service Pack; 1.3.15.Quantidade de processadores; 1.3.16.Quantidade de memória RAM; 1.3.17.Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory); 1.3.18. Endereço IP; 1.3.19.Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido. 1.3.20.Atualizações do Windows Updates instaladas 1.3.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD 1.3.22.Vulnerabilidades de aplicativos instalados na máquina 1.4. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterara-las; 1.5. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: 1.5.1. Mudança de gateway; 1.5.2. Mudança de subnet DNS; 1.5.3. Mudança de domínio; 1.5.4. Mudança de servidor DHCP; 1.5.5. Mudança de servidor DNS; 1.5.6. Mudança de servidor WINS; 1.5.7. Aparecimento de nova subnet; 1.6. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet; 1.7. Capacidade de instalar outros servidores administrativos para balancear a carga e aperfeiçoar tráfego de link entre sites diferentes; 1.8. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus; 1.9. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos; 1.10. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede; 1.11. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo. 1.12. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML. 1.13. Capacidade de gerar traps SNMP para monitoramento de eventos; 1.14. Capacidade de enviar e-mails para contas específicas em caso de algum evento; 1.15. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server; 1.16. Deve possuir compatibilidade com Cisco Network Admission Control (NAC); 1.17. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo). 1.18. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor; 1.19. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de	UND	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT	1.500	70,00	105.000,00

	tempo); 1.20. Capacidade de realizar atualização incremental de vacinas nos computadores clientes; 1.21. Capacidade de reportar vulnerabilidades presentes nos computadores. 1.22. Capacidade de realizar inventário de hardware de todas as máquinas clientes 1.23. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes 1.24. Capacidade de diferenciar máquinas virtuais de máquinas físicas 2. Estações Windows – 2.1. Compatibilidade: 2.1.1. Microsoft Windows XP Professional SP3 2.1.2. Microsoft Windows XP Professional x64 Edition SP2 2.1.3. Microsoft Windows Vista SP2 2.1.4. Microsoft Windows Vista x64 Edition SP2 2.1.5. Microsoft Windows Seven Professional/Enterprise/Ultimate 2.1.6. Microsoft Windows Seven Professional/Enterprise/Ultimate x64 2.1.7. Microsoft Windows 8 2.1.8. Microsoft Windows Embedded Standard 7 SP1 2.1.9. Microsoft Windows Embedded Standard 7 x64 Edition SP1 2.1.10. Microsoft Windows Embedded POS Ready 2009 com SP maisatual 2.2. Características: 2.2.1. Deve prover as seguintes proteções: 2.2.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; 2.2.3. Antivírus de Web (módulo para verificação de sites e downloads contra vírus) 2.2.4. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos) 2.2.5. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, Google Talk, etc.) 2.2.6. Firewall com IDS 2.2.7. Autoproteção (contra ataques aos serviços/processos do antivírus) 2.2.8. Controle de dispositivos externos 2.2.9. Controle de acesso a sites por categoria 2.2.10.Controle de execução de aplicativos 2.2.11.Controle de vulnerabilidades do Windows e dos aplicativos instalados 2.2.12.Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota; 2.2.13.As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa). 2.2.14.Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução; 2.2.15.Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 2.2.16.Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado; 2.2.17.Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas; 2.2.18. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks); 2.2.19.Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 2.2.20.Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo; 2.2.21.Capacidade de verificar somente arquivos novos e alterados; 2.2.22.Capacidade de verificar objetos usando heurística; 2.2.23.Capacidade de agendar uma pausa na verificação; 2.2.24.Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado; 2.2.25.O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: 2.2.25.1. Perguntar o que fazer, ou; 2.2.25.2. Bloquear acesso ao objeto; 2.2.25.3. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração préestabelecida pelo administrador); 2.2.25.4. Caso positivo de desinfecção: 2.2.25.5. Restaurar o objeto para uso; 2.2.25.6. Caso negativo de desinfecção: 2.2.25.7. Mover para quarentena ou apagar (de acordo com a configuração préestabelecida pelo administrador); 2.2.26.Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto. 2.2.27.Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL); 2.2.28.Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings; 2.2.29.Capacidade de verificar links inseridos em e-mails contra phishings; 2.2.30.Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera; 2.2.31. Capacidade de verificação de corpo e anexos de e-mails usando heurística; 2.2.32.O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve: 2.2.32.1. Perguntar o que fazer, ou; 2.2.32.2. Bloquear o e-mail; 2.2.32.3. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração préestabelecida pelo administrador); 2.2.32.4. Caso positivo de desinfecção: 2.2.32.5. Restaurar o e-mail para o usuário; 2.2.32.6. Caso negativo de desinfecção: 2.2.32.7. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador); 2.2.33.Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena. 2.2.34. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados. 2.2.35.Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador, com a possibilidade de restauração de um anexo deletado; 2.2.36.Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas; 2.2.37.Deve ter suporte total ao protocolo IPv6; 2.2.38.Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail; 2.2.39.Na verificação de tráfego web, caso encontrado código malicioso o programa deve: 2.2.39.1. Perguntar o que fazer, ou; 2.2.39.2. Bloquear o acesso					

	ao objeto e mostrar uma mensagem sobre o bloqueio, ou; 2.2.39.3. Permitir acesso ao objeto; 2.2.40.O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes: 2.2.40.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou; 2.2.40.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação. 2.2.41. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web. 2.2.42.Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas. 2.2.43.Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa. 2.2.44.Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas. 2.2.45.Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/). 2.2.46.Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica; 2.2.47.Deve possuir módulo IDS (Intrusion Detection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas. 2.2.48.O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: 2.2.48.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 2.2.48.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados. 2.2.49.Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: 2.2.49.1. Discos de armazenamento locais; armazenamento removível; Impressoras; CD/DVD; Drives de disquete; Modems; Dispositivos de fita; Dispositivos multifuncionais; Leitores de smartcard; Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth. 2.2.50.Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário. 2.2.51.Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário. 2.2.52. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento. 2.2.53.Capacidade de configurar novos dispositivos por Class ID/Hardware ID 2.2.54.Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento. 2.2.55.Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do aplicativo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.). 2.2.56.Capacidade de bloquear execução de aplicativo que está em armazenamento externo. 2.2.57.Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo. 2.2.58.Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web. 2.2.59.Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web. 3. Estações de trabalho Linux – Compatibilidade: 3.1. Plataforma 32-bits: 3.1.1. Red Hat Enterprise Linux 5.5 Desktop 3.1.2. Red Hat Enterprise Linux 6 Desktop 3.1.3. Fedora 14 3.1.4. CentOS-5.5 3.1.5. SUSE Linux Enterprise Desktop 10 SP3 3.1.6. SUSE Linux Enterprise Desktop 11 SP1 3.1.7. openSUSE Linux 11.3 3.1.8. Debian GNU/Linux 6.0.1 3.1.9. Mandriva Linux 2010 3.1.10. Ubuntu10.04 LTS Desktop Edition 3.1.11. Plataforma 64-bits: 3.1.12.RedHat Enterprise Linux 5.5 3.1.13.Red Hat Enterprise Linux 6 Desktop 3.1.14. Fedora 14 3.1.15.CentOS-5.5 3.1.16. SUSE Linux Enterprise Desktop 10 SP3 3.1.17. SUSE Linux Enterprise Desktop 11 SP1 3.1.18. openSUSE Linux 11.3 3.1.19.Debian GNU/Linux 6.0.1 3.1.20.Ubuntu10.04 LTS Desktop 3.2. Características: 3.2.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; 3.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora. 3.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 3.2.4. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 3.2.5. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes; 3.2.6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; 3.2.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. 3.2.8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; 3.2.9. Capacidade de pausar automaticamente					

	varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 3.2.10.Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo; 3.2.11.Capacidade de verificar objetos usando heurística; 3.2.12. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena 3.2.13. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados 3.2.14.Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux). 4. Servidores Windows –Compatibilidade: 4.1. Microsoft Windows Small Business Server 2008 Standard x64 4.2. Microsoft Windows Small Business Server 2011 Essentials/Standard x64 4.3. Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64 4.4. Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64 4.5. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64 4.6. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64 4.7. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1 4.8. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1 4.9. Microsoft Windows Hyper-V Server 2008 R2 SP1 4.10. Microsoft Terminal baseado em Windows Server 2003 4.11. Microsoft Terminal baseado em Windows Server 2008 4.12. Microsoft Terminal baseado em Windows Server 2008 R2 4.13. Citrix Presentation Server 4.0 e 4.5 4.14. Citrix XenApp 4.5, 5.0 e 6.0 4.15. Características: 4.15.1.Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; 4.15.2.Autoproteção contra ataques aos serviços/processos do antivírus 4.15.3. Firewall com IDS 4.15.4.Controle de vulnerabilidades do Windows e dos aplicativos instalados 4.15.5.Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota; 4.15.6.As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora. 4.15.7.Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 4.15.8.Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 4.15.9.Gerenciamento de tarefa (criar ou excluir tarefas de verificação) 4.15.10. Leitura de configurações 4.15.11. Modificação de configurações 4.15.12. Gerenciamento de Backup e Quarentena 4.15.13. Visualização de relatórios 4.15.14. Gerenciamento de relatórios 4.15.15. Gerenciamento de chaves de licença 4.15.16. Gerenciamento de permissões (adicionar/excluir permissões acima) 4.15.17. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: 4.15.18. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 4.15.19. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados. 4.15.20. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total. 4.15.21. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.) 4.15.22. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS) 4.15.23. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares; 4.15.24. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor. 4.15.25. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor. 4.15.26. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas. 4.15.27. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 4.15.28. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qual quer objeto detectado com o veredicto escolhido seja ignorado; 4.15.29. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 4.15.30. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo; 4.15.31. Capacidade de verificar somente arquivos novos e alterados; 4.15.32. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.) 4.15.33. Capacidade de verificar objetos usando heurística; 4.15.34. Capacidade de configurar diferentes ações para diferentes tipos de ameaças; 4.15.35. Capacidade de agendar uma pausa na verificação; 4.15.36. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado; 4.15.37. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: 4.15.37.1. Perguntar o que fazer, ou; 4.15.37.2. Bloquear acesso ao objeto; 4.15.37.3. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração préestabelecida pelo administrador); 4.15.37.4. Caso positivo de desinfecção: 4.15.37.5. Restaurar o objeto para uso; 4.15.37.6. Caso					

	negativo de desinfecção: 4.15.37.7. Mover para quarentena ou apagar (de acordo com a configuração préestabelecida pelo administrador); 4.15.37.8. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto. 4.15.38. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena 4.15.39. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados 4.15.40. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa. 5. Servidores Linux –Compatibilidade: 5.1. Plataforma 32-bits: 5.1.1. Red Hat Enterprise Linux 6 Server; 5.1.2. Red Hat Enterprise Linux 5.5 Server 5.1.3. Fedora 14; 5.1.4. CentOS-5.5; 5.1.5. SUSE Linux Enterprise Server 11 SP1; 5.1.6. Novell Open Enterprise Server 2 SP3; 5.1.7. OpenSUSE Linux 11.3; 5.1.8. Mandriva Enterprise Server 5.2; 5.1.9. Ubuntu 10.04.2 LTS Server; 5.1.10.Debian GNU/Linux 6.0.1; 5.1.11. FreeBSD 7.4; 5.1.12. FreeBSD 8.2. 5.1.13. Plataforma 64-bits: 5.1.14.Red Hat Enterprise Linux 6 Server; 5.1.15.Red Hat Enterprise Linux 5.5 Server 5.1.16. Fedora 14; 5.1.17.CentOS-5.5; 5.1.18. SUSE Linux Enterprise Server 11 SP1; 5.1.19.Novell Open Enterprise Server 2 SP3; 5.1.20. openSUSE Linux 11.3; 5.1.21.Ubuntu 10.04.2 LTS Server; 5.1.22.Debian GNU/Linux 6.0.1; 5.1.23. FreeBSD 7.4; 5.1.24. FreeBSD 8.2. 5.2. Características: 5.2.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; 5.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora. 5.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 5.2.4. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 5.2.5. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes; 5.2.6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; 5.2.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. 5.2.8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; 5.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 5.2.10.Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo; 5.2.11.Capacidade de verificar objetos usando heurística; 5.2.12. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena 5.2.13. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados 5.2.14.Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux) 6. Smartphones - Compatibilidade: 6.1.1. Symbian OS 9.1, 9.2 Series 60 e Symbian^3 6.1.2. Windows Mobile 5.0, 6.0, 6.1 e 6.5 6.1.3. BlackBerry 4.5, 4.6, 4.7, 5.0 e 6.0 6.1.4. Android OS 1.5, 1.6, 2.0, 2.1, 2.2 e 2.3 6.2. Características: 6.2.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de: 6.2.2. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser. 6.2.3. Arquivos abertos no smartphone 6.2.4. Programas instalados usando a interface do smartphone 6.2.5. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento; 6.2.6. Deverá isolar em área de quarentena os arquivos infectados; 6.2.7. Deverá atualizar as bases de vacinas de modo agendado; 6.2.8. Deverá bloquear spams de SMS através de Black lists; 6.2.9. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado; 6.2.10.Deverá ter função de limpeza de dados pessoais à distância, em caso de roubo, por exemplo. 6.2.11.Deverá ter firewall pessoal; 6.2.12. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1 6.2.13. Possibilidade de instalação remota utilizando o Sybase Afaria 6.5 6.3. Outros Requisitos: 6.3.1. O objeto bem como seus componentes/periféricos, deverão ser originais de fábrica, novos (sem uso, reforma ou recondicionamento); 6.3.2. Caso o componente/periférico não se encontre mais disponível no mercado, devese observar que o componente/periférico substituto deve ter, no mínimo, a mesma qualidade e especificação técnica do produto fora de linha; 6.3.3. Apresentar prospecto (documentação técnica) com as características técnicas detalhadas do objeto, especificando marca, modelo, código do produto (partnumber) e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, possíveis expansões e “upgrades”, comprovando-os através de “folders” e demais literaturas técnicas editadas pelos fabricantes, sendo que a não apresentação não implicará na desclassificação da empresa. 6.3.4. Serão aceitas cópias das especificações obtidas no sitio na internet do fabricante juntamente com o endereço do sitio; informar na proposta marca modelo e código do produto (partnumber) do objeto; 6.3.5. Informar na proposta o sítio do fabricante na internet, onde deverá constar no sítio o objeto proposto, como modelo e código do produto (partnumber), com documentação técnica para constatação; 7. Informações Adicionais: 7.1. A Solução deve ser fornecida com os componentes necessários para sua completa instalação e o perfeito funcionamento da solução; 8. Garantia E Suporte: 8.1. O software proposto deverá possuir Garantia, Suporte e Subscrição de no mínimo 03 (três) anos do fabricante;					
	VALOR TOTAL					R$ 105.000,00