MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO
GABINETE DA REITORIA
Rua do Rouxinol, 115 - Bairro do Imbuí - CEP: 41720052 - Salvador-BA
E-mail: gabinete@ifbaiano.edu.br

OF Nº. 093/2012/IF BAIANO/GAB.

Salvador, 07 de fevereiro de 2012.

À Sua Senhoria
Manoel Alves Bezerra Junior
Pró-Reitor de Administração
Universidade Federal de Roraima

Assunto: Aquisição de software aplicativo.

Prezado Senhor,

Solicitamos a Vossa Senhoria adesão a Ata de Registro de preço número **0101/2011** da **Universidade Federal de Roraima.** A seguir as informações do item para aquisição.

Item	Descrição	Fornecedor	Qtd.
001	SOFTWARE APLICATIVO	RPJ COMERCIO E SERVICOS DA AMAZONIA LTDA	1300

Atenciosamente,

NILTON SANTANA DOS SANTOS
Reitor Substituto

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE RORAIMA
PRÓ-REITORIA DE ADMINISTRAÇÃO E DESENVOLVIMENTO SOCIAL

Ofício nº 49/2012-PRADS/UFRR.

Boa Vista, 08 de Fevereiro de 2012.

Ao
Instituto Federal de Educação, Ciência e Tecnologia Baiano.
GABINETE DA REITORIA.
Nilton Santana dos Santos.
Reitor Substituto.

Assunto: Ata de Registro de Preço - Pregão Eletrônico nº 101/2011-UFRR.

Senhora Diretora,

Ao cumprimentá-lo, em resposta ao Ofício nº 93/2012 – IFº BAIANO / GAB, datado de 07 de Fevereiro de 2012, informamos que a Universidade Federal de Roraima autoriza essa UG a fazer uso da Ata de Registro de Preços do Pregão Eletrônico 101/2011 - UFRR, na condição de UG Não Participante, para contratar, nos termos, condições e especificações contidas na Ata de Registro de Preços e no edital do certame licitatório.

Na oportunidade, solicitamos que verifiquem junto ao fornecedor se os mesmos poderão atendê-los, e informamos que a Ata de Registro de Preços e o Resultado por Fornecedor estão disponíveis no site comprasnet.gov.br – cod. desta UG-154080.

Atenciosamente,

Manuel Alves Bezerra Junior.
Pró-Reitor de Administração e
Desenvolvimento Social.

Nilton de Santana dos Santos
Reitor Substituto

END.: Av. Ene Garcêz, 2413, Aeroporto, Campus do Parelarima, Boa Vista-RR, CEP 69304-000, Fone/FAX: 3621-3113
E-mail: junior@prads.ufrr.br ou prads@ufrr.br

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO
GABINETE DA REITORIA
Rua do Rouxinol,115 - Bairro do Imbuí - CEP: 41720052 - Salvador-BA
E-mail: gabinete@ifbaiano.edu.br

OF Nº. 092/2012/IF BAIANO/GAB.

Salvador, 07 de fevereiro de 2011.

À Sua Senhoria
Milena Cabral
Analista de Licitações
RPJ COMERCIO E SERVIÇOS DA AMAZONIA LTDA

Assunto: Aquisição de software aplicativo.

Prezada Senhora,

Solicitamos a Vossa Senhoria adesão a **Ata de Registro de preço número 0101/2011 da Universidade Federal de Roraima.** A seguir as informações do item para aquisição.

Item	Descrição	Fornecedor	Qtd.
001	SOFTWARE APLICATIVO	RPJ COMERCIO E SERVICOS DA AMAZONIA LTDA	1300

Atenciosamente,

NILTON SANTANA DOS SANTOS
Reitor Substituto

Multcom
Soluções e Conectividade

10 anos

Manaus/AM, 08 de Fevereiro de 2012.

Ao
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia Baiano.
A/C: Sr. Nilton Santana dos Santos
Reitor Substituto

Em resposta ao ofício nº 092/2012-IF BAIANO/GAB

Assunto: Adesão a Ata de Registro de Preços.

A RPJ Comércio e Serviços da Amazônia Ltda., inscrita no CNPJ sob o nº 05.047.556/0001-57, sediada à Rua Manoel Marques de Souza, nº. 01 Bairro Parque Dez, Manaus-AM, por intermédio de seu representante legal o Sra. Milena Cabral de Figueiredo Palva, portador da identidade nº. 1374802-5 SSP/AM, e CPF nº. 633.384.912-04, vêm por meio desta, informar que:
Em resposta ao ofício nº 092/2012-IF BAIANO/GAB, solicitando adesão à ata do Pregão Eletrônico nº 101/2011, da unidade Gestora 154080-UFRR, informamos nosso, parecer favorável nos termos, condições e especificações contidas nas Atas supracitadas.

Desta forma aproveitamos a oportunidade para agradecer e colocar-nos a disposição para qualquer informação ou esclarecimento que julgar necessário.

Certos de sua compreensão,

05.047.556/0001-57
RPJ COMÉRCIO E SERVIÇOS
DA AMAZÔNIA LTDA
Rua Manoel Marques de Souza, 01
Cj. Castelo Branco Pq. Dez
Cep: 69.055-240
Manaus AM

Atenciosamente,

Milena Cabral
Analista de Licitações
92 3236-0196
licitacoes@multcom.com

Distribuidor:

TELCON

Manaus-AM, 08 de Fevereiro de 2012.

Ao
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Clência e Tecnologia Baiano.
A/C: Sr. Nilton Santana dos Santos
Reitor Substituto

Empresa: RPJ Comércio e Serviços da Amazônia Ltda
CNPJ: 05.047.556/0001-57
Endereço: Rua Manoel Marques de Souza, nº. 01 Cj. Castelo Branco P-10 Manaus/AM CEP: 69055-240
Telefone: (92) 3236-0196 Fax: (92) 3236-7284
E-mail: licitacoes@multcom.com

PROPOSTA DE PREÇOS PRODUTOS

ITEM	DESCRIÇÃO	UND	Qtd	VALOR UNITÁRIO R$	VALOR TOTAL R$
01	**LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR 36 (TRINTA E SEIS) MESES:** **REQUISITOS MÍNIMOS:** 2.1Servidor de Administração e Console Administrativa a.Compatibilidade: 1.1.1Microsoft 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 1.1.5Microsoft Windows Server 2008 x64 SP1 1.1.6Microsoft Windows Server 2008 R2 1.1.7Microsoft Windows Server 2008 R2 Core 1.1.8 Microsoft Windows XP Professional SP2 ou superior 1.1.9 Microsoft Windows XP Professional x64	UN	1300	**R$ 47,00**	**R$ 61.000,00**

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

	1.1.10 Microsoft Windows Vista SP1 1.1.11Microsoft Windows Vista x64 SP1 1.1.12 Microsoft Windows Seven 1.2Características: 1.2.1 A console deve ser acessada via WEB (HTTPS) ou MMC; 1.2.2 Capacidade de remover remotamente qualquer solução de anti-virus (própria ou de terceiros) que estiver presente nas estações e servidores; 1.2.3 Capacidade de instalar remotamente a solução de anti-virus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory; 1.2.4Capacidade de instalar remotamente a solução de segurança em smartphones Symbian, Windows Mobile e BlackBerry, utilizando estações como intermediadoras; 1.2.5 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivirus; 1.2.6 Capacidade de gerenciar smartphones (tanto Symbian quanto Windows Mobile e BlackBerry) protegidos pela solução anti-virus; 1.2.7 Deve gerenciar todos os módulos das soluções acima em uma única console. 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				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 -- Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCOM

	software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de anti-virus para que seja instalado nas máquinas clientes; 1.2.11 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas; 1.2.12Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção; 1.2.13Capacidade 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; 1.2.14Capacidade 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 antivirus instalado. Caso não possuir, deve instalar o anti-virus automaticamente; 1.2.15Capacidade 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; 1.2.16Capacidade 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; 1.2.17Deve fornecer as seguintes informações dos computadores; 1.2.17.1Se o anti-virus está instalado; 1.2.17.2Se o anti-virus está iniciado;				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.murtcom.com

TELCOM

	1.2.17.3Se o anti-virus está atualizado; 1.2.17.4Minutos/horas desde a última conexão da máquina com o servidor administrativo; 1.2.17.5Minutos/horas desde a última atualização de vacinas 1.2.17.6Data e horário da última verificação executada na máquina; 1.2.17.7Versão do anti-virus instalado na máquina; 1.2.17.8Se é necessário reiniciar o computador para aplicar mudanças; 1.2.17.9Data e horário de quando a máquina foi ligada; 1.2.17.10Quantidade de vírus encontrados (contador) na máquina; 1.2.17.11Nome do computador; 1.2.17.12Domínio ou grupo de trabalho do computador; 1.2.17.13Data e horário da última atualização de vacinas; 1.2.17.14Sistema operacional com ServicePack; 1.2.17.15Quantidade de processadores; 1.2.17.16Quantidade de memória RAM; 1.2.17.17Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory); 1.2.17.18Endereço IP; 1.2.18Deve permitir bloquear as configurações do anti-virus instalado nas estações e servidores de maneira que o usuário não consiga alterarálas; 1.2.19Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: 1.2.19.1Mudança de gateway; 1.2.19.2Mudança de subnet DNS; 1.2.19.3Mudança de domínio; 1.2.19.4Mudança de servidor DHCP; 1.2.19.5Mudança de servidor DNS; 1.2.19.6Mudança de servidor WINS; 1.2.19.7Aparecimento de nova subnet;				

	1.2.20Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet; 1.2.21Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes; 1.2.22Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de anti-virus; 1.2.23Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos; 1.2.24Capacidade 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; 1.2.25Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML. 1.2.26Capacidade de gerar traps SNMP para monitoramento de eventos; 1.2.27Capacidade de enviar mensagens via NETSEND para máquina específicas em caso de algum evento; 1.2.28Capacidade de enviar emails para contas específicas em caso de algum evento; 1.2.29Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server; 1.2.30Deve possuir compatibilidade com Cisco Network Admission Control (NAC); 1.2.31Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta				

	(Crystal Reports, por exemplo). 1.2.32Capacidade 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; 1.2.33Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo); 1.2.34Capacidade de realizar atualização incremental de vacinas nos computadores clientes; 2Estações Windows – 2.1Compatibilidade: 2.1.1 Microsoft Windows 2000 Professional Service Pack 4 ou superior 2.1.2 Microsoft Windows XP Home Edition 2.1.3 Microsoft Windows XP Professional SP1 ou superior 2.1.4 Microsoft Windows XP Professional x64 Edition 2.1.5 Microsoft Windows Vista 2.1.6 Microsoft Windows Vista x64 2.1.7 Microsoft Windows Seven Professional/Enterprise/Ultimate 2.1.8Microsoft Windows Seven Professional/Enterprise/Ultimate x64 2.2Características: 2.2.1 Deve prover as seguintes proteções: 2.2.1.1Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; 2.2.1.2Antivirus de Web (módulo para verificação de sites e downloads contra vírus) 2.2.1.3Antivírus de Email (módulo para verificação de emails recebidos e				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

	enviados, assim como seus anexos) 2.2.1.4Anti-Spam (módulo de anti-spam pessoal) 2.2.1.5Firewall com IDS 2.2.1.6Auto-proteção (contra ataques aos serviços/processos do antivírus) 2.2.1.7Controle de dispositivos externos 2.2.2Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota; 2.2.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa). 2.2.4 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução; 2.2.5 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 2.2.6Capacidade 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; 2.2.7 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; 2.2.8 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver				

	funcionando a partir de baterias (notebooks); 2.2.9 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 2.2.10Capacidade 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; 2.2.11Capacidade de verificar somente arquivos novos e alterados; 2.2.12Capacidade de verificar objetos usando heurística; 2.2.13Capacidade de agendar uma pausa na verificação; 2.2.14Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado; 2.2.15O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: 2.2.15.1Perguntar o que fazer, ou; 2.2.15.2Bloquear acesso ao objeto; 2.2.15.2.1Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); 2.2.15.2.2Caso positivo de desinfecção: 2.2.15.2.2.1Restaurar o objeto para uso; 2.2.15.2.3Caso negativo de desinfecção: 2.2.15.2.3.1Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador); 2.2.16Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto. 2.2.17Capacidade de verificar emails recebidos e enviados nos protocolos				

	POP3, IMAP, NNTP, e SMTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL); 2.2.18Capacidade de verificar tráfego de ICQ e MSN contra vírus e links phishings; 2.2.19Capacidade de verificar links inseridos em emails contra phishings; 2.2.20Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera; 2.2.21Capacidade de verificação de corpo e anexos de emails usando heurística; 2.2.22O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve: 2.2.22.1Perguntar o que fazer, ou; 2.2.22.2Bloquear o email; 2.2.22.2.1Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); 2.2.22.2.2Caso positivo de desinfecção: 2.2.22.2.2.1Restaurar o email para o usuário; 2.2.22.2.3Caso negativo de desinfecção: 2.2.22.2.3.1Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador); 2.2.23Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena. 2.2.24Possibilidade de verificar somente emails recebidos ou recebidos e enviados. 2.2.25Capacidade de filtrar anexos de email, apagando-os ou renomeandoos de acordo com a configuração feita pelo administrador, com a possibilidade de restauração de um anexo deletado; 2.2.26Capacidade de verificação de tráfego HTTP e qualquer script do				

Distribuidor:

Rua Manoel Marques de Souza, n01, ej.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCON

	Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas; 2.2.27Deve ter suporte total ao protocolo IPv6; 2.2.28Capacidade de alterar as portas monitoradas pelos módulos de Web e Email; 2.2.29Na verificação de tráfego web, caso encontrado código malicioso o programa deve: 2.2.29.1Perguntar o que fazer, ou; 2.2.29.2Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou; 2.2.29.3Permitir acesso ao objeto; 2.2.30O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: 2.2.30.1Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou; 2.2.30.2Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação. O administrador deve ter a capacidade de escolher quanto tempo de buffer o programa irá realizar. 2.2.31Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web. 2.2.32Deve 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. 2.2.33Deve possuir módulo que analise cada macro do VBA executada, procurando por sinais de atividade maliciosa. 2.2.34Deve 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. 2.2.35Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/). 2.2.36Deve possuir módulo de bloqueio de Banners e Popups de propagandas não-solicitadas, com opção de lista de exclusão; 2.2.37Deve possuir módulo de proteção de atividades do modem, possibilitando a criação de uma lista de números que podem ser discados; 2.2.38Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica; 2.2.39Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas. 2.2.40O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: 2.2.40.1Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 2.2.40.2Filtragem por aplicação: onde o administrador poderá escolher qual aplicação terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados. 2.2.41Deve possuir módulo de anti-spam, que utilize tecnologias PDB (análise de cabeçalho), GSG (análise de elementos gráficos), tecnologia baseada				

	no teorema de Bayes (http://pt.wikipedia.org/wiki/Filtro_bayesiano) além de White e Black Lists e algorítmo de reconhecimento de frases comuns de spams. 2.2.42Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: 2.2.42.1Dispositivos de comunicação USB (modems, telefones, etc.) 2.2.42.2Impressoras USB 2.2.42.3Dispositivos de armazenamento USB 2.2.42.4Drives de CD\DVD-ROM 2.2.42.5Drives de disquete 2.2.42.6Dispositivos IEEE 1394 (Firewire) 2.2.42.7Modems 2.2.42.8Dispositivos PCMCIA 2.2.42.9Dispositivos COM e LPT 2.2.42.10Drives de fita 2.2.42.11Dispositivos 1284 Dot4 2.2.42.12Impressoras 1284 Dot4 2.2.42.13Dispositivos Infra-vermelhos (IRDA) 2.2.42.14Leitores de cartões (SD, MemoryStick, etc) 2.2.42.15Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc) 2.2.42.16Dispositivos Bluetooth 2.2.43Deve ter capacidade para desabilitar o autoplay em todos os dispositivos (drives de cd, usb, rede, etc) 2.2.44Deve ter capacidade para desabilitar o processamento de arquivos autorun.inf sem desabilitar o autoplay por completo. 3Estações de trabalho Linux – 3.1Compatibilidade: 3.1.1 Plataforma 32-bits: 3.1.1.1Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92) 3.1.1.2Fedora 9 (kernel 2.6.25) 3.1.1.3SUSE Linux Enterprise Desktop 10				

	SP2 (kernel 2.6.16.60-0.21) 3.1.1.4openSUSE Linux 11.0 (kernel 2.6.25) 3.1.1.5Debian GNU/Linux 4.0 r4 (kernel 2.6.24) 3.1.1.6Mandriva Corporate Desktop 4 (kernel 2.6.12) 3.1.1.7Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25) 3.1.1.8Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008) 3.1.2 Plataforma 64-bits: 3.1.2.1Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92) 3.1.2.2Fedora 9 (kernel 2.6.25) 3.1.2.3SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21) 3.1.2.4openSUSE Linux 11.0 (kernel 2.6.25) 3.2Características: 3.2.1 Deve prover as seguintes proteções: 3.2.1.1Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; 3.2.1.2As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora. 3.2.2Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 3.2.2.1Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 3.2.2.2Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possivel a restauração de objetos que contenham informações importantes;				

Distribuidor:

Rua Manoel Marques de Souza, n01, c].
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCOM

	3.2.2.3Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; 3.2.2.4Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. 3.2.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; 3.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 3.2.5 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; 3.2.6 Capacidade de verificar objetos usando heurística; 3.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena 3.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados 3.2.9Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux). 4Servidores Windows – 4.1Compatibilidade: 4.1.1 Microsoft Windows 2000 Server Service Pack 4 + Update Rollup 1 ou superior 4.1.2 Microsoft Windows 2000				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCON

	Advanced Server Service Pack 4 + Update Rollup 1 ou superior 4.1.3 Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition Service Pack 1 ou superior 4.1.4 Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition x64 4.1.5 Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition 4.1.6 Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition x64 4.1.7 Microsoft Windows Storage Server 2003 R2 4.1.8 Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition 4.1.9 Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition x64 4.1.10Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition 4.1.11Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition x64 4.1.12Microsoft Terminal baseado em Windows 2000 Server 4.1.13Microsoft Windows Small Business Server 2003 4.1.14Microsoft Windows Small Business Server 2008 4.1.15Windows Essential Business Server 2008 4.1.16Microsoft Terminal baseado em Windows 2003 Server 4.1.17Microsoft Terminal baseado em Windows 2008 Server 4.1.18Citrix Metaframe XPe FR3; 4.1.19Citrix Presentation Server 3.0 4.1.20Citrix Presentation Server 4.0 4.1.21Citrix Presentation Server 4.5 4.2Características:				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCOM

	4.2.1 Deve prover as seguintes proteções: 4.2.1.1Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; 4.2.1.2Auto-proteção contra ataques aos serviços/processos do antivírus 4.2.2Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota; 4.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora. 4.2.4Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 4.2.4.1Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 4.2.4.2Gerenciamento de tarefa (criar ou excluir tarefas de verificação) 4.2.4.3Leitura de configurações 4.2.4.4Modificação de configurações 4.2.4.5Gerenciamento de Backup e Quarentena 4.2.4.6Visualização de relatórios 4.2.4.7Gerenciamento de relatórios 4.2.4.8Gerenciamento de chaves de licença 4.2.4.9Gerenciamento de permissões (adicionar/excluir permissões acima) 4.2.5Capacidade 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. 4.2.6Capacidade de resumir automaticamente tarefas de verificação				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

TELCON

	que tenham sido paradas por anormalidades (queda de energia, erros, etc) 4.2.7Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte Ininterrupta de energia (uninterruptible Power supply – UPS) 4.2.8Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares; 4.2.9Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor. 4.2.10Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor. 4.2.11Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas. 4.2.12Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 4.2.13Capacidade 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; 4.2.14Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 4.2.15Capacidade 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; 4.2.16Capacidade de verificar somente arquivos novos e alterados; 4.2.17Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc) 4.2.18Capacidade de verificar objetos usando heurística; 4.2.19Capacidade de configurar diferentes ações para diferentes tipos de ameaças; 4.2.20Capacidade de agendar uma pausa na verificação; 4.2.21Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado; 4.2.22O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: 4.2.22.1Perguntar o que fazer, ou; 4.2.22.2Bloquear acesso ao objeto; 4.2.22.2.1Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); 4.2.22.2.2Caso positivo de desinfecção: 4.2.22.2.2.1Restaurar o objeto para uso; 4.2.22.2.3Caso negativo de desinfecção: 4.2.22.2.3.1Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador); 4.2.23Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto. 4.2.24Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena				

	4.2.25Possibilidade de escolha da pasta onde arquivos restaurados do backup e arquivos serão gravados 4.2.26Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa. 5Servidores Linux – 5.1Compatibilidade: 5.1.1 Plataforma 32-bits: 5.1.1.1Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92) 5.1.1.2Fedora 9 (kernel 2.6.25) 5.1.1.3SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21) 5.1.1.4Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12) 5.1.1.5openSUSE Linux 11.0 (kernel 2.6.25) 5.1.1.6Debian GNU/Linux 4.0 r4 (kernel 2.6.24) 5.1.1.7Mandriva Corporate Server 4 (kernel 2.6.12) 5.1.1.8Ubuntu 8.04.1 Server Edition (kernel 2.6.25) 5.1.2Plataforma 64-bits: 5.1.2.1Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92) 5.1.2.2Fedora 9 (kernel 2.6.25) 5.1.2.3SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21) 5.1.2.4openSUSE Linux 11.0 (kernel 2.6.25) 5.1.2.5 5.2Características: 5.2.1 Deve prover as seguintes proteções: 5.2.1.1Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; 5.2.1.2As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.				

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 -- Manaus/AM
Phone: 55 92 3236 0196
http://www.multicom.com

	5.2.2Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: 5.2.2.1Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 5.2.2.2Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes; 5.2.2.3Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; 5.2.2.4Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados. 5.2.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; 5.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 5.2.5 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; 5.2.6 Capacidade de verificar objetos usando heurística; 5.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e				

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multicom.com

TELCON

	arquivos em quarentena 5.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados 5.2.9Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux) 6Servidores Novell Netware: 6.1Compatibilidade: 6.1.1 Novell Netware 5.x Support Pack 6 ou superior 6.1.2 Novell Netware 6.0 Support Pack 3 ou superior 6.1.3 Novell Netware 6.5 6.2 Características: 6.2.1 Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados; 6.2.2 Deve possuir verificação manual e agendada de acordo com a configuração do administrador; 6.2.3 Capacidade de realizar update de maneira automatica, via internet ou LAN; 6.2.4 Capacidade de fazer um rollback das vacinas; 6.2.5 Capacidade de mover arquivos suspeitos ou infectados para área de quarentena; 6.2.6 Capacidade de criar logs detalhados e salvar resultados das verificações agendadas; 6.2.7 Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados; 6.2.8 Capacidade de notificar o administrador de varreduras concluidas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou email; **Marca: Kaspersky** **Modelo: Business Space Security**				

	Garantia: 3 anos on-site				
Valor Total da Proposta R$ 61.000,00 (Sessenta e Um Mil)					

Validade de Proposta: 20 (Vinte) dias.

Prazo de Entrega: 30(trinta) dias

Prazo de Pagamento: Nota de empenho com deposito em conta.

Informações Bancárias:
Banco do Brasil
Nº. do Banco: 001
Agência: 3378-2
C/C: 5850-5

Atenciosamente,

Milena Cabral
Analista de Licitação
Tel.: 3236-0196
Licitacoes@multcom.com

Distribuidor:

Rua Manoel Marques de Souza, n01, cj.
Castelo Branco
Parque Dez, CEP 69055-240 – Manaus/AM
Phone: 55 92 3236 0196
http://www.multcom.com

SK Tecnologia Ltda.
CNPJ: 03.820.167/0001-97 IE:116.160.704.119
Rua Humberto I, 236 – 2º Andar
04018-030 - Vila Mariana - São Paulo-SP
Tel • Fax: (11) 5083-6445
Email: sk@sktec.com.br site: www.sktec.com.br

São Paulo, 06 de Fevereiro de 2012.

Ao
Instituto Federal de Educação, Ciência e Tecnologia Baiano.

Prezado,

É com grande satisfação que encaminhamos à sua empresa proposta comercial para fornecimento de Antivírus.

Descrição dos produtos:

Item	Descrição	Qtde	Unit.	Total
01	LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR 36 (TRINTA E SEIS) MESES:	1300	62,00	80.600,00

Total da proposta R$ 80.600,00

Condições de Pagamento: até 30 (trinta) dias após entrega.

Prazo de entrega: 45 dias.

Frete incluso: Sim. **Impostos inclusos:** Sim.

Validade da proposta: Esta proposta terá a validade de 60 dias após a sua emissão.

Garantia: Todos os Itens possuem garantia de 03 anos on site.

Atenciosamente

Monique Amaral
monique@sktec.com.br

03 820 167/0001-97
SK TECNOLOGIA LTDA.
Rua Humberto I, 236 - Cj. 22
CEP 04018-030 - V. Mariana
SÃO PAULO-SP

LUSTRABITS
TECNOLOGIA DA INFORMAÇÃO

À

Secretaria de Educação Profissional e Tecnológica

Instituto Federal de Educação, Ciência e Tecnologia Baiano.

Nesta,

Conforme, solicitação encaminho proposta.

Item	DESCRIÇÃO DO MATERIAL / SERVIÇO	Quant.	UND	Valor Unit. R$	Valor Total R$
01	LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY	Und	1300	R$ 70,00	R$ 91.000,00

Valor Total da Proposta R$ 91.000,00

CONDIÇÕES DE COMERCIALIZAÇÃO

Valor Total da Proposta: R$ 91.000,00
Validade da Proposta: 30 dias após a edição dessa proposta.
Condições de Pagamento: Conforme Nota de Empenho
Moeda: REAL

Tributos inclusos nos preços acima

CONDIÇÕES GERAIS

O faturamento dos itens constantes nesta proposta será efetuado

Atenciosamente,

Gualber Kolbert
Consultor Comercial
Lustrabits TI Ltda.
3236-6901 / 8414-5898

04.009.632/0001-77
LUSTRABITS TECNOLOGIA DA INFORMAÇÃO LTDA
Rua: Dr. Thomas nº 149
Bairro: Nossa Srª. das Graças
CEP 69.035-053
MANAUS - AM

São Paulo, 26 de Fevereiro de 2012.

Cliente:
Ao
Instituto Federal de Educação, Ciência e Tecnologia Baiano.

PROPOSTA DE PREÇO:

ITEM	Descrição	Qtd	Valor Unitário	Valor Total
01	LICENÇA DE USO SOFTWARE ANTIVÍRUS KASPERSKY BUSINESS SPACE SECURITY POR	1300	R$ 59,90	R$ 77.870,00
Valor Total da Proposta. R$ 77.870,00 (Setenta e Sete Mil Oitocentos e Setenta Reais)				

Condições:

Prazo de entrega: a previsão informada deverá ser confirmada quando da colocação do pedido.
Validade da proposta: 10 dias a contar da data de emissão.
Forma de pagamento: nota de empenho com deposito bancário
Preço dos produtos: encontram-se inclusos os Impostos
Frete: Incluso considerando somente uma entrega. Caso o cliente opte por entregas parciais os fretes excedentes serão por conta do cliente. Qualsquer danos ocorridos após o recebimento dos equipamentos serão de responsabilidade do cliente.
Garantia dos equipamentos: serão considerados os mesmos prazos oferecidos pelo fabricante, sendo doze meses, no caso de defeito de fabricação.

Denilson Marques
Diretor de vendas
CNPJ:08.984.746/0001-99

AV JOSE FELIPE DA SILVA N:349 SALA 3 - BAIRRO BUTANTA – CEP-05372-040 - SAO PAULO - SP
FONE FAX : (55) 11-3784-2524

SERVICO PUBLICO FEDERAL
SIAFI - SISTEMA INTEGRADO DE ADMINISTRACAO FINANCEIRA DO GOVERNO FEDERAL

N O T A D E E M P E N H O

EMISSAO : 22Ago12 NUMERO: 2012NE800438 ESPECIE: EMPENHO DE DESPESA
EMITENTE : 158129/26404 - INST.FED.DE EDUC.,CIENC.E TEC.BAIANO -REITORI
CNPJ : 10724903/0001-79 FONE: 71 3186-0001
ENDERECO : RUA DO ROUXINOL, 115 - IMBUI SALVADOR - BA
MUNICIPIO : 3849 - SALVADOR UF: BA CEP: 41720-052

CREDOR : 05047556/0001-57 - RPJ COMERCIO E SERVICOS DA AMAZONIA LTDA
ENDERECO : MANOEL MARQUES DE SOUZA 01 CONJ CASTELO BRA PARQUE 10 DE NOVEMB
MUNICIPIO : 0255 - MANAUS UF: AM CEP: 69055-240
TAXA CAMBIO:
OBSERVACAO / FINALIDADE
ATENDER DESPESAS COM AQUISIÇ├O DE LICENÇAS DE USO DE SOFTWARE ANTIVIRUS PARA A TENDER AS NECESSIDADES DA REITORIA. LOCAL DE ENTREGA: SALVADOR-BA. FORNECEDOR: 92 32360196 / 32367284 / LICITACOES@MULTCOM.COM PROC ORIGEM: 05001012011

CLASS : 1 26404 12363203120RL0029 044639 0112000000 449039 151406 A20RLP01FIP
TIPO : ORDINARIO MODALIDADE DE LICITACAO: PREGAO
AMPARO: INCISO: PROCESSO: 23129001779201109
UF/MUNICIPIO BENEFICIADO: BA /
ORIGEM DO MATERIAL :
REFERENCIA DA DISPENSA: NUM. ORIG.:

VALOR EMPENHO : 16.450,00
DEZESSEIS MIL, QUATROCENTOS E CINQUENTA REAIS**********
****
****
****

ESPECIFICACAO DO MATERIAL OU SERVICO

ND: 449039 SUBITEM: 93 -AQUISICAO DE SOFTWARE
SEQ.: 1 QUANTIDADE: 350 VALOR UNITARIO: 47,00
VALOR DO SEQ. : 16.450,00

350,00000 unid.
SOFTWARE APLICATIVO
LICENÇA DE USO SOFTWARE ANTIV┌RUS KASPERSKY BUSINESS SPACE SECURITY POR 36 (TRINTA E SEIS) MESES, para utilizaç├o em estaçΣes e servidores, com serviço de suporte técnico, manutenç├o e atualizaç├o de licenças.
MARCA: KASPERSKY ITEM DO PROCESSO: 00001 ITEM DE MATERIAL: 000150191

T O T A L : 16.450,00

SEBASTIAO EDSON MOURA
ORDENADOR

ELOIVALDO FAGUNDES PEREIR
GESTOR FINANCEIRO

NILTON DE SANTANA SANTOS
ORDENADOR SUBSTITUTO

GERFSON SILVA ROVHA
GESTOR FINANCEIRO SUBSTITUTO