ANEXO 2
TERMO DE REFERÊNCIA

JUSTIFICATIVA
O presente Termo de Referência é a contratação de empresa especializada na prestação de serviços de licença de antivírus para estação de trabalho e servidores para proteção da rede de computadores da Fundação **CEPERJ** para um período de 12 (doze) meses conforme especificações abaixo.

OBJETO DA CONTRATAÇÃO DE SERVIÇOS

O presente objeto é a contratação de empresa especializada na prestação de serviços de licença antivírus para estação de trabalho e servidores, para um período de 12 (doze) meses.

ESPECIFICAÇÕES TÉCNICAS

Software: Ferramenta antivírus, antisspyware e antimalware com gerenciamento centralizado, instalação e suporte (7x24) atendimento ilimitados presenciais e remotos.

Quantidade: Licenças de uso para 200 (duzentos) equipamentos de estações de trabalho e servidores para um período de 12 (doze) meses, com garantia de suporte para nossas versões Windows e Linux.

Sistema Operacional/Serviços a serem cobertos pela solução:
MS Windows 2003;
MS Windows 2012R2 / 2008 Server;
MS Windows Vista;
MS Windows 7;
MS Windows 8 e 8.1.

Requisitos mínimo de Equipamentos:
O sistema deverá ser capaz de atuar sobre equipamentos com 512MB de RAM na estação do usuário no mínimo.

Idioma Características da Ferramenta:
Características gerais da solução
Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho e deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes.
O fabricante deverá ter solução de antivírus para Servidores, Estações de trabalho.
O conjunto de softwares que compõe a solução de antivírus para servidores e estações de trabalho deverão ser totalmente gerenciáveis através da mesma console de gerenciamento centralizado e de forma que todos os produtos sejam monitorados através desta.
Fornecer todo o material necessário para a instalação dos produtos solicitados.
Manuais necessários à instalação, manutenção e utilização da solução, nos seguintes meios: CD e/ou Website em Inglês ou Português do Brasil.
Apresentação de projeto detalhado do desenho da solução ofertada, abrangendo todo o conjunto de softwares, aplicação e gerenciamento unificado.
A solução deverá possuir ferramentas de varredura, detecção, análise e remoção de malwares, riskwares, spywares e demais formas de vírus e códigos maliciosos conhecidos, bem como Firewall, IDS/IPS, Controle de Aplicativos e Quarentena de Rede. Estas devem ser totalmente integradas, instaladas através de um único pacote sem a necessidade de instalação de módulos adicionais.

Solução de monitoramento remoto com utilização de interface gráfica (GUI), para administração, monitoração e gerenciamento da solução ofertada e que seja disponibilizada sua instalação em plataforma Windows e Linux, podendo o administrador escolher a plataforma desejada de acordo com sua necessidade.
Repositório remoto de distribuição de atualizações da lista de vírus e do mecanismo de varredura (ScanEngine) sem limite de instalações, podendo o administrador instalar quantos necessitar sem ônus com suporte para as plataformas Windows e Linux.
Prevenção de epidemia manual ou automática.
A propriedade de todos os componentes da solução passa a ser do (CLIENTE).
O fabricante do antivírus deve possuir site indicando ameaças de malware presentes mundo em tempo real, através de indicação gráfica e mapa mundial.
O fabricante deve possuir site próprio para coleta de amostras de arquivos infectados.
O fabricante deve possuir site próprio para coleta de falsos positivos.
O fabricante deverá participar do programa "Microsoft Active ProtectionProgram" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante.
Especificações Técnicas para o Software de Gerenciamento Centralizado para toda a Solução de Segurança.
Possuir gerenciamento e configuração remota para a funcionalidade de controle de dispositivos.
Possuir gerenciamento e configuração remota para a funcionalidade de antivírus, anti-spyware, detecção de rootkit e proteção de browser.
Possuir gerenciamento e configuração remota para a funcionalidade de controle de aplicativos e firewall
Possuir gerenciamento e configuração remota para a funcionalidade de IDS/IPS
Possuir gerenciamento e configuração remota para a funcionalidade de Zero Hour e/ou Zero Day.
Possuir gerenciamento e configuração remota para a funcionalidade de Quarentena de rede.
Gerenciar os produtos antivírus como uma árvore de diretórios parametrizável pelo administrador.
Agendamento de verificação de comunicação entre o gerenciador e os produtos gerenciados.
Suportar o gerenciamento acima de 5.000 máquinas a partir de um único servidor.
Permitir a criação de usuários para acesso à console de gerenciamento, com opção de usuário administrador e usuário para leitura (readonly).
Permitir a criação de usuários com permissão de somente leitura para visualizar subpastas e/ou subdomínios, não acessando outras estruturas de diferente nível hierárquico.
Permitir a criação de usuários com permissão administrativa para configurar subpastas e/ou subdomínios, não afetando outras estruturas de diferente nível hierárquico.
Permitir logins simultâneos de usuários administradores ao sistema de gerenciamento da solução.
Manter um registro de ações realizadas pelos administradores no sistema de gerenciamento da solução de segurança.
Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.
Comunicação segura entre os servidores de gerenciamento e clientes gerenciados através de assinatura digital, com chave pública e privada.
Detecção de domínios e grupos de trabalho a partir da estrutura de diretórios pré-existentes.
Importar a estrutura organizacional (OUs) do MS Active Directory para o serviço de gerenciamento da solução de segurança.
Suporte a NAP (Network Access Protection)
Atualização de listas, vacinas, mecanismos de rastreamento e desinfecção através da Internet via protocolo HTTP e distribuindo estas para todas as demais ferramentas que compõem a solução de antivírus automaticamente sem a intervenção do administrador.
As atualizações devem ser incrementais, inclusive o download, este deve ser gerenciado de forma que baixe somente a parte que lhe falta e do ponto onde foi interrompido.

Deve suportar conexões DialUp para download de atualizações e detectar quando esta estiver disponível e proceder com o download.
Deve ter capacidade de ser o repositório central de atualizações, independentemente da plataforma, Microsoft e Linux, repositório de políticas e relatórios sem a necessidade de instalação de software adicional além dos pacotes desenvolvidos pelo fabricante da solução de segurança.
Permitir a instalação do Antivírus nos clientes a partir de um único servidor de gerenciamento da solução remotamente.
Permitir a alteração das configurações dos Antivírus nos clientes de maneira remota para todos os produtos.
Deve ser capaz de bloquear as configurações nas estações de trabalho sem a necessidade de senha, evitando que os usuários alterem as configurações do produto.
Opção de atualização automática de políticas de prevenção a partir da console de gerenciamento.
Políticas em caso de epidemia de vírus criando regras de bloqueio contra os ataques até que a vacina seja criada para estações/servidores com plataforma Microsoft e Linux.
Geração de relatórios que contenham informações sobre as infecções e atualizações da solução.
Exportar relatórios para os seguintes formatos: HTML, XML e CSV.
Enviar alertas em caso de epidemias através de e-mail e Popups.
Permitir a visualização de relatórios contendo as seguintes informações:
Última conexão com o servidor, última política aplicada.
Sumário dos produtos antivírus instalados (com indicação das versões dos módulos instalados).
Top 10 com os de quantidade de infecção.
Histórico de infecções.
Histórico das definições de vacinas.
O módulo IPS deve apresentar o último ataque sofrido, bem como dados sobre a origem do mesmo.
Indicação de hotfixes instalados.
Dados do host (Sistema Operacional e versão do mesmo, WINS Name, DNS Name, IP).
O armazenamento dos logs, alertas, status e qualquer informação pertinente a solução de segurança deve ser armazenada em um banco de dados fornecido e integrado a solução.
Possuir a capacidade de armazenar os eventos em banco de dados centralizado. Se a solução necessitar de um banco de dados proprietário este deverá ser fornecido, devidamente licenciado para a licitante. Não serão aceitas versões gratuitas de bancos de dados de terceiros.
Suporte para instalação em plataformas Linux e Microsoft atendendo no mínimo os sistemas operacionais abaixo relacionados:
Microsoft:
Windows Server 2003 SP1 ou superior 32-bit, Edições: Standard, Enterprise, Web Edition, Small Business Server.
Windows Server 2003 SP1 ou superior 64-bit, Edições: Standard, Enterprise.
Windows Server 2008 SP1 32-bit, Edições: Standard, Enterprise, Web Server.
Windows Server 2008 SP1 ou superior 64-bit, Edições: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server.
Windows Server 2008 R2 com ou sem SP1, Edições: Standard, Enterprise, Web Server.
Windows Server 2012, Edições: Essentials, Standard, Datacenter.
Windows Server 2012 R2, Edições: Essentials, Standard, Datacenter.
Linux:
Red Hat Enterprise Linux 6 32/64-bit.
Red Hat Enterprise Linux 5 32/64-bit.

CentOS 6 32/64-bit.
SUSE Linux Enterprise Server 11 32/64-bit.
SUSE Linux Enterprise Server 10 32/64-bit.
SUSE Linux Enterprise Desktop 11 32/64-bit.
openSUSE Linux 12 32/64-bit.
Debian GNU Linux Squeeze 6.0 32/64-bit.
Debian GNU Linux 7.2 Wheezy 32/64-bit.
Ubuntu 10.04 Lucid Lynx 32/64-bit.
Ubuntu 12.04 Precise Pangolin 32/64-bit.
O serviço de gerenciamento da solução de segurança deve suportar ser instalado tanto em plataforma Linux como em plataforma Microsoft. Permitindo ao administrador escolher a plataforma em que o serviço de gerenciamento será instalado. A console de gerenciamento também deve suportar ser instalada em plataforma Linux e Microsoft, permitindo ao administrador escolher a plataforma e inclusive utilizar um ambiente misto de administração, como o servidor de gerenciamento em um computador Linux e a console em um computador Microsoft e vice-versa.
Possuir um dashboard com informações do estado geral da solução de segurança e hosts gerenciados.
Possuir download direto (a partir da console de gerenciamento) de novas versões do antivírus ou link para página do fabricante para download de novas versões do antivírus durante a vigência da garantia do mesmo, dessa forma mitigando a possibilidade de entrar em falsa página para download de falsas atualizações do antivírus.
A solicitação de verificação de atualização de vacinas e políticas de segurança deve ser oriunda da estação de trabalho para servidor de gerenciamento e não o contrário.
Utilizar protocolo seguro (HTTPS) para consulta/visualização de relatórios.
Capacidade de gerenciar e aplicar as atualizações de softwares da Microsoft e outros fabricantes, considerando no mínimo nos seguintes softwares:
• Microsoft Access;
• Acrobat Reader;
• Adobe Flash;
• Apache Tomcat;
• Apple iTunes;
• Apple QuickTime;
• BlackBerry Desktop;
• CCleaner;
• Citrix MetaFrame;
• Citrix Presentation;
• Citrix XenApp;
• DirectX;
• Microsoft Excel;
• Microsoft Exchange Server;
• Foxit Reader;
• Mozilla Firefox;
• Google Chrome;
• Microsoft Infopath;
• Microsoft Internet Information Services;
• Microsoft ISA Server;
• LibreOffice;
• Microsoft Forefront;
• Microsoft FrontPage;

- Microsoft Lync;
- Microsoft Office;
- Microsoft Project;
- Microsoft SharePoint;
- Microsoft Virtual Server;
- Microsoft Visio;
- Microsoft Visual Basic;
- Microsoft Visual FoxPro;
- Microsoft Visual C++
- Microsoft Visual Studio;
- Microsoft Windows Defender;
- Notepad++
- Microsoft OneNote;
- Opera;
- Oracle OpenOffice;
- Microsoft Outlook;
- Microsoft PowerPoint;
- Microsoft Project;
- Microsoft Publisher;
- RealPlayer;
- RealVNC;
- Safari;
- Salesforce Chatter Desktop;
- SeaMonkey;
- ShavlikNetChk Project;
- Skype;
- Microsoft SQL Server;
- Sun Java Runtime Environment;
- Thunderbird;
- TortoiseSVN;
- UltraVNC;
- VLC Media Player;
- VMWare;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows Media Player;
- Microsoft Windows Server 2003;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2012;
- Microsoft Windows Small Business Server 2003;
- Microsoft Windows Small Business Server 2008;
- Microsoft Windows Small Business Server 2011;
- WinRAR;

• WinZIP;
• Microsoft Word;
• Zimbra Desktop;

Capacidade de aplicar as atualizações de software, sem a necessidade de intervenção do usuário final.
Capacidade de configurar grupos distintos para update de software, dessa forma, podendo marcar quais grupos sofrerão atualização de software e quais não sofrerão atualização de software.
Gerar alertas sobre atualizações críticas.
Possibilidade de criar lista de programas para exclusão da verificação da necessidade de atualização de software.
Especificações Técnicas da solução de Segurança para Estações de Trabalho.
Suporte, no mínimo, aos seguintes sistemas operacionais: SP3, Windows Vista 32 e 64 Bits, Windows 7 32 e 64 Bits, Windows 8 32 e 64 Bits, Suse Linux, Debian GNU Linux, Ubuntu, RedHat e CentOS.
Toda a solução deverá funcionar com agente único na estação de trabalho a fim de diminuir o impacto ao usuário final.
A interface dos clientes anti-vírus e anti-spyware para estações de trabalho deve ter a opção de ser instalada em português do Brasil sem exceção.
Instalação da solução de antivírus e anti-spyware remotamente via push, via política de gerenciamento, via MSI através do MS GPO e por scripts.
Permitir instalação "silenciosa".
Permitir atualizações através de login script, Internet/Intranet, CD-ROM e arquivo off line.
Permitir instalação remota sem forçar a reinicialização da máquina.
Agrupar estações de trabalho por domínio ou grupo, ou permitir definir qual domínio ou grupo a estação irá pertencer.
Configuração diferenciada para cada estação, grupo de estações, domínio ou grupos de domínios.
Monitoramento e gerenciamento unificados através de uma console centralizada de todos os clientes da rede a partir de um servidor central, possibilitando a criação de configurações específicas para cada cliente ou grupo de clientes, atendendo os requisitos de sistemas operacionais constantes deste TR.
Funcionar tanto no ambiente corporativo (rede interna) como em VPN.
Atualizar listas de vírus, vacinas e mecanismos de rastreamento automaticamente através de um site local pré-definido ou pela Internet para todos os clientes com plataforma Microsoft e Linux.
Definir intervalos de tempo para os computadores solicitarem as atualizações podendo este tempo ser definido em minutos, horas e dias.
Atualização automática que suporte serviço de Proxy autenticado.
Atualização em clientes móveis (LapTops de colaboradores externos e usuários remotos) a partir do site do fabricante do antivírus, ou de outra fonte definida pelo administrador, podendo o administrador definir as fontes de atualização por prioridade. Ex.: Primeiro o servidor de atualizações da rede interna depois o site do fabricante na internet.
Capacidade de rastreamento em tempo real, manual ou agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado.
Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas.
Rastreamento manual com interface gráfica em português do Brasil.
Detecção de cookies potencialmente indesejáveis no sistema.
Detecção heurística durante a varredura em tempo real, manual e agendada.
Possuir módulo ZERO DAY, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo ZERO DAY deve ser efetuada através de hash.

Permitir a atualização de um determinado segmento de rede através de uma ou mais estações de trabalho eleitas para serem os repositórios deste seguimento de rede, sem a necessidade de instalação de um módulo adicional nas estações ou servidores para realizar esta tarefa. Esta função deve fazer parte do pacote de instalação padrão do módulo antivírus para estações de trabalho, sem a necessidade de instalação de módulo adicional.
Rastrear arquivos compactados no mínimo nos seguintes formatos: ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR e TGZ.
Criação de uma lista de exclusão de pastas ou arquivos que não devem ser rastreados.
Possuir módulo Firewall integrado à ferramenta e gerenciado pela mesma console dos módulos antivírus e anti-spyware.
Bloquear em estações com plataforma Microsoft e Linux, portas TCP e UDP comuns e específicas.
Permitir a criação de serviços que utilizam portas específicas e protocolos TCP e UDP.
Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com versões desatualizadas das assinaturas de vírus, neste caso, a estação cliente é colocada em quarentena, limitando o acesso à rede desta estação.
Possuir módulo IDS/IPS integrado na ferramenta e gerenciado pela mesma console dos módulos antivírus, anti-spyware e firewall.
Possuir módulo para controle de discagens (dialercontrol) permitindo criar uma lista de telefones permitidos e não permitidos para discagem.
Disponibilizar os seguintes relatórios: sumário de eventos de IPS por assinatura, por alvo, por endereço IP origem, os 10 principais clientes atacados, as 10 principais assinaturas, sumário das aplicações bloqueadas.
Possuir módulo de controle de aplicativos, bloqueando aplicativos mesmo se estes tiverem seus nomes alterados pelo usuário e seu gerenciamento através da mesma console de gerenciamento dos módulos antivírus, anti-spyware, firewall e IDS/IPS.
Deve possuir módulo para varredura do tráfego HTTP durante a navegação via browser analisando o tráfego em busca de códigos maliciosos.
A solução deve possuir a capacidade de bloqueio de URL´s, incluindo bloqueio de URL´s que utilizem o protocolo HTTPS para navegação.
A solução deve conter um filtro de reputação WEB, alertando o usuário e bloqueando a página web quando esta for suspeita.
O filtro de reputação deve identificar durante a pesquisa em sites de busca, no mínimo Google e Yahoo, sites suspeitos, assinalando cada um deles com um carimbo de confiável ou não confiável.
Gerar notificações para o usuário em caso de detecção de vírus.
Gerar notificações para o administrador de rede quando ocorrer uma epidemia de vírus (outbreakalert) através de e-mail e NT Event Log.
Bloqueio de acesso às funções de configuração do software nas estações remotas.
Desinstalar remotamente a solução de antivírus na estação.
Atualização automática e incremental das listas de vírus.
Atualização e mudanças de configuração em tempo real através do protocolo http com verificação da assinatura digital do pacote de atualização.
Procurar códigos maliciosos em arquivos potencialmente infectáveis, pelo tipo real de arquivo.
Proteção e remoção contra spywares em tempo real em plataformas VISTA / WIN7 / WIN8.
Proteção contra vírus para clientes pop3 durante o acesso ao Servidor de Correio.
Armazenamento de log de ocorrência de vírus local e no servidor.
Através do uso de política, impedir a desinstalação não autorizada ou remoção do módulo residente em memória do cliente de antivírus.
Possuir módulo para bloqueio de dispositivos.

Permitir bloquear dispositivos no mínimo pelo Hardware ID, ID do dispositivo, ID compatível e Classe GUID.
Permitir bloquear dispositivos como, no mínimo, Modems 3G, Dispositivos de armazenamento em massa, câmeras de vídeo embutidas e móveis, mouse com e sem fio, teclados, cd-rom, leitores de cartão, leitores de discos flexíveis (disquetes), discos rígidos (HDs)
O bloqueio de dispositivos deve permitir bloquear um único dispositivo e liberar todos os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: Bloquear qualquer Pendrive exceto um em um único computador.
As regras de bloqueio de dispositivos devem permitir ser aplicadas por grupo, host e todo o domínio.
Integração com Microsoft NAP.
Possuir a funcionalidade de mudança de perfil automático do firewall, de acordo com o ambiente de rede em que o usuário se encontra (ex: Perfil de escritório, perfil de local público, perfil em ambiente residencial, etc.).
Possuir a possibilidade de emitir relatórios com ID de dispositivos anexos ao computador, para eventual bloqueio, sem necessidade de uso de outro software ou necessidade do administrador efetuar consulta ao Windows.
Possibilidade de emitir relatório de dispositivos presentes no computador, no mínimo com as seguintes informações:
1 ID do Dispositivo;
2 Nome do Dispositivo;
3 ID do Hardware;
4 ID Compatível;
5 Classe do Dispositivo;
6 Estado do dispositivo;
Especificação técnica da solução de Segurança para Servidores de rede.
Suporte para as plataformas:
Microsoft:
Microsoft Windows Server 2003 32 e 64 bits com ultimo Service Pack.
Microsoft Windows Server 2003 R2.
Microsoft Windows 2008 Server 32 e 64 bits.
Microsoft Windows 2008 Server R2.
Microsoft Small Business Server 2003.
Microsoft Small Business Server 2003 R2.
Microsoft Small Business Server 2008.
Microsoft Small Business Server 2011 Standard Edition.
Microsoft Small Business Server 2011 Essentials.
Microsoft Windows Server 2012.
Microsoft Windows Server 2012 Essentials.
Linux:
CentOS 5.5 32 e 64 bits.
CentOS 6.4, 6.5 32 e 64 bits.
Debian 6.0 32 e 64 bits.
Debian 7.0 32 e 64 bits.
Red Hat Enterprise Linux 5.5, 5.9, 5.10 32 e 64 bits.
Red Hat Enterprise Linux 6.4, 6.5 32 e 64 bits.
SUSE Linux Enterprise Server 11 32 e 64 bits (SP1 e SP3).
Ubuntu 10.04 (LucidLynx) 32 e 64 bits.
Ubuntu 12.04 e 12.04.2 (Precise Pangolin) 32 e 64 bits.
Ser gerenciado pela mesma ferramenta de gerenciamento da solução de segurança para estações de trabalho.

A interface dos clientes da solução de segurança para servidores de ser acessível, também, via Browser, através do protocolo HTTPS, de qualquer ponto da rede, acessível somente por usuários com direito de administração.
Instalação da solução de segurança deve permitir se executada remotamente via push, via política de gerenciamento, via MSI através do MS GPO, no caso de plataforma Microsoft e por scripts e manualmente quando plataforma Linux.
Permitir instalação "silenciosa".
Permitir atualizações através de login script, Internet/Intranet, CD-ROM e arquivo off line.
Permitir instalação remota sem forçar a reinicialização da máquina.
Bloqueio de acesso às configurações locais do software.
Agrupar servidores por domínio ou grupo, ou permitir definir qual domínio ou grupo o servidor irá pertencer.
Configuração diferenciada para cada servidor, grupo de servidores, domínio ou grupos de domínios.
Monitoramento e gerenciamento unificados através de uma console centralizada de todos os clientes da rede a partir de um servidor central, possibilitando a criação de configurações específicas para cada cliente ou grupo de clientes, atendendo os requisitos de sistemas operacionais constantes neste TR
Atualizar a lista de vírus, mecanismo de rastreamento, desinfecção automaticamente, a partir de um local específico na rede e site do fabricante na Internet.
Atualização automática através de serviço de Proxy com e sem necessidade autenticação.
Realizar rastreamento em tempo real e de forma manual e agendada em todos os servidores da rede.
Rastreamento em tempo real a ser realizado durante entrada e saída (gravação e leitura) de arquivos no servidor.
Capacidade de rastreamento em tempo real, manual e agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado.
Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo e estações específicas.
Rastreamento manual com interface gráfica para clientes Microsoft e Linux.
Possuir módulo ZERO DAY, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo ZERO DAY deve ser efetuada através de hash.
Possuir a capacidade de detecção e remoção de vírus de macro em tempo real
Ferramenta de detecção e remoção de vírus, torjans, spyware e rootkits
Rastrear arquivos compactados no mínimo nos seguintes formatos: ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR e TGZ.
Capacidade de procurar códigos maliciosos em arquivos potencialmente infectáveis, pelo tipo real de arquivo.
Exclusão de pastas e arquivos que não devem ser rastreados.
Exclusão de extensões de arquivos que não devem ser rastreados.
Gerar notificações ao administrador de rede e eventos de vírus (notificação e alertas de epidemias) através de e-mail e NT Event Log.
Gerar relatório de incidente (logs) centralizado.
Detectar e bloquear conteúdo malicioso (sobre o protocolo HTTP) para fornecer proteção adicional contra malware durante a navegação.
Prevenir, proteger e alertar contra exploits do navegador web e sites desonestos para usuários locais e remotos (para Windows ou Linux).
A proposta deverá ser de uma única marca, não sendo aceito soluções hibridas e de vários fabricantes.

Treinamento/Implantação/instalação: O fornecedor da solução deverá providenciar treinamento/implantação da ferramenta proposta, visando atender as necessidades/implantação da solução proposta.
O programa para o treinamento deverá ser previamente aprovado pela contratante, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático;

No caso do treinamento fornecido não ser satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a *contratada* deverá realizar novo treinamento sem ônus adicional à contratante;
O material didático deverá estar incluído, sem custo adicional para a contratante;
Ao final do treinamento a *contratada* deverá emitir documento comprobatório da realização do Treinamento. Este documento deverá ser assinado pela *contratada*.
A *contratada* deverá apresentar, para aprovação da contratante, plano detalhado de implantação, especificando os procedimentos e prazos a serem adotados;
Todos os serviços necessários à implantação do software fornecido deverão ser obrigatoriamente descritos no plano de implantação, considerando a alocação de técnicos certificados pelo fabricante em análise e segurança de rede, não podendo gerar indisponibilidade dos serviços;
Após o recebimento do empenho a contratada deverá instalar a solução de Antivírus no prazo de 30 dias no máximo sem exceção.
A *contratada* será responsável pela remoção de quaisquer outros antivírus que a administração possuir, seja remotamente ou presencialmente total do parque de servidores e estações.

Período de Garantia do representante ou Fabricante (de Licenciamento): O período de licenciamento do software de Antivírus será de 12 (doze) meses, com suporte técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana Durante o período de licenciamento o fabricante vai garantir o funcionamento do software, com suporte técnico prestado em caso de falha. Deverá ser garantida neste prazo a atualização de versões, releases, componentes (vacinas, bibliotecas, filtros, etc), módulos e assinaturas dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento.
Iniciando ao fim da licença atualmente vigente.
Garantia do Fabricante e Capacitação:
A *contratada* deverá apresentar na fase de habilitação:
Carta de Revenda Autorizada do fabricante do Software a credenciando a prestar suporte, instalação do produto, fornecimento. A carta deverá ser do fabricante da Solução nomeando a revenda autorizada com a sua respectiva data de emissão e sua validade.
Apresentar certificado indicando o profissional da licitante que deverá implementar a solução. A licitante poderá apresentar mais um ou mais analistas certificado na solução. O certificado deverá ser emitido pelo fabricante oficial do Hardware e Software e a *contratada* deve apresentar o vinculo, seja CLT, Sócio cotista ou contratado, mas neste caso deve ser registrado em cartório provando o vinculo entre a licitante e o prestador.

Suporte Técnico do representante ou fabricante: Atender às necessidades do **ADM** para suporte técnico do software de Antivírus, com o objetivo de defender pró-ativamente o ambiente de TI da **ADM**, contra as possíveis ameaças que todo momento as organizações estão sujeitas.
Deverá ser prestado através de contato telefônico, Site de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou No Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência de acordo com os níveis de severidade indicados tabela 1 e 2.
O suporte técnico deverá ser obrigatoriamente fornecido em língua portuguesa;
O software de Antivírus fornecido deverá garantir a detecção limpeza e ou remoção de ocorrências nas estações e servidores protegidos, de forma automática, e em pelo menos 99,9% (noventa e nove vírgula nove) dos casos. Caso o software não detecte e remova a infecção automaticamente, a *contratada* será acionada e deverá fornecer vacina para solucionar o problema;
Em condições normais da rede o software de Antivírus fornecido deverá garantir a atualização automática das assinaturas de Vírus em pelo menos 96% (noventa e seis por cento) das estações e servidores em até no máximo 180 (cento e oitenta) minutos após o recebimento da mesma pelo servidor de Antivírus;

Descritivo de Antivírus

Tabela 1 Severidades:

Níveis de Severidade dos Chamados	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos consultas sobre problemas, dúvidas gerais sobre o software de antivírus.

Tabela de Prazos de Atendimentos ao Software				
Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
On Site e telefone	Início de Atendimento	1 hora	2 horas	24 horas
	Término de Atendimento	2 horas	4 horas	72 horas
Telefone, e-mail e Web-helpdesk	Início de Atendimento	-	-	24 horas
	Término de Atendimento	-	-	72 horas

A *contratada* deverá possuir Help desk para abertura de "chamados", disponibilizando telefones 011 ou 0800 para aberturas de chamados técnicos.

Deverá apresentar por declaração comprovando possuir condições para a prestação dos serviços para o **ADM** nas condições estipuladas acima.

Modelo de Proposta: Solução de Segurança

Item	Qtd.	Marca	Origem	V. Unitário	Valor Total
Licenciamento,Instalação, Migração, Projeto, de software de Segurança por 12 meses. Incluso na proposta: Treinamento 03 pessoas no mínimo. Suporte técnico por 12 meses ilimitado, presencial ou remoto (7x24).					
Valor TOTAL					