EMATER-DF – Empresa de Assistência Técnica e Extensão Rural do Distrito Federal

TERMO DE REFERÊNCIA EMATER-DF	
ELEMENTO DE DESPESA	**33.90.39 Serviços de Terceiros Pessoa Jurídica**
GRUPO	**05 Serviços Técnicos Profissionais**
CÓDIGO DO ITEM	**3.3.90.39.05.08.0001.000162-01**
PROCESSO 072.000.191/2015	

1. DO OBJETO:

Contratação de empresa especializada para fornecimento de 400 licenças de antivírus, com console de gerenciamento, incluindo instalação, treinamento e suporte técnico on-site ou remoto para atender as necessidades da EMATER-DF.

2. DA JUSTIFICATIVA:

Diante da crescente ameaça de softwares com códigos maliciosos e da necessidade de proteção do parque tecnológico da Emater-DF contra prejuízos gerados por tais códigos, da proteção da informação e da garantia de atuação rápida e suporte em caso de incidentes e principalmente à garantia de continuidade dos serviços no que tange o acesso e disponibilidade da informação e dos arquivos a qual esta empresa necessita.

Com o vencimento do contrato do software que atualmente exercia este papel e com a impossibilidade de renovação do contrato atual, foi levantada a necessidade desta proteção e do seu papel fundamental para a Emater-DF.

Informamos que o Almoxarifado da Gerência de Material e Patrimônio, sendo o responsável pelo controle do estoque dos materiais adquiridos pela EMATER-DF, avaliou o Pedido de Compra, e verificou que não possui o material solicitado em estoque.

A Metodologia para chegar ao quantitativo foi: pesquisa ao software de atendimento que apresentou o seguinte:

- 350 Desktops HP
- 050 Notebooks

Totalizando 400 equipamentos.

3. DAS ESPECIFICAÇÕES DO OBJETO:

Características levantadas pela equipe de T.I da Emater-DF e descritas abaixo:

3.1. Servidor de Administração e Console Administrativa

a) Compatibilidade com Microsoft Windows Server 2008
b) Compatibilidade com Microsoft Windows Server 2008 x64 SP1
c) Compatibilidade com Microsoft Windows Server 2008 R2
d) Compatibilidade com Microsoft Windows Server 2012
e) Compatibilidade com Microsoft Windows XP Professional SP2 ou superior
f) Compatibilidade com Microsoft Windows XP Professional x64
g) Compatibilidade com Microsoft Windows 7
h) Compatibilidade com Microsoft Windows 7 x64
i) Compatibilidade com Microsoft Windows 8
j) Compatibilidade com Microsoft Windows 8 x64
k) A console deve ser acessada via WEB (HTTPS) ou MMC;
l) Capacidade de remover remotamente qualquer solução de anti-virus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual anti-virus;
m) 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;
n) Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução anti-virus;
o) Capacidade de gerenciar smartphones e tablets (Windows Mobile, BlackBerry, Android e iOS) protegidos pela solução anti-virus;
p) Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
q) 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;
r) Capacidade de fazer distribuição remota de qualquer 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;
s) Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
t) Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;

u) Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
v) Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
w) 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;
x) 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 anti-virus automaticamente;
y) 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;
z) 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;

3.1.1. Deve fornecer as seguintes informações dos computadores:
a) Se o anti-virus está instalado;
b) Se o anti-virus está iniciado;
c) Se o anti-virus está atualizado;
d) Minutos/horas desde a última conexão da máquina com o servidor administrativo;
e) Minutos/horas desde a última atualização de vacinas
f) Data e horário da última verificação executada na máquina;
g) Versão do anti-virus instalado na máquina;
h) Se é necessário reiniciar o computador para aplicar mudanças;
i) Data e horário de quando a máquina foi ligada;
j) Quantidade de vírus encontrados (contador) na máquina;
k) Nome do computador;
l) Domínio ou grupo de trabalho do computador;
m) Data e horário da última atualização de vacinas;
n) Sistema operacional com Service Pack;
o) Quantidade de processadores;
p) Quantidade de memória RAM;

q) Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
r) Endereço IP;
s) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
t) Atualizações do Windows Updates instaladas
u) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD
v) Vulnerabilidades de aplicativos instalados na máquina

3.1.2. Deve permitir bloquear as configurações do anti-virus instalado nas estações e servidores de maneira que o usuário não consiga altera-las;

3.1.3. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

a) Mudança de gateway;
b) Mudança de subnet DNS;
c) Mudança de domínio;
d) Mudança de servidor DHCP;
e) Mudança de servidor DNS;
f) Mudança de servidor WINS;
g) Aparecimento de nova subnet;

3.1.4. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

3.1.5. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

3.1.6. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de anti-virus;

3.1.7. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

3.1.8. 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;

3.1.9. 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.

3.1.10. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF e HTML.

3.1.11. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

3.1.12. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

3.1.13. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

3.1.14. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

3.1.15. 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;

3.1.16. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

3.1.17. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

3.1.18. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

3.1.19. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

3.1.20. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

3.2. Compatibilidade com Estações Windows

a) Microsoft Windows XP Professional SP3
b) Microsoft Windows 7 Professional/Enterprise/Ultimate
c) Microsoft Windows 7 Professional/Enterprise/Ultimate x64
d) Microsoft Windows 8 Professional/Enterprise
e) Microsoft Windows 8 Professional/Enterprise x64

3.3. Características Estações Windows:

3.3.1. Deve prover as seguintes proteções:

a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

c) Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
d) Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc)
e) Firewall com IDS;
f) Autoproteção (contra ataques aos serviços/processos do antivírus);
g) Controle de dispositivos externos;
h) Controle de acesso a sites por categoria;
i) Controle de execução de aplicativos;
j) Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.3.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.3.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários em no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

3.3.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

3.3.5. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.3.6. 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;

3.3.7. 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;

3.3.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.3.9. 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;

3.3.10. Capacidade de verificar somente arquivos novos e alterados;

3.3.11. Capacidade de verificar objetos usando heurística;

3.3.12. Capacidade de agendar uma pausa na verificação;

3.3.13. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.3.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou;

b) Bloquear acesso ao objeto;

c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

Em caso positivo de desinfecção deve:

d) Restaurar o objeto para uso;

Em caso negativo de desinfecção:

e) Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

f) Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.3.15. 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);

3.3.16. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

3.3.17. Capacidade de verificar links inseridos em e-mails contra phishings;

3.3.18. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer e Firefox ;

3.3.19. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

3.3.20. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou;

b) Bloquear o e-mail;

c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

Em caso positivo de desinfecção:

d) Restaurar o e-mail para o usuário;

Caso negativo de desinfecção:

e) Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

3.3.21. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.

3.3.22. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

3.3.23. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.

3.3.24. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;

3.3.25. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

3.3.26. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

a) Perguntar o que fazer, ou;
b) Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
c) Permitir acesso ao objeto;

3.3.27. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

a) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
b) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

3.3.28. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

3.3.29. 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.

3.3.30. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

3.3.31. 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.

3.3.32. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

3.3.33. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

3.3.34. Deve 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.

3.3.35. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

b) 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 a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.3.36. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

a) Discos de armazenamento locais
b) Armazenamento removível
c) Impressoras
d) CD/DVD
e) Drives de disquete
f) Modems
g) Dispositivos de fita
h) Dispositivos multifuncionais
i) Leitores de smart card
j) Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)
k) Wi-Fi
l) Adaptadores de rede externos
m) Dispositivos MP3 ou smartphones
n) Dispositivos Bluetooth

3.3.37. 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.

3.3.38. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

3.3.39. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

3.3.40. Capacidade de configurar novos dispositivos por Class ID/Hardware ID

3.3.41. 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.

3.3.42. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).

3.3.43. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

3.3.44. 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.

3.3.45. 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.

3.3.46. 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.

3.4. Compatibilidade em estações de trabalho Linux

Plataforma 32-bits:

a) Canaima 3
b) Red Flag Desktop 6.0 SP2
c) Red Hat Enterprise Linux 5.8 Desktop
d) Red Hat Enterprise Linux 6.2 Desktop
e) Fedora 16
f) CentOS-6.2
g) SUSE Linux Enterprise Desktop 10 SP4
h) SUSE Linux Enterprise Desktop 11 SP2
i) openSUSE Linux 12.1
j) openSUSE Linux 12.2
k) Debian GNU/Linux 6.0.5
l) Mandriva Linux 2011
m) Ubuntu 10.04 LTS

n) Ubuntu 12.04 LTS

Plataforma 64-bits:

a) Canaima 3
b) Red Flag Desktop 6.0 SP2
c) Red Hat Enterprise Linux 5.8
d) Red Hat Enterprise Linux 6.2 Desktop
e) Fedora 16
f) CentOS-6.2
g) SUSE Linux Enterprise Desktop 10 SP4
h) SUSE Linux Enterprise Desktop 11 SP2
i) openSUSE Linux 12.1
j) openSUSE Linux 12.2
k) Debian GNU/Linux 6.0.5
l) Ubuntu 10.04 LTS
m) Ubuntu 12.04 LTS

3.5. Características em estações Linux:

3.5.1. Deve prover as seguintes proteções:

a) Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
c) Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
d) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
e) Gerenciamento 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;
f) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
g) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.5.2. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.5.3. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.5.4. 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;

3.5.5. Capacidade de verificar objetos usando heurística;

3.5.6. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

3.5.7. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

3.5.8. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.6. Compatibilidade em Servidores Windows

a) Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
b) Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
c) Microsoft Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 x86/x64
d) Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1
e) Microsoft Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1
f) Microsoft Windows Server 2012 Foundation/Essentials/Standard x64
g) Microsoft Windows Hyper-V Server 2008 R2 SP1
h) Microsoft Terminal baseado em Windows Server 2003
i) Microsoft Terminal baseado em Windows Server 2008
j) Microsoft Terminal baseado em Windows Server 2008 R2
k) Citrix Presentation Server 4.0 e 4.5
l) Citrix XenApp 4.5, 5.0 e 6.0

3.7. Características:

3.7.1. Deve prover as seguintes proteções:

a. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b. Autoproteção contra ataques aos serviços/processos do antivírus
c. Firewall com IDS
d. Controle de vulnerabilidades do Windows e dos aplicativos instalados

3.7.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.7.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.7.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
   a. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
   b. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
   c. Leitura de configurações
   d. Modificação de configurações
   e. Gerenciamento de Backup e Quarentena
   f. Visualização de relatórios
   g. Gerenciamento de relatórios
   h. Gerenciamento de chaves de licença
   i. Gerenciamento de permissões (adicionar/excluir permissões acima)

3.7.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
   a. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
   b. 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 a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.7.6. 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.

3.7.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)

3.7.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)

3.7.9. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

3.7.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

3.7.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.

3.7.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

3.7.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.7.14. 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;

3.7.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.7.16. 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;

3.7.17. Capacidade de verificar somente arquivos novos e alterados;

3.7.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc)

3.7.19. Capacidade de verificar objetos usando heurística;

3.7.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.7.21. Capacidade de agendar uma pausa na verificação;

3.7.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.7.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a. Perguntar o que fazer, ou;
b. Bloquear acesso ao objeto;
c. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

Caso positivo de desinfecção:

d. Restaurar o objeto para uso;

Caso negativo de desinfecção:

e. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.7.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

3.7.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

3.7.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

3.7.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.8. Compatibilidade Servidores Linux

Plataforma 32-bits:

a) Canaima 3
b) Asianux Server 3 SP4
c) Asianux Server 4 SP1
d) Red Hat Enterprise Linux 6.2 Server;
e) Red Hat Enterprise Linux 5.8 Server
f) Fedora 16;
g) CentOS-6.2;
h) SUSE Linux Enterprise Server 11 SP2;
i) Novell Open Enterprise Server 11;
j) openSUSE Linux 12.1;
k) openSUSE Linux 12.2;
l) Mandriva Enterprise Server 5.2;
m) Ubuntu Server 10.04.2 LTS;
n) Ubuntu Server 12.04 LTS;
o) Debian GNU/Linux 6.0.5;
p) FreeBSD 8.3;
q) FreeBSD 9.

Plataforma 64-bits:

a) Canaima 3
b) Asianux Server 3 SP4
c) Asianux Server 4 SP1
d) Red Hat Enterprise Linux 6.2 Server;
e) Red Hat Enterprise Linux 5.8 Server
f) Fedora 16;
g) CentOS-6.2;
h) SUSE Linux Enterprise Server 11 SP2;
i) Novell Open Enterprise Server 11;
j) openSUSE Linux 12.1;

k) openSUSE Linux 12.2;
l) Mandriva Enterprise Server 5.2;
m) Ubuntu Server 10.04.2 LTS;
n) Ubuntu Server 12.04 LTS;
o) Debian GNU/Linux 6.0.5;
p) FreeBSD 8.3;
q) FreeBSD 9.

3.8.1. Características:

3.8.2. Deve prover as seguintes proteções:

a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
c) Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
d) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
e) Gerenciamento 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;
f) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
g) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
h) Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
i) Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
j) 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;
k) Capacidade de verificar objetos usando heurística;

l) Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
m) Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
n) Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

3.9. Compatibilidade em estações de trabalho Windows:

a) Microsoft Windows XP Professional SP3
b) Microsoft Windows Vista Business/Enterprise/Ultimate SP2
c) Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
d) Microsoft Windows 7 Professional/Enterprise/Ultimate
e) Microsoft Windows 7 Professional/Enterprise/Ultimate x64
f) Microsoft Windows 8 Professional/Enterprise
g) Microsoft Windows 8 Professional/Enterprise x64

3.10. Características em estações de trabalho Windows:

a) O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.
b) Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
c) Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
d) Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
e) Permitir criar vários usuários de autenticação pré-boot.
f) Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
g) Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
h) Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
i) Criptografar todos os arquivos individualmente.
j) Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
k) Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
l) Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar

acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.

m) Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.

n) Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.

3.11. Gerenciamento de Sistemas:

o) Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal.

p) Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.

q) Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.

r) Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.

s) Capacidade de gerenciar licenças de softwares de terceiros.

t) Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

u) Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.

4. DA ESTRUTURA E TOPOLOGIA DE REDE DA EMATER-DF:

4.1. Fica facultado às empresas licitantes solicitar documento de topologia de rede da Emater-DF, visando entender melhor a estrutura da rede e seus componentes a fim de avaliar se o desempenho e o funcionamento da solução será satisfatório ;

4.2. Informações de caráter técnico podem ser prestadas pelo **Sr. Fabrício Portes Braga**, mediante agendamento prévio através do telefone 3311-9458

5. DA GARANTIA E DO SUPORTE TÉCNICO DA SOLUÇÃO:

5.1 As intervenções para suporte técnico e revisão de políticas deverão ser realizadas no local ou remotamente conforme prazos estabelecidos abaixo:

a) URGENTE - em casos que a ausência da manutenção ou suporte afetem consideravelmente o desempenho da rede ou a risco de comprometimento da disponibilidade de arquivos ou lentidão excessiva ou fato relevante (vírus) que esteja prejudicando mais de 30% dos equipamentos da Emater-DF.

I Remotamente, em até 12 horas da abertura do chamado;

II Presencialmente, em até 24 horas da abertura do chamado;

b) Normal - nos demais casos onde não exista urgência, o atendimento deverá ser realizado por agendamento entre as partes, não devendo ultrapassar 5 dias úteis

c) Em caso de não atendimento sem justificativa plausível, as penalidades abaixo podem vir a ser aplicadas:

Níveis	**Penalidade**
Urgente	**Multa de 1%** do valor do contrato, acrescidos de 0,1% por hora subsequente até a solução completa do problema.
Normal	**Multa de 0,33%** do valor do contrato, acrescidos de 0,1% por hora subsequente até a solução completa do problema.

6. DA TRANSFERÊNCIA DE TECNOLOGIA:

6.1 A licitante deverá promover um treinamento técnico mediante solicitação e agendamento, **sem ônus para a contratante** a no mínimo 3 funcionários indicados pela contratante. O treinamento deverá ser realizado nas dependências da licitante ou de forma remota (utilizando recursos de videoconferência ou tutoria on-line) e comportar no mínimo os seguintes pontos:

6.1.1 Operação do software de gerenciamento;

6.1.2 Análise de relatórios visando identificar infecções

6.1.3 Criação de políticas;

6.1.4 Identificação e correção de vulnerabilidades

6.1.5 Instalação e desinstalação remota de softwares;

6.1.6 Geração de relatórios e inventário de softwares

6.1.7 Geração de relatórios e inventário de hardwares

6.1.8 Criação, agendamento e execução de tarefas nas máquinas cliente;

6.1.9 Identificação e instalação do software localmente;

6.1.10 Geração de pacotes para instalação;

6.1.11 Funções do Firewall;

6.1.12 Definição e utilização de máquina cliente como repositório de vacinas

6.1.13 Controle de dispositivos externos;

6.1.14 Controle de acesso a sites por categoria;

6.1.15 Controle de execução de aplicativos;

6.2 A licitante deverá emitir certificado ao final do treinamento.

6.3 O prazo para execução do treinamento deve ser de no máximo 30 dias após a instalação do software, sob pena de inexecução parcial do contrato.

6.4 O treinamento deverá abortar todas as funcionalidades do equipamento, possuir carga horária de 12 horas, ocorrer em local físico disponibilizado pela licitante ou via videoconferência em horário comercial a ser definido pela licitante.

6.5 A licitante deverá fornecer material relacionado ao treinamento (apostila) em meio digital.

7. DA QUALIFICAÇÃO TÉCNICA:

7.1. A licitante deverá comprovar ter em seu quadro de funcionários, técnicos com certificação do fabricante da solução.

7.2. A licitante deverá apresentar comprovação de aptidão, mediante atestados de capacidade técnica, fornecidos por pessoas jurídicas de direito público ou privado, comprobatórios de atendimento satisfatório, similar ao objeto da presente licitação.

8. DA ESTIMATIVA DE CUSTO TOTAL:

8.1. A estimativa de custo total para a presente contratação deverá ser conforme anexo I;

9. DA ENTREGA, RECEBIMENTO E GARANTIA DOS EQUIPAMENTOS:

9.1. **Do prazo de entrega e instalação:** o prazo de **entrega e instalação** dos softwares será de até **15 (quinze) dias corridos** após a assinatura do contrato;

9.2. **Do recebimento provisório do objeto:** os softwares serão recebidos provisoriamente após **a entrega e instalação dos mesmos** para efeito de posterior verificação do funcionamento e da conformidade da solução com a especificação exigida neste Termo de Referência;

9.3. **Do recebimento definitivo do objeto:** o recebimento definitivo será realizado **após o período de funcionamento experimental de 5 dias úteis** com a verificação da qualidade, quantidade e funcionamento dos softwares e funções entregues pela licitante. Após o recebimento definitivo, será emitido o **Termo de Aceitação Definitivo** pela pessoa designada para este fim e o atesto da Nota Fiscal por empregado a ser designado em documentação própria;

9.4. Caso o software entregue estar em desacordo com o especificado neste Termo de Referência será rejeitado parcial ou totalmente, conforme o caso, podendo ser aplicadas sanções previstas.

9.5. O atendimento deverá ser realizado no local de instalação do Software de Gerenciamento, mais especificamente no **Ed. Sede da Emater-DF,** Empresa de Assistência Técnica e Extensão Rural do Distrito Federal **Parque Estação Biológica, Ed. Sede EMATER-DF CEP: 70.770.915 Brasília - DF** e deve ser realizado de forma presencial.

10. DO PAGAMENTO:

10.1. O pagamento deverá ser efetuado **em até 30 dias após o recebimento definitivo do objeto,** em conformidade com a legislação vigente;

10.2. O pagamento ficará condicionado à comprovação de regularidade junto à fazenda pública federal, estadual e municipal, assim como regularidade junto à receita federal (CND), fundo de garantia por tempo de serviço (FGTS), tribunal superior do trabalho (CNDT) e apresentação de **nota fiscal eletrônica** conforme protocolo icms 42, de 3 de julho de 2009 e suas alterações;

10.3. As empresas com sede ou domicílio no distrito federal, com créditos de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais), os pagamentos serão efetuados exclusivamente, mediante crédito em conta corrente, em nome do beneficiário junto ao Banco de Brasília S/A – BRB. Para tanto, deverão apresentar o número da conta corrente e agência onde deseja receber seus créditos, de acordo com o decreto nº 32.767/2011;

10.4. Empresas de outros estados que não tenham filial ou representação no Distrito Federal, poderão indicar conta corrente de outro banco, conforme decreto n º 32.767/2011.

11. DAS OBRIGAÇÕES DA LICITANTE:

11.1. **Entregar e instalar** os softwares, na localidade indicada, no prazo pactuado, utilizando apenas softwares fornecidos pelo fabricante da solução;

11.2. Responsabilizar-se por todas as despesas diretas ou indiretas tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no cumprimento de suas obrigações;

11.3. Cumprir prazos e condições estipulados neste Termo de Referência, observando-se as regras estabelecidas na Lei 8.666/93;

11.4. Responder pelos danos causados a EMATER-DF e/ou a terceiros decorrentes de culpa ou dolo de seus empregados e/ou prepostos quando da instalação e prestação de assistência técnica;

11.5. Cumprir todas as normas internas da EMATER-DF, bem como aquelas que regulam as ações de higiene e segurança do trabalho;

11.6. Prestar todos os esclarecimentos que lhe forem solicitados pela contratante;

11.7. Responsabilizar-se pelo pagamento de salários, encargos e demais verbas decorrentes do objeto desta contratação;

11.8. Manter durante a execução do contrato todas as **condições de habilitação**, assim como, fornecer sempre, à medida que forem vencendo os prazos de validade da documentação apresentada, novo(s) documento(s) que comprovem todas as condições de habilitação e qualificação exigidas para contratação, bem como os que comprovem sua compatibilidade com as obrigações assumidas;

12. DAS OBRIGAÇÕES DA CONTRATANTE:

12.1. Permitir livre acesso aos empregados da empresa vencedora ao local de entrega, instalação e execução dos serviços de garantia, desde que devidamente identificados;

12.2. Informar à LICITANTE e seus prepostos, tempestivamente, todas as providências necessárias ao bom andamento para a entrega dos softwares; prestar as informações e os esclarecimentos que venham a ser solicitados pela LICITANTE;

12.3. Comunicar prontamente a Licitante toda e qualquer anormalidade verificada nos softwares e/ou nos fornecimentos executados;

12.4. Efetuar o recebimento dos softwares conforme especificações do objeto e indicar o local para instalação dos mesmos;

12.5. Designar empregado para fiscalização da entrega e instalação do objeto desse Termo de Referência e da prestação da garantia;

12.6. **Rejeitar no todo ou em parte** o objeto entregue em desacordo com as especificações contidas neste Termo de Referência;

12.7. Exercer a fiscalização dos bens e serviços, na forma prevista na Lei n° 8.666/93, inclusive do cumprimento das obrigações e encargos sociais e trabalhistas pela LICITANTE, no que se refere à execução do contrato;

12.8. Verificar prazos, garantias, certidões e atestar notas fiscais;

12.9. Efetuar o pagamento em conformidade com a legislação vigente no Distrito Federal.

13. . DAS PENALIDADES

12.1. Pelo descumprimento de quaisquer cláusulas ou condições dispostas neste Projeto Básico, serão aplicadas as penalidades estabelecidas no Decreto nº 26.851/06 e atualizações, que regulamenta a aplicação de sanções administrativas previstas na Lei nº 8.666/93 e suas alterações, sem prejuízo aos definidos no item 5 deste termo, facultada à EMATER-DF, a rescisão unilateral do contrato.

14. DAS CONSIDERAÇÕES SOBRE A TOPOLOGIA DE REDE DA EMATER-DF:

Possui característica de descentralização, ou seja, um core da rede, que possui a função de agregador e 24 representações localizadas dispersas geograficamente por todo o Distrito Federal e entorno.

A tecnologia de comunicação entre a Sede e as representações, é basicamente rádio, o *throughput* médio é de 3 Mbps, existe ligação de fibra óptica entre dois pontos de concentração que demandam mais banda e 4 representações localizadas no entorno do DF não possuem ligação direta com a unidade Sede, possuindo apenas acesso a internet.

O documento que descreve em detalhes a topologia de rede da Emater-DF, poderá ser solicitado através do e-mail: fabricio.braga@emater.df.gov.br ou telefone (61) 3311-9458

15. DO FORO:

15.1. Fica eleito o foro da Justiça do Distrito Federal para dirimir as dúvidas não solucionadas administrativamente oriundas do comprimento das obrigações estabelecidas.

Brasília-DF, de junho de 2015.

Fernando Frazão da Silva
Gerente de Tecnologia da Informação

Fabrício Portes Braga
Técnico Especializado

Alessandro Miguel Ferreira Silva
Gerente de Material e Patrimônio