GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE FAZENDA E PLANEJAMENTO - SEFAZ
CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO – PRODERJ

1- DO OBJETO

1.1- Registro de Preços - RP, por 12 (doze) meses, visando à contratação de empresas para o fornecimento de licenciamento de produtos e serviços de segurança da informação como Desktops, Notebooks, Celulares, Tablets e Servidores, a saber: Licença de uso de Softwares e Serviços de instalação, customização, *mentoring, preventi*vas e corretivas, referentes aos softwares.

1.2- JUSTIFICATIVA

1.2.1- Com a explosão de uso de dispositivos móveis e a evolução no uso de dispositivos de armazenamento através de interfaces externas como a USB, e até a popularização do uso de computação e armazenamento em nuvem, a segurança de perímetro torne-se insuficiente para garantia à segurança em redes de dados locais. Os dispositivos como firewalls de rede, filtros webs, IDS e IPS não conseguem mais atuar de forma centralizada para garantir a segurança da informação dentro de redes locais, sendo necessário para isso que cada *endpoint* que esteja conectado a rede consiga prover dispositivos de segurança para si mesmo e desta forma contribuir para a segurança da rede como um todo.

1.2.2- Dentro deste cenário as redes de dados que atendem aos diversos órgãos do Estado do Rio de Janeiro encontram-se hoje totalmente desprotegidas, pois o software de proteção para *endpoint* utilizado nas estações de trabalho e notebooks eram “embarcados” junto ao equipamento que era alugado.

1.2.3- Com o termino dos contratos de aluguel às empresas fornecedoras deste serviço, deixaram de ter a obrigação de fornecer atualizações para o software de segurança. Logo, todos os mais de 30.000 (trinta mil) computadores conectados as redes de dados estão sem atualização e desta forma, apresentando vulnerabilidades de segurança como vimos recentemente na mídia, onde várias empresas foram atacadas e tiveram inclusive seus sistemas feitos de “refém”.

1.2.4- Ainda há de se considerar, que o novo processo de aluguel de microcomputadores e notebooks não inclui mais o fornecimento deste tipo de software, sendo necessária a aquisição por parte de cada órgão.

1.2.5- É importante ressaltar que o fornecimento do software em separado do equipamento possibilitará neste caso uma economia em ambos os certames, visto a possibilidade de empresas especializadas atuarem em cada certame de forma independente.

1.2.6- Outro ponto a ser considerado, se refere à padronização deste tipo de software para todo o Estado do Rio de Janeiro, pois através desta padronização será possível ter uma visão geral da situação de segurança dos *endpoints* possibilitando uma atuação mais efetiva do PRODERJ como gestor de segurança da informação.

1.2.7- Concluímos então que a contratação objeto deste certame e urgente e essencial para garantir a segurança dos sistemas de informação utilizados no Estado do Rio de Janeiro.

1.3– PLANILHA DE ITENS E PARA COTAÇÃO

	Item	Descritivo	Unidade	QTD	Valor unitário	Valor Total
Licenças	1.1	Servidor de administração e Console Administrativa	Por servidor de administração	114		
	1.2	Estações Windows	Por *endpoint*	74.092		
	1.3	Estações MAC OS X	Por *endpoint*	107		
	1.4	Estações de trabalho Linux	Por *endpoint*	295		
	1.5	Servidores Windows	Por *endpoint*	1.131		
	1.6	Servidores Linux	Por *endpoint*	960		
	1.7	Smartphones e tablets	Por *endpoint*	8.227		
	1.8	Gerenciamento de dispositivos móveis (MDM)	Por *endpoint*	8.163		
	1.9	Criptografia	Por *endpoint*	736		
	1.10	Gerenciamento de sistemas	Por *endpoint*	4.056		
Serviços	1.11	Instalação	UST	2.690		
	1.12	Customização	UST	2.180		
	1.13	Mentoring	UST	2.705		
	1.14	Manutenção corretiva e preventiva	UST	9.369		

2 – DA DESCRIÇÃO DOS PRODUTOS E SERVIÇOS

2.1 - Servidor de Administração e Console Administrativa

2.1.1 Compatibilidade:

Microsoft Windows Server 2008 (Todas edições);
Microsoft Windows Server 2008 x64 SP1 (Todas edições);
Microsoft Windows Server 2008 R2 (Todas edições);
Microsoft Windows Server 2012 (Todas edições);
Microsoft Windows Server 2012 R2 (Todas edições);
Microsoft Windows Small Business Server 2008 (Todas edições);
Microsoft Windows Small Business Server 2011 (Todas edições);
Microsoft Windows 7 Professional / Enterprise / Ultimate;

Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
Microsoft Windows 8 Professional / Enterprise;
Microsoft Windows 8 Professional / Enterprise x64;
Microsoft Windows 8.1 Professional / Enterprise;
Microsoft Windows 8.1 Professional / Enterprise x64.

2.1.2 Suporta as seguintes plataformas virtuais:

VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0;

Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
Microsoft VirtualPC 6.0.156.0;
Parallels Desktop 7 e superior;
Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
Citrix XenServer 6.1, 6.2.

2.1.3 Características:

2.1.4 A console deve ser acessada via WEB (HTTPS) ou MMC;
2.1.5 Console deve ser baseada no modelo cliente/servidor;
2.1.6 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
2.1.7 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
2.1.8 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
2.1.9 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
2.1.10 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
2.1.11 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
2.1.12 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
2.1.13 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
2.1.14 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
2.1.15 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
2.1.16 Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS e Android;
2.1.17 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
2.1.18 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
2.1.19 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
2.1.20 Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
2.1.21 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
2.1.22 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
2.1.23 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
2.1.24 A comunicação entre o cliente e o servidor de administração deve ser criptografada;

2.1.25 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

2.1.26 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

2.1.27 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

2.1.28 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

2.1.29 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

2.1.30 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;

2.1.31 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

2.1.32 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.

2.1.33 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;

2.1.34 Deve fornecer as seguintes informações dos computadores:

2.1.34.1 Se o antivírus está instalado;

2.1.34.2 Se o antivírus está iniciado;

2.1.34.3 Se o antivírus está atualizado;

2.1.34.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.1.34.5 Minutos/horas desde a última atualização de vacinas;

2.1.34.6 Data e horário da última verificação executada na máquina;

2.1.34.7 Versão do antivírus instalado na máquina;

2.1.34.8 Se é necessário reiniciar o computador para aplicar mudanças;

2.1.34.9 Data e horário de quando a máquina foi ligada;

2.1.34.10 Quantidade de vírus encontrados (contador) na máquina;

2.1.34.11 Nome do computador;

2.1.34.12 Domínio ou grupo de trabalho do computador;

2.1.34.13 Data e horário da última atualização de vacinas;

2.1.34.14 Sistema operacional com Service Pack;

2.1.34.15 Quantidade de processadores;

2.1.34.16 Quantidade de memória RAM;

2.1.34.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

2.1.34.18 Endereço IP;

2.1.34.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
2.1.34.20 Atualizações do Windows Updates instaladas;
2.1.34.21 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
2.1.34.22 Vulnerabilidades de aplicativos instalados na máquina;
2.1.35 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
2.1.36 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
2.1.36.1 Alteração de Gateway Padrão;
2.1.36.2 Alteração de subrede;
2.1.36.3 Alteração de domínio;
2.1.36.4 Alteração de servidor DHCP;
2.1.36.5 Alteração de servidor DNS;
2.1.36.6 Alteração de servidor WINS;
2.1.36.7 Alteração de subrede;
2.1.36.8 Resolução de Nome;
2.1.36.9 Disponibilidade de endereço de conexão SSL;
2.1.37 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
2.1.38 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
2.1.39 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
2.1.40 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
2.1.41 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;
2.1.42 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;
2.1.43 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
2.1.44 Capacidade de gerar traps SNMP para monitoramento de eventos;
2.1.45 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
2.1.46 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
2.1.47 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
2.1.48 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
2.1.49 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;
2.1.50 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
2.1.51 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2.1.52 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

2.1.53 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
2.1.54 Capacidade de realizar inventário de hardware de todas as máquinas clientes;
2.1.55 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
2.1.56 Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3. Estações Windows

Compatibilidade:

Microsoft Windows Embedded 8.0 Standard x64;
Microsoft Windows Embedded 8.1 Industry Pro x64;
Microsoft Windows Embedded Standard 7* x86 / x64 SP1;
Microsoft Windows Embedded POSReady 7* x86 / x64;
Microsoft Windows XP Professional x86 SP3 e superior;
Microsoft Windows Vista x86 / x64SP2 e posterior;
Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
Microsoft Windows 8 Professional/Enterprise x86 / x64;
Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
Microsoft Windows 10 Pro / Enterprise x86 / x64.

3.1 Características:

3.1.2- Deve prover as seguintes proteções:
3.1.3- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.1.4- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
3.1.5- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
3.1.6- Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
3.1.7- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
3.1.8- Firewall com IDS;
3.1.9- Autoproteção (contra-ataques aos serviços/processos do antivírus);
3.1.10- Controle de dispositivos externos;
3.1.11- Controle de acesso a sites por categoria;
3.1.12- Controle de acesso a sites por horário;
3.1.13- Controle de acesso a sites por usuários;

3.1.14- Controle de execução de aplicativos;
3.1.15- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
3.1.16- Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.1.17- As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
3.1.18- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.1.19- 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;
3.1.20- 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;
3.1.21- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.1.22- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.1.23- 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 tomar a partir da extensão do arquivo;
3.1.24- Capacidade de verificar somente arquivos novos e alterados;
3.1.25- Capacidade de verificar objetos usando heurística;
3.1.26- Capacidade de agendar uma pausa na verificação;
3.1.27- Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
3.1.28- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
3.1.29- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.1.29 a) Perguntar o que fazer, ou;
3.1.29 b) Bloquear acesso ao objeto;
3.1.30- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.1.31- Caso positivo de desinfecção:
3.1.31- a) Restaurar o objeto para uso.
3.1.32- Caso negativo de desinfecção:
3.1.32- b) Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).
3.1.33- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.1.34- 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);
3.1.35- Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
3.1.36- Capacidade de verificar links inseridos em e-mails contra phishings;
3.1.37- Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
3.1.38- Capacidade de verificação de corpo e anexos de e-mails usando heurística;
3.1.39- O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
3.1.39- a)Perguntar o que fazer, ou;
3.1.39- b)Bloquear o e-mail.
3.1.40- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.1.41 Caso positivo de desinfecção:
3.1.41- a) Restaurar o e-mail para o usuário.
3.1.42 Caso negativo de desinfecção:
3.1.42- b) Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

3.1.43- Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
3.1.44- Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
3.1.45- Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
3.1.46- Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
3.1.47- Deve ter suporte total ao protocolo IPv6;
3.1.48- Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
3.1.49- Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
3.1.49- a)Perguntar o que fazer, ou;
3.1.49- b)Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
3.1.49- c)Permitir acesso ao objeto.
3.2 - O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
3.2.1- Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
3.2.2- Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
3.2.3- Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
3.2.4- 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;
3.2.5- Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
3.2.6- 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;
3.2.7- Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
3.2.8- Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
3.2.9- 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;
3.2.10- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
3.2.10.1- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; e
3.2.10.2- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
3.2.11- Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
3.2.11.1- Discos de armazenamento locais;
3.2.11.2- Armazenamento removível;
3.2.11.3- Impressoras;
3.2.11.4- CD/DVD;
3.2.11.5- Drives de disquete;
3.2.11.6- Modems;
3.2.11.7- Dispositivos de fita;
3.2.11.8- Dispositivos multifuncionais;

3.2.11.9- Leitores de smart card;
3.2.11.10- Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
3.2.11.11- Wi-Fi;
3.2.11.12- Adaptadores de rede externos;
3.2.11.13- Dispositivos MP3 ou smartphones;
3.2.11.14- Dispositivos Bluetooth; e
3.2.11.15- Câmeras e Scanners.
3.3- Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
3.3.1- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
3.3.2- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
3.3.3- Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
3.3.4- 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;
3.3.5- 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);
3.3.6- Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
3.3.7- 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;
3.3.8- 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 à web; e
3.3.9- 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 à web.

4) Estações Mac OS X

4.1- Compatibilidade:

4.1.1- Mac OS X 10.11 (El Capitan);
4.1.2- Mac OS X 10.10 (Yosemite);
4.1.3- Mac OS X 10.9 (Mavericks).
4.1.4- Mac OS X 10.8 (Mountain Lion)
4.1.5- Mac OS X 10.7 (Lion)
4.1.6- Mac OS X 10.12 (Sierra)

5 Características:

5.1.1- Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.1.2- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.1.3- A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
5.1.4- Deve possuir suportes a notificações utilizando o Growl;

5.1.5- As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
5.1.6- Capacidade de voltar para a base de dados de vacina anterior;
5.1.7- Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
5.1.8- 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;
5.1.9- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
5.1.10- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
5.1.11- Capacidade de verificar somente arquivos novos e alterados;
5.1.12- Capacidade de verificar objetos usando heurística;
5.1.13- Capacidade de agendar uma pausa na verificação;
5.1.14- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.1.14-1. Perguntar o que fazer, ou;
5.1.14-2. Bloquear acesso ao objeto;
5.1.14-2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.1.14-2.2. Caso positivo de desinfecção:
5.1.14-2.2.1. Restaurar o objeto para uso;
5.1.14-2.3. Caso negativo de desinfecção:
5.1.14-2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.1.15- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.1.16- Capacidade de verificar arquivos de formato de email;
5.1.17- Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
5.1.18- Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

6. Estações de trabalho Linux

6.1. Compatibilidade:

6.1.1- Plataforma 32-bits:

6.1.1-1. Canaima 3;
6.1.1-2. Red Flag Desktop 6.0 SP2;
6.1.1-3. Red Hat Enterprise Linux 5.8 Desktop;

6.1.1-4. Red Hat Enterprise Linux 6.2 Desktop;
6.1.1-5. Fedora 16;
6.1.1-6. CentOS-6.2;
6.1.1-7. SUSE Linux Enterprise Desktop 10 SP4;
6.1.1-8. SUSE Linux Enterprise Desktop 11 SP2;
6.1.1-9. openSUSE Linux 12.1;
6.1.1-10. openSUSE Linux 12.2;
6.1.1-11. Debian GNU/Linux 6.0.5;
6.1.1-12. Mandriva Linux 2011;
6.1.1-13. Ubuntu 10.04 LTS;
6.1.1-14. Ubuntu 12.04 LTS.

6.1.2- Plataforma 64-bits:

6.1.2-1. Canaima 3;
6.1.2-2. Red Flag Desktop 6.0 SP2;
6.1.2-3. Red Hat Enterprise Linux 5.8;
6.1.2-4. Red Hat Enterprise Linux 6.2 Desktop;
6.1.2-5. Fedora 16;
6.1.2-6. CentOS-6.2;
6.1.2-7. SUSE Linux Enterprise Desktop 10 SP4;
6.1.2-8. SUSE Linux Enterprise Desktop 11 SP2;
6.1.2-9. openSUSE Linux 12.1;
6.1.2-10. openSUSE Linux 12.2;
6.1.2-11. Debian GNU/Linux 6.0.5;
6.1.2-12. Ubuntu 10.04 LTS;
6.1.2-13. Ubuntu 12.04 LTS.

6.2. Características:

6.2.1- Deve prover as seguintes proteções:
6.2.1-1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.1-2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.2.2- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.2.2-1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

6.2.2-2. 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;
6.2.2-3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.2.2-4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

6.2.3- Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

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

6.2.5- 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 tomar a partir da extensão do arquivo;

6.2.6- Capacidade de verificar objetos usando heurística;

6.2.7- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

6.2.8- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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

7. Servidores Windows

7.1. Compatibilidade:

7.2. Plataforma 32-bits:

7.2.1- Microsoft Windows Server 2003 Standard / Enterprise (SP2);

7.2.2- Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);

7.2.3- Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

7.2.4- Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

7.3. Plataforma 64-bits:

7.3.1- Microsoft Windows Server 2003 Standard / Enterprise (SP2);

7.3.2- Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);

7.3.3- Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

7.3.4- Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

7.3.5- Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

7.3.6- Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

7.3.7- Microsoft Windows Storage Server 2008 R2;

7.3.8- Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);

7.3.9- Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

7.3.10- Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

7.3.11- Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

7.3.12- Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

7.3.13- Microsoft Windows Storage Server 2012 (Todas edições);

7.3.14- Microsoft Windows Storage Server 2012 R2 (Todas edições);

7.3.15- Microsoft Windows Hyper-V Server 2012;

7.3.16- Microsoft Windows Hyper-V Server 2012 R2.

7.4. Características:

7.4.1- Deve prover as seguintes proteções:
7.4.1-1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
7.4.1-2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
7.4.1-3. Firewall com IDS;
7.4.1-4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
7.4.2- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
7.4.3- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
7.4.4- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
7.4.4-1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
7.4.4-2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
7.4.4-3. Leitura de configurações;
7.4.4-4. Modificação de configurações;
7.4.4-5. Gerenciamento de Backup e Quarentena;
7.4.4-6. Visualização de relatórios;
7.4.4-7. Gerenciamento de relatórios;
7.4.4-8. Gerenciamento de chaves de licença;
7.4.4-9. Gerenciamento de permissões (adicionar/excluir permissões acima);
7.4.5- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
7.4.5-1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
7.4.5-2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
7.4.6- 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;
7.4.7- Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
7.4.8- Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*);
7.4.9- Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

7.4.10- Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
7.4.11- Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
7.4.12- Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
7.4.13- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
7.4.14- 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;
7.4.15- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
7.4.16- 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 tomar a partir da extensão do arquivo;
7.4.17- Capacidade de verificar somente arquivos novos e alterados;
7.4.18- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
7.4.19- Capacidade de verificar objetos usando heurística;
7.4.20- Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
7.4.21- Capacidade de agendar uma pausa na verificação;
7.4.22- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
7.4.23- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
7.4.23-1. Perguntar o que fazer, ou;
7.4.23-2. Bloquear acesso ao objeto;
7.4.23-2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
7.4.23-2.2. Caso positivo de desinfecção:
7.4.23-2.2.1. Restaurar o objeto para uso;
7.4.23-2.3. Caso negativo de desinfecção:
7.4.23-2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
7.4.24- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
7.4.25- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
7.4.26- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
7.4.27- Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

8. Servidores Linux

8.1. Compatibilidade:

8.1- a) Plataforma 32-bits:

8.1.1- Red Hat Enterprise Linux Server 5.x;
8.1.2- Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);

8.1.3- CentOS 6.x (6.0 - 6.6);
8.1.4- SUSE® Linux Enterprise Server 11 SP3;
8.1.5- Ubuntu Server 12.04 LTS;
8.1.6- Ubuntu Server 14.04 LTS;
8.1.7- Ubuntu Server 14.10;
8.1.8- Oracle Linux 6.5;
8.1.9- Debian GNU/Linux 7.5, 7.6, 7.7;
8.1.10- openSUSE 13.1.
8.1.11- Plataforma 64-bits:
8.1.12- Red Hat Enterprise Linux Server 5.x;
8.1.13- Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
8.1.14- Red Hat Enterprise Linux Server 7;
8.1.15- CentOS-6.x (6.0 - 6.6);
8.1.16- CentOS-7.0;
8.1.17- SUSE Linux Enterprise Server 11 SP3;
8.1.18- SUSE Linux Enterprise Server 12;
8.1.19- Novell Open Enterprise Server 11 SP1;
8.1.20- Novell Open Enterprise Server 11 SP2;
8.1.21- Ubuntu Server 12.04 LTS;
8.1.22- Ubuntu Server 14.04 LTS;
8.1.23- Ubuntu Server 14.10;
8.1.24- Oracle Linux 6.5;
8.1.25- Oracle Linux 7.0;
8.1.26- Debian GNU/Linux 7.5, 7.6, 7.7;
8.1.27- openSUSE® 13.1.

9 Características:

9.1 Deve prover as seguintes proteções:
9.1.1- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
9.1.2- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
9.1.3- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
9.1.3-1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
9.1.3-2. 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;

9.1.3-3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

9.1.3-4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

9.1.4- Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

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

9.1.6- 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 tomar a partir da extensão do arquivo;

9.1.7- Capacidade de verificar objetos usando heurística;

9.1.8- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

9.1.9- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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

10 Smartphones e Tablets

10.1 Compatibilidade:

10.1.1 Apple iOS 7.0 – 8.X;

10.1.2 Windows Phone 8.1;

10.1.3 Android OS 2.3 – 5.1.

10.2 Características:

10.2.1 Deve prover as seguintes proteções:

10.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

10.2.1.1.1 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

10.2.1.1.2 Arquivos abertos no smartphone;

10.2.1.1.3 Programas instalados usando a interface do smartphone

10.2.1.2 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

10.2.2 Deverá isolar em área de quarentena os arquivos infectados;

10.2.3 Deverá atualizar as bases de vacinas de modo agendado;

10.2.4 Deverá bloquear spams de SMS através de Black lists;

10.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

10.2.6 Capacidade de desativar por política:

10.2.7 Wi-fi;
10.2.7.1- Câmera;
10.2.7.2- Bluetooth.
10.2.8 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
10.2.9 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
10.2.10 Deverá ter firewall pessoal (Android);
10.2.11 Capacidade de tirar fotos quando a senha for inserida incorretamente;
10.2.12 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

10.2.13 Capacidade de enviar comandos remotamente de:
10.2.13.1- Localizar;
10.2.13.2- Bloquear.
10.2.14 Capacidade de detectar Jailbreak em dispositivos iOS;
10.2.15 Capacidade de bloquear o acesso a site por categoria em dispositivos;
10.2.16 Capacidade de bloquear o acesso a sites phishing ou malicioso;
10.2.17 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
10.2.18 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
10.2.19 Capacidade de configurar White e blacklist de aplicativos;
10.2.20 Capacidade de localizar o dispositivo quando necessário;
10.2.21 Permitir atualização das definições quando estiver em “roaming”;
10.2.22 Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
10.2.23 Capacidade de enviar URL de instalação por e-mail;
10.2.24 Capacidade de fazer a instalação através de um link QRCode;
10.2.25 Capacidade de executar as seguintes ações caso a desinfecção falhe:
a) Deletar;
b) Ignorar;
c) Quarentenar;
d) Perguntar ao usuário.

11 Gerenciamento de dispositivos móveis (MDM)

11.1 Compatibilidade:

11.1.1 Dispositivos conectados através do Microsoft Exchange ActiveSync:
11.1.1.1 Apple iOS;
11.1.1.2 Windows Phone;
11.1.1.3 Android.
11.1.2 Dispositivos com suporte ao Apple Push Notification (APNs).
11.1.2.1 Apple iOS 3.0 ou superior.
11.1.2.2

11.2 Características:

11.2.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
11.2.2 Capacidade de ajustar as configurações de:
11.2.2.1 Sincronização de e-mail;
11.2.2.2 Uso de aplicativos;
11.2.2.3 Senha do usuário;
11.2.2.4 Criptografia de dados;
11.2.2.5 Conexão de mídia removível.
11.2.3 Capacidade de instalar certificados digitais em dispositivos móveis;

11.2.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS;
11.2.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
11.2.6 Capacidade de, remotamente, bloquear um dispositivo iOS.

12 Criptografia

12.1 Compatibilidade:

12.1.1 Microsoft Windows XP Professional SP3 ou superior;
12.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2;
12.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;

12.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate;
12.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64;
12.1.6 Microsoft Windows 8 Professional/Enterprise;
12.1.7 Microsoft Windows 8 Professional/Enterprise x64;
12.1.8 Microsoft Windows 8.1 Professional / Enterprise;
12.1.9 Microsoft Windows 8.1 Professional / Enterprise x64;
12.1.10 Microsoft Windows 10 Pro x86 / x64;
12.1.11 Microsoft Windows 10 Enterprise x86 /x64.

12.2 Características:

12.2.1 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;
12.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
12.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
12.2.4 Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
12.2.5 Permitir criar vários usuários de autenticação pré-boot;
12.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
12.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
12.2.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
12.2.7.2 Criptografar todos os arquivos individualmente;

12.2.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

12.2.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

12.2.8 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;

12.2.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

12.2.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

12.2.11 Verifica compatibilidade de hardware antes de aplicar a criptografia;

12.2.12 Possibilita estabelecer parâmetros para a senha de criptografia;

12.2.13 Bloqueia o reuso de senhas;

12.2.14 Bloqueia a senha após um número de tentativas pré-estabelecidas;

12.2.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

12.2.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

12.2.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

12.2.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

12.2.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

12.2.20 Permite criar um grupo de extensões de arquivos a serem criptografados;

12.2.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

12.2.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

13 Gerenciamento de Sistemas

13.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;

13.2 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

13.3 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;

13.4 Capacidade de gerenciar licenças de softwares de terceiros;

13.5 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

13.6 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;

13.7 Possibilita fazer distribuição de software de forma manual e agendada;
13.8 Suporta modo de instalação silenciosa;
13.9 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
13.10 Possibilita fazer a distribuição através de agentes de atualização;
13.11 Utiliza tecnologia multicast para evitar tráfego na rede;
13.12 Possibilita criar um inventário centralizado de imagens;
13.13 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
13.14 Suporte a WakeOnLan para deploy de imagens;
13.15 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

13.16 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
13.17 Capacidade de gerar relatórios de vulnerabilidades e patches;
13.18 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
13.19 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
13.20 Permite baixar atualizações para o computador sem efetuar a instalação
13.21 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
13.22 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
13.23 Permite selecionar produtos a serem atualizados pela console de gerenciamento;
13.24 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

14 Ju*stificativa para agrupamento em um único lote:*

14.1- O primeiro ponto a ser considerado é que o agrupamento das licenças aqui propostas não restringe a participação nem a competitividade, visto que, existem vários fornecedores que estão habilitados a fornecer todas as licenças, sem restrição.

14.2- A outra questão a ser considerada refere-se à interoperabilidade entre as diversas licenças ofertadas. Um único item não é capaz de oferecer sozinho um serviço de TIC, sendo necessária a integração com outros produtos, desta forma a separação do lote por itens acarretaria em um alto custo na gestão de diversos fornecedores para um único serviço de TIC, que será gerido.

14.3- Ainda há de se considerar que projetos que sejam oriundos desta ata irão ter forte interoperabilidade entre diversas licenças e serviços aqui ofertados. Logo quando temos um único fornecedor o trabalho de gestão fica mais eficiente e eficaz, pois o CONTRATANTE pode focar no sucesso do projeto sem a necessidade de gerenciamento de conflitos entre vários fornecedores.

15. SERVIÇOS

15.1 – Descritivo:

15.1- Os serviços ofertados têm seu escopo limitado a serviços que sejam direcionados as licenças de software descritas neste certame, ou seja, a CONTRATADA atuará exclusivamente em serviços relacionados aos produtos ofertados nos itens de licenciamento.

15.2- A unidade de medida adotada em cada classe de serviço denomina-se Unidade de Serviço Técnico – UST, que corresponde ao esforço para a realização e conclusão das atividades definidas, independentemente da quantidade de recursos alocados condicionados a pagamento por resultados e atendimento aos níveis de serviços.

15.3- Não está previsto a contratação de serviços continuados para sustentação e operação de ambientes. Os serviços fornecidos devem estar caracterizados em uma das seguintes classes:

a) Instalação

Serviços de instalação dos softwares

b) Customização

Customização a parametrização, conforme especificações técnicas disponibilizadas pela CONTRATANTE.

c) Mentoring

15.4- Passagem de conhecimento técnico dos softwares. Essa passagem de conhecimento deverá ser realizada no modelo *hands-on,* onde a CONTRATADA deverá prover um profissional devidamente certificado em tecnologia Microsoft.

15.5- O escopo do *mentoring* será especificado pela CONTRATANTE e poderá ser fornecido no formato de treinamento oficial do fabricante.

d) Manutenção preventiva

Realização de procedimentos de *tunning,* instalações de correções e atualizações dos softwares.

e) Manutenção corretiva e preventiva

Realização de correções de falhas, mal funcionamento e performance abaixo dos padrões estabelecidos pela CONTRATANTE.

15.6- As tabelas abaixo apresentam as expectativas de esforço, em UST – Unidade de Serviço Técnico para as classes de serviços já definida e baseadas nas tecnologias Microsoft fornecidas, conforme quantitativos abaixo:

15.7- Os quantitativos serão calculados de acordo com o número de licenças solicitadas.

	Item	Descrição	Unidade	Valor estimado para cada 100 *endpoints*
Serviços	1.11	Instalação	UST	16
	1.12	Customização	UST	24
	1.13	Mentoring	UST	16
	1.14	Manutenção corretiva e preventiva	UST	32

Total de USTs	
Valor unitário da UST	
Valor total	

16 - DAS OBRIGAÇÕES DO CONTRATANTE

*16.1- Efetuar os pagamentos devidos à Contratada, na forma estabelecida no **Edital**.*

16.2 – Fornecer à Contratada os documentos, informações e demais elementos que possuir ligados ao presente Contrato.

16.3 - Designar comissão responsável para o acompanhamento e fiscalização do objeto licitado.

16.4 - Receber o objeto, após a verificação do atendimento integral das especificações requeridas.

16.5 – Supervisionar e controlar os serviços executados, a fim de atestar as faturas apresentadas pela Contratada.

16.6 - Comunicar à Contratada qualquer anormalidade ocorrida na execução do objeto, diligenciando para que as irregularidades ou falhas sejam plenamente corrigidas.

16.7 - Notificar, por escrito, a Contratada da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e a ampla defesa.

17 - DAS OBRIGAÇÕES DA CONTRATADA

17.1 - Assinar a Ata de Registro de Preço, no prazo e condições previstos no **Edital.**

17.2 - Entregar os produtos contratados, nas versões originais do fabricante em inglês, no prazo de até 30 (trinta) dias úteis, a contar da data da formalização do instrumento contratual ou da autorização de fornecimento pelos Órgãos Aderentes.

17.3 – Fornecer upgrades para novas versões e novos patches disponibilizados pelo fabricante.

17.4 - Disponibilizar canais de acesso 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, através de número de telefone de discagem gratuita (0800) e/ou Internet, para abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares; e permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos da Microsoft.

17.5 - Dar garantias técnicas dos serviços executados (treinamento e suporte técnico especializado) e dos produtos entregues.

17.6 - Possuir em seu quadro de empregados, Profissionais Certificados, para atendimento dos serviços.

17.7 - Comprovar o atendimento do **subitem 17.6**, na ocasião da assinatura da Ata do Registro de Preços, através das cópias do registro na CTPS, ficha de empregado, Contrato de Trabalho ou de Contrato de Prestação de Serviços e ainda, com os respectivos certificados.

17.8 - Sujeitar-se à fiscalização do órgão Contratante quanto ao acompanhamento do cumprimento das obrigações pactuadas, prestando-lhe todos os esclarecimentos solicitados, bem como atendendo às reclamações consideradas procedentes.

17.9 - Aceitar, nas mesmas condições pactuadas, os acréscimos ou supressões que se fizerem necessários no objeto licitado, até o limite previsto no § 1º do art. 65 da Lei nº 8.666/93.

18- REQUISITOS DE SEGURANÇA

18.1- A empresa contratada para prestação dos serviços deverá observar os seguintes requisitos quanto à Segurança da Informação e Comunicações:

18.1.1-Tomar todas as providências necessárias para que seus funcionários, prepostos e/ou contratados observem os regulamentos, normas e instruções de segurança da informação e comunicações adotados pelo CONTRATANTE, inclusive, a Política de Segurança da Informação e Comunicações, Normas de Segurança e o Termo de Confidencialidade, quando estiverem executando serviços nas instalações do CONTRATANTE;

18.1.2-Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou deles dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação;

18.1.3- Toda informação confidencial disponível em razão desta contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses: (I) término ou rompimento do Contrato; (II) solicitação do CONTRATANTE;

18.1.4-Utilizar programas de proteção e segurança de informações, a fim de evitar qualquer acesso não autorizado aos seus sistemas ou softwares, seja em relação aos que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados para o CONTRATANTE, ainda que por meio de link;

18.1.5- Quando solicitado por escrito pelo CONTRATANTE, realizar, prioritária e concomitantemente, as alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado; e

18.1.6- Assegurar que os dispositivos fornecidos pelo CONTRATANTE para armazenamento de informações (exemplo: mídias magnéticas, eletrônicas, óticas) ou, ainda, os ambientes tecnológicos, canais de comunicação entre as partes (exemplo: sites, links, hiperlinks, etc.), estejam livres de programas de computadores ou outros recursos tecnológicos que possam causar perda de integridade, confidencialidade ou disponibilidade de dados ou informações do CONTRATANTE (exemplo: vírus, cavalos de Tróia, etc.).

19- NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS

19.1- Níveis de serviço são critérios objetivos e mensuráveis estabelecidos pelo CONTRATANTE com a finalidade de aferir e avaliar diversos fatores relacionados com os serviços contratados, bem como para orientar o pagamento por resultados obtidos.

19.2- A contratação prevê a definição de Níveis de Serviço como meio de aferição dos chamados atendidos. No modelo proposto haverá aferição e avaliação mensal dos níveis de serviço acordados. Em geral, os níveis de serviço são aferidos em função da qualidade e desempenho. Para a presente contratação, os níveis de serviços indicarão os prazos máximos para resposta e efetiva solução dos chamados ou Ordem de Serviço.

19.3 - Caberá à CONTRATADA a elaboração de relatórios a serem apresentados ao CONTRATANTE para aferição dos níveis de serviço, descrito abaixo:

Nº 01 - INDICADOR DE ORDENS DE SERVIÇO ATENDIDAS NO PRAZO	
Características do Indicador	**Descrição**
1. Finalidade	Os indicadores de evolução serão aferidos a cada entrega de um pacote, previsto na Ordem de Serviço, entregue pela Contratada ao CONTRATANTE.
2. Meta a cumprir	Indicador de Faixa de Ajuste inferior a 11 (onze).
3. Instrumento de medição	Relatório de Ordens de Serviço
4. Forma de acompanhamento	A CONTRATADA deverá gerar o relatório de ordens de serviço concluídas e homologadas pela CONTRATANTE, contendo os seguintes itens para avaliação: 1. Identificador da OS; 2. Quantidade de Horas Previstas da OS; 3. Nome das Atividades Previstas na OS; 4. Data de início da execução da OS; 5. Esforço previsto para execução da OS em dias; 6. Tempo total utilizado para a execução da OS em dias.
5. Periodicidade	Mensal
6. Mecanismo de Cálculo	1. Índice de Atendimento de Prazo dos Pacotes da OS (IAPe) a. IAPe: Prevê multas para o não atendimento de prazos de entrega dos pacotes acordados em Ordem de Serviço 2. Fórmula: a. IAPe = (Qtde dias úteis realizados / Qtde dias úteis previstos) – 1 * 100 i. 14.1.2 Para cálculo da variável “Qtde dias úteis realizados”, será considerada como data de conclusão a última data de entrega de todos os itens de um pacote acordados em Ordem de Serviço pela Contratada; ii. 14.1.3 Qtde dias úteis realizados = Data de Conclusão do Pacote – Data de Início do Pacote
7. Início de Vigência	Data da assinatura do Contrato

8. Faixas de ajuste no pagamento	**Resultado atingido no item "6. Mecanismo de Cálculo (IAPe)"**	**Descrição**
	Abaixo de 20%	Nível aceitável – Não será cobrada multa. Será considerado 100% do valor da OS
	Entre 20,01 e 40%	Multa de 0,5% sobre o valor da respectiva OS
	Entre 40,01 e 60%	Multa de 1% sobre o valor da respectiva OS
	Entre 60,01 e 80%	Multa de 1,5% sobre o valor da respectiva OS
	Acima de 80%	Multa de 2% sobre o valor da respectiva OS

N º 02 – INDICADOR DE SERVIÇOS COM DESVIO DE QUALIDADE	
Item	**Descrição**
1. Finalidade	Indicador para avaliar a qualidade sobre as Ordens de Serviços evolutivas, corretivas e adaptativas dos tipos DEMANDA, ROTINEIRA ou INCIDENTES entregues pela CONTRATADA à CONTRATANTE.
2. Meta a cumprir	Indicador de Faixa de ajuste igual a 1 (um).
3. Instrumento de medição	A CONTRATADA deverá gerar o relatório de ordens de serviço entregues para a CONTRATANTE, contendo os seguintes itens para avaliação: 1. Identificador da OS; 2. Nome da Atividade; 3. Quantidade de Recusas da Ordem de Serviço por desvio de qualidade dos serviços prestados; 4. Responsável da CONTRATANTE pela homologação.

<table>
<tr><td>4. Forma de acompanhamento</td><td colspan="3">A CONTRATADA deverá efetuar a entrega mensal dos serviços, e submeter a um responsável indicado pela CONTRATANTE pela avaliação, aprovação e homologação das Ordens de Serviços.

Caso a CONTRATANTE verifique que algumas das cláusulas de recebimento definitivo da OS não estejam de acordo com o definido neste documento e no item “17 ACEITE, ALTERAÇÃO E CANCELAMENTO DOS SERVIÇOS”, será sinalizado que ocorreu desvio da qualidade na Ordem de Serviço.</td></tr>
<tr><td>5. Periodicidade</td><td colspan="3">Mensal</td></tr>
<tr><td>6. Mecanismo de Cálculo</td><td colspan="3">Fórmula: Quantidade de Recusas da Ordem de Serviço por desvio de qualidade dos serviços prestados.

Para o cálculo da fórmula acima, será considerado o seguinte:
1. Quantidade de Recusas da Ordem de Serviço por desvio de qualidade dos serviços prestados: é a Quantidade total mensal das recusas da Ordem de Serviço por desvio de qualidade durante o ciclo de vida.
2. O Resultado atingido nesse item é a quantidade absoluta de artefatos recusados por entrega mensal efetuada.</td></tr>
<tr><td>7. Início de Vigência</td><td colspan="3">Data da assinatura do Contrato.</td></tr>
<tr><td rowspan="5">8. Faixas de ajuste no pagamento</td><td>Resultado atingido no item “6. Mecanismo de Cálculo”</td><td>Descrição</td><td>Considerar Faixa de ajuste</td></tr>
<tr><td>0 a 5</td><td>Nível aceitável - Será considerado 100% do valor da OS</td><td>Igual a 1 (um)</td></tr>
<tr><td>6 a 10</td><td>Será considerado 99% do valor da OS</td><td>Igual a 0,99 (nove vírgula seis décimos)</td></tr>
<tr><td>11 a 15</td><td>Será considerado 98% do valor da OS</td><td>Igual a 0,98 (nove vírgula três décimos)</td></tr>
<tr><td>Acima de 15</td><td>Será considerado 97% do valor da OS</td><td>Igual a 0,97 (zero vírgula noventa).</td></tr>
</table>

16.4- Pelo descumprimento das metas exigidas nas tabelas “Tabela 1 - Cálculos de Níveis de Serviços Atendidos no Prazo” e “Tabela 2 - Cálculos de Níveis de Serviços com Desvio de Qualidade”, serão aplicados os percentuais de glosa;

16.5- A apuração dos indicadores será calculada sempre com base na data e hora de registro inicial da demanda e no horário de funcionamento de cada serviço. No cálculo destes indicadores, serão desconsiderados os períodos em que as demandas estiveram suspensas ou não estiveram sob responsabilidade da CONTRATADA. Para tanto, a suspensão e a transferência de demandas deverão observar estritamente as condições e os procedimentos estabelecidos pela equipe técnica do CONTRATANTE.

16.6- A frequência de aferição e avaliação dos níveis de serviço será mensal, devendo a CONTRATADA elaborar relatório gerencial de serviços, apresentando-o ao CONTRATANTE até o 5º (quinto) dia útil do mês subsequente ao da prestação do serviço. Devem constar nesse relatório, entre outras informações, as metas de níveis de serviço alcançadas com a devida justificativa pelo não atendimento da meta exigida, se for o

caso; recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual.

17. **DO PAGAMENTO**

17.1- Licenças - A CONTRATADA estará autorizada a emitir sua nota fiscal de cobrança após a entrega dos itens contratados pela CONTRATANTE. Junto a nota fiscal além das documentações solicitados no edital a CONTRATADA deverá anexar uma carta de aceite dos itens contratados, que deve ser assinada por pelo menos 2 (dois) fiscais nomeados do contrato.

Serviço - O pagamento se dará de acordo com o cronograma de execução das OSs abertas pelo CONTRATANTE. Deverá ser anexada junto a nota fiscal uma cópia da OS referente a nota fiscal, assim como carta de aceite assinada por no mínimo 2 fiscais do contrato.

18. DA GESTÃO DOS CONTRATOS

18.1- A gestão de todos os contratos oriundos de adesão a esta Ata, realizados por Órgãos da Administração direta e indireta do Estado do Rio de Janeiro, terá como gestor o PRODERJ e o Órgão Participante.

18.2- Em qualquer tempo da vigência do contrato os gestores poderão solicitar mais informações que considerem relevantes ao trabalho de gestão e governança dos contratos oriundos desta Ata.

18.3- O Órgão Aderente deverá enviar mensalmente ao PRODERJ relatório da solução adquirida informando:

18.3.1- Quantidade de estações de trabalho, dispositivos móveis e servidores em uso, indicando:

a) Sistema operacional;
b) Nome da máquina;
c) Usuário;
d) Local onde está instalado; e
e) Indicar se o *endpoint* está instalado e atualizado.

18.4- O órgão usuário do objeto contratado deverá nomear uma comissão de fiscalização do contrato, que será responsável por atestar o pagamento das faturas mediante a conferência de que a CONTRATADA atendeu todos os requisitos deste projeto básico.

18.5- O órgão usuário do objeto contratado deverá designar equipe técnica responsável pela gestão da solução.

18.6- Durante a execução dos serviços a CONTRATADA deverá seguir as melhoras práticas preconizadas no PMBOK, ITIL e Cobit.

19. DA COTAÇÃO

19.1- As PROPONETES deverão fazer sua cotação somando o valor total de licenciamento com o valor total de USTs solicitadas.

19.2- Será considerada a melhor proposta a que alcançar o menor valor global na soma desses dois itens.

19.3- Por se tratar de uma Ata de Registro de Preços com foco especifico em uma tecnologia, amplamente utilizada no Estado, optou-se pela não separação em lotes dos itens, visto a estreita relação existente entre o fornecimento das licenças e os serviços disponibilizados nesta Ata.

- **********