CONTRATO Nº 020/2019

CONTRATO DE LICENCIAMENTO DE ANTIVÍRUS CORPORATIVO, NA VERSÃO DE PLATAFORMA MICROSOFT WINDOWS E GNU/LINUX E SERVIÇOS CORRELATOS QUE ENTRE SI CELEBRAM A CÂMARA MUNICIPAL DE RIO BRANCO - ACRE E A EMPRESA ESYWORLD SISTEMAS E INFORMÁTICA LTDA - EPP.

A CÂMARA MUNICIPAL DE RIO BRANCO - ACRE, inscrita no CNPJ/MF sob o nº. 04.035.143/0001-90, com sede na Rua 24 de Janeiro, n.º 53 – Bairro Seis de Agosto - Rio Branco - Acre, neste ato representado por seu Presidente, Vereador **Antônio Lira de Morais**, brasileiro, portador do [redacted], residente e domiciliado nesta Cidade e pelo seu Primeiro Secretário, Vereador **Railson Correia da Costa**, brasileiro, portador do [redacted], residente e domiciliado nesta Cidade, doravante denominado simplesmente **CONTRATANTE** e, de outro lado, a empresa **ESYWORLD SISTEMAS E INFORMÁTICA LTDA - EPP,** inscrita no CNPJ sob nº. 03.899.222/0001-86, com sede Rua Geraldo Flausino Gomes, Conj. 13, 153 e 154, Cidade Monções, São Paulo/SP - CEP: 04575-060, neste ato representada pelo **BINJAMIN HANOCH**, portador da cédula de identidade [redacted] e inscrito no [redacted], denominada simplesmente **CONTRATADA**, tendo em vista a solicitação/PBS nº 03/2019 da Coordenadoria de Tecnologia da Informação desta Casa Legislativa, Processo de Dispensa de Licitação nº 17654/2019, Parecer Jurídico nº 194/2019, e de conformidade com a Lei Federal nº 8.666/93, notadamente seu **artigo 24, II**, resolvem celebrar entre si o presente termo de contrato, mediante o estabelecimento das seguintes cláusulas:

CLÁUSULA PRIMEIRA: OBJETO DO CONTRATO

Fornecimento de solução de antivírus corporativo, na versão de plataforma Microsoft Windows e GNU/Linux, provendo proteção para estações de trabalho, notebooks e servidores (nos quantitativos e especificações contidas no Anexo Único); com subscrição de 02 (dois) anos, sendo renovável por igual período.

CLÁUSULA SEGUNDA: PREÇO E PAGAMENTO

2.1. O valor do presente contrato será de **R$ 7.482,00** (sete mil, quatrocentos e oitenta e dois reais), já incluídos todos os impostos, taxas e demais despesas, tais como frete, embalagens, seguro, garantia e quaisquer outras que sejam pertinentes.

2.2. O pagamento será efetuado até o 5º (quinto) dia útil após a apresentação da nota fiscal devidamente atestada por servidor responsável e das certidões de regularidade fiscal.

2.3. Não haverá sob nenhuma hipótese, pagamento antecipado.

CLÁUSULA TERCEIRA: ESPECIFICAÇÕES DO OBJETO

3.1. A CONTRATADA deverá possuir registro de parceria técnica comercial com o Fabricante da solução, comprovada através de carta de autorização de fornecimento expedida pelo fabricante ou indicado em URL oficial do fabricante da solução ofertada.

3.2. A CONTRATADA deverá utilizar os produtos legados de software - sistemas operacionais de servidores e estações de trabalho, suites office, etc disponibilizados pela CONTRATANTE, quando aplicáveis, objetivando redução de impacto e investimento para a implantação.

3.3. Detalhamento técnicos dos produtos, conforme Anexo Único.

CLÁUSULA QUARTA: DA ENTREGA E DO RECEBIMENTO DO OBJETO

4.1. - A CONTRATADA deverá efetuar a entrega dos produtos ao CONTRATANTE em até 7 (sete) dias úteis, após o recebimento da ordem de compra. A entrega será feita por e-mail ao responsável de TI da Câmara Municipal de Rio Branco - CMRB.

4.2. A entrega será feita por e-mail ao responsável de TI da Câmara Municipal de Rio Branco - CMRB.

4.3. Caso se verifique que o material entregue possui características diferentes do que foi proposto pela CONTRATADA, e estas não possam ser supridas, será determinada a rescisão do contrato ou nova realização de entrega, que deverá ocorrer nos prazos máximos contidos no termo de referência contados da notificação, sendo que os custos correrão por conta da CONTRATADA.

CLAUSULA QUINTA - DA GARANTIA DO OBJETO

5.1. Os prazos de vigência da garantia dos serviços será:

a. 24 (vinte e quatro) meses para as licenças;

CLÁUSULA SEXTA: RESPONSABILIDADE DAS PARTES

6.1 Constituem obrigações da CONTRATANTE:

a. Efetuar o pagamento ajustado;

b. Viabilizar, por todos os meios ao seu alcance, para que a CONTRATADA possa executar as obrigações decorrentes deste contrato, que lhe são afetas;

c. Comunicar à CONTRATADA qualquer irregularidade na execução das cláusulas do presente contrato, para que a mesma possa saná-la.

d. Disponibilizar profissional responsável remotamente para acompanhar a execução das atividades, conforme solicitação de alocação pela coordenação do trabalho;.

CLÁUSULA SÉTIMA - DA VIGÊNCIA DO CONTRATO

7.1. O presente contrato terá vigência de 24 (vinte e quatro) meses, a contar de sua assinatura, podendo ser prorrogável até o prazo de 48 meses, na forma do art. 57, IV, da Lei nº 8.666/93.

CLÁUSULA OITAVA: DOTAÇÃO ORÇAMENTÁRIA

8.1 As despesas decorrentes deste contrato serão atendidas pelas seguintes dotações orçamentárias:

- **Programa de Trabalho**: 001.031.2001.0000
- **Aplicação Programada**: Administração da Câmara Municipal de Rio Branco
- **Fonte**: 1
- **Natureza da Despesa**: 3.3.90.39.00

CLÁUSULA NONA: RESCISÃO CONTRATUAL

9.1 Poderá ocorrer pelas causas e na forma previstas nos artigos 77, 78 e 79 da Lei Federal nº 8.666/93.

9.2 O descumprimento das obrigações assumidas neste contrato deverá ser objeto de comunicação escrita, tendo a parte inadimplente o, prazo de cinco (05) dias para alegar o que entender de direito.

CLÁUSULA DÉCIMA: DOS ACRESCIMOS E DAS SUPRESSÕES

10.1 A CONTRATADA se obriga a aceitar os acréscimos ou supressões até o limite de 25% (vinte e cinco por cento) do valor atualizado do presente Contrato.

CLÁUSULA DÉCIMA PRIMEIRA: TRANSFERÊNCIA DO CONTRATO

11.1 A CONTRATADA não poderá transferir o presente contrato, no todo ou em parte, sem o expresso consentimento da CONTRATANTE, dado por escrito, sob pena de rescisão deste contrato.

CLÁUSULA DÉCIMA SEGUNDA: CASOS OMISSOS

12.1 Os casos omissos, oriundos do presente contrato, serão resolvidos à luz da Lei Federal nº 8.666/93 e alterações posteriores, e dos princípios gerais do direito.

CLÁUSULA DÉCIMA TERCEIRA: SANÇÕES ADMINISTRATIVAS PARA O CASO DE RESCISÃO CONTRATUAL

13.1. Pela inexecução total ou parcial do presente contrato, a CONTRATANTE poderá, garantida a prévia defesa, aplicar a CONTRATADA, as sanções previstas nos artigos 86 e 87 da Lei Federal nº 8.666/93, sendo que, caso a CONTRATANTE resolva aplicar multas ao CONTRATADO, estas observarão os seguintes critérios:

I - multa de 0,2% (zero vírgula dois por cento) por dia de atraso e por ocorrência de fato em desacordo com o estabelecido neste contrato, até o máximo de 10% (dez por cento) sobre o valor total do contrato;

II - multa de 10% (dez por cento) sobre o valor total deste contrato, no caso de inexecução total ou parcial do objeto contratado.

13.2. A imposição de qualquer penalidade não exime a CONTRATADA do cumprimento de suas obrigações, nem de promover as medidas necessárias para reparar ou ressarcir eventuais danos causados à CONTRATANTE.

CLÁUSULA DÉCIMA QUARTA: DO FORO

As partes elegem, de comum acordo, o Foro da Comarca de Rio Branco - Estado do Acre para dirimir eventuais controvérsias emergentes da aplicação deste contrato.

E, por estarem ajustados, assinam o presente instrumento em três (03) vias de igual teor e forma.

Rio Branco-Acre, 24 de junho de 2019.

CONTRATANTE:

ANTONIO LIRA DE MORAIS:[redacted]
Assinado de forma digital por ANTONIO LIRA DE MORAIS:[redacted]
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora Raiz Brasileira v2, ou=AC SOLUTI, ou=AC SOLUTI Multipla, ou=Certificado PF A3, cn=ANTONIO LIRA DE MORAIS:[redacted]
Dados: 2019.06.24 12:28:17 -05'00'

ANTÔNIO LIRA DE MORAIS
Presidente - CMRB

RAILSON CORREIA DA COSTA:[redacted]
Assinado de forma digital por RAILSON CORREIA DA COSTA:[redacted]
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora Raiz Brasileira v2, ou=AC SOLUTI, ou=AC SOLUTI Multipla, ou=Certificado PF A3, cn=RAILSON CORREIA DA COSTA:[redacted]
Dados: 2019.06.24 14:11:27 -05'00'

RAILSON CORREIA
1º Secretario - CMRB

CONTRATADA:

ESYWORLD SISTEMAS E INFORMÁTICA LTDA - EPP
CNPJ 03.899.222/0001-86
Representante: BINJAMIN HANOCH
[redacted]

ANEXO ÚNICO

QUANTITATIVO E ESPECIFICAÇÃO DOS SERVIÇOS

Item	Descrição	Quantidade	
		Unidade	Pedida
01	Contratação de pessoa jurídica para fornecimento de solução de ANTIVÍRUS Corporativo, na versão de plataforma Microsoft Windows e GNU/Linux, provendo proteção para estações de trabalho, notebooks e servidores; com subscrição de 02 anos, sendo renovável por igual período.	Unidade	100

1. Servidor de Administração e Console Administrativa
1.1.Compatibilidade:
1.1.1.Microsoft Windows Server 2003 SP2 (Todas edições);
1.1.2. Microsoft Windows Server 2003 x64 SP2 (Todas edições);
1.1.3. Microsoft Windows Server 2008 (Todas edições);
1.1.4.Microsoft Windows Server 2008 x64 SP1 (Todas edições);
1.1.5.Microsoft Windows Server 2008 R2 (Todas edições);
1.1.6.Microsoft Windows Server 2012 (Todas edições);
1.1.7.Microsoft Windows Server 2012 R2 (Todas edições);
1.1.8.Microsoft Windows Small Business Server 2003 SP2 (Todas edições);
1.1.9.Microsoft Windows Small Business Server 2008 (Todas edições);
1.1.10. Microsoft Windows Small Business Server 2011 (Todas edições);
1.1.11. Microsoft Windows XP Professional SP2 ou superior;
1.1.12. Microsoft Windows XP Professional x64 SP2 ou superior;
1.1.13. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
1.1.14. Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;
1.1.15. Microsoft Windows 7 Professional / Enterprise / Ultimate;
1.1.16. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
1.1.17. Microsoft Windows 8 Professional / Enterprise;
1.1.18. Microsoft Windows 8 Professional / Enterprise x64;
1.1.19. Microsoft Windows 8.1 Professional / Enterprise;
1.1.20. Microsoft Windows 8.1 Professional / Enterprise x64.
1.1.21. Microsoft Windows 10 Professional / Enterprise / Education x64
1.2. Suporta as seguintes plataformas virtuais:
1.2.1. VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0;
1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

1.2.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
1.2.4. Microsoft VirtualPC 6.0.156.0;
1.2.5. Parallels Desktop 7 e superior;
1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
1.2.7. Citrix XenServer 6.1, 6.2.
1.3. Características:
1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. Console deve ser baseada no modelo cliente/servidor;
1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.3.5. 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;
1.3.6.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;
1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.3.8. 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;
1.3.9.Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.3.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.3.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
1.3.13. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
1.3.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.3.15. 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;
1.3.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
1.3.17. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
1.3.18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.3.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.3.20. 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;

1.3.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.3.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.3.23. 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.
1.3.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.3.25. 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;
1.3.26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.3.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
1.3.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
1.3.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
1.3.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
1.3.31. Deve fornecer as seguintes informações dos computadores:
1.3.31.1. Se o antivírus está instalado;
1.3.31.2. Se o antivírus está iniciado;
1.3.31.3. Se o antivírus está atualizado;
1.3.31.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.3.31.5. Minutos/horas desde a última atualização de vacinas;
1.3.31.6. Data e horário da última verificação executada na máquina;
1.3.31.7. Versão do antivírus instalado na máquina;
1.3.31.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.3.31.9. Data e horário de quando a máquina foi ligada;
1.3.31.10. Quantidade de vírus encontrados (contador) na máquina;
1.3.31.11. Nome do computador;
1.3.31.12. Domínio ou grupo de trabalho do computador;
1.3.31.13. Data e horário da última atualização de vacinas;

1.3.31.14. Sistema operacional com Service Pack;
1.3.31.15. Quantidade de processadores;
1.3.31.16. Quantidade de memória RAM;
1.3.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.3.31.18. Endereço IP;
1.3.31.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.3.31.20. Atualizações do Windows Updates instaladas;
1.3.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.3.31.22. Vulnerabilidades de aplicativos instalados na máquina;
1.3.32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.3.33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.3.33.1. Alteração de Gateway Padrão;
1.3.33.2. Alteração de subrede;
1.3.33.3. Alteração de domínio;
1.3.33.4. Alteração de servidor DHCP;
1.3.33.5. Alteração de servidor DNS;
1.3.33.6. Alteração de servidor WINS;
1.3.33.7. Alteração de subrede;
1.3.33.8. Resolução de Nome;
1.3.33.9. Disponibilidade de endereço de conexão SSL;
1.3.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.3.35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.3.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.3.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.3.38. 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 atualizarse e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.3.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.3.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.3.41. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.3.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

1.3.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.3.44. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
1.3.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
1.3.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
1.3.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.3.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.3.49. 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.
1.3.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.3.51. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
2. Estações Windows
2.1. Compatibilidade:
2.1.1. Microsoft Windows Embedded 8.0 Standard x64;
2.1.2.Microsoft Windows Embedded 8.1 Industry Pro x64;
2.1.3.Microsoft Windows Embedded Standard 7* x86 / x64 SP1;
2.1.4.Microsoft Windows Embedded POSReady 7* x86 / x64;
2.1.5.Microsoft Windows XP Professional x86 SP3 e superior;
2.1.6. Microsoft Windows Vista x86 / x64SP2 e posterior;
2.1.7.Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
2.1.8. Microsoft Windows 8 Professional/Enterprise x86 / x64;
2.1.9.Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
2.1.10. Microsoft Windows 10 Pro / Enterprise x86 / x64.
2.2. Características:
2.2.1. Deve prover as seguintes proteções:
2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
2.2.1.5. O Endpoint deve possuir opção para rastreamento por linha de

comando, parametrizável, com opção de limpeza;
2.2.1.6. Firewall com IDS;
2.2.1.7. Autoproteção (contra-ataques aos serviços/processos do antivírus);
2.2.1.8. Controle de dispositivos externos;
2.2.1.9. Controle de acesso a sites por categoria;
2.2.1.10. Controle de acesso a sites por horário;
2.2.1.11. Controle de acesso a sites por usuários;
2.2.1.12. Controle de execução de aplicativos;
2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2.2.2.Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
2.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
2.2.5.Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
2.2.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
2.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
2.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.2.9.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 tomar a partir da extensão do arquivo;
2.2.10. Capacidade de verificar somente arquivos novos e alterados;
2.2.11. Capacidade de verificar objetos usando heurística;
2.2.12. Capacidade de agendar uma pausa na verificação;
2.2.13. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
2.2.14. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
2.2.15. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
2.2.15.1. Perguntar o que fazer, ou;
2.2.15.2. Bloquear acesso ao objeto;
2.2.15.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.15.2.2. Caso positivo de desinfecção:
2.2.15.2.2.1. Restaurar o objeto para uso;
2.2.15.2.3. Caso negativo de desinfecção:
2.2.15.2.3.1. Mover para quarentena ou apagar (de acordo com a

configuração pré-estabelecida pelo administrador);
2.2.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
2.2.17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
2.2.18. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
2.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
2.2.22.
2.2.23. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
2.2.23.1. Perguntar o que fazer, ou;
2.2.23.2. Bloquear o e-mail;
2.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.23.2.2. Caso positivo de desinfecção:
2.2.23.2.2.1. Restaurar o e-mail para o usuário;
2.2.23.2.3. Caso negativo de desinfecção:
2.2.23.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.24. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
2.2.25. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
2.2.26. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
2.2.27. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
2.2.28. Deve ter suporte total ao protocolo IPv6;
2.2.29. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
2.2.30. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
2.2.30.1. Perguntar o que fazer, ou;
2.2.30.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
2.2.30.3. Permitir acesso ao objeto;
2.2.31. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.2.31.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2.2.31.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
2.2.32. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
2.2.33. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências

características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
2.2.34. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
2.2.35. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
2.2.36. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
2.2.37. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
2.2.38. 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;
2.2.39. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.2.39.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.2.39.2. 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.
2.2.40. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
2.2.40.1. Discos de armazenamento locais;
2.2.40.2. Armazenamento removível;
2.2.40.3. Impressoras;
2.2.40.4. CD/DVD;
2.2.40.5. Drives de disquete;
2.2.40.6. Modems;
2.2.40.7. Dispositivos de fita;
2.2.40.8. Dispositivos multifuncionais;
2.2.40.9. Leitores de smart card;
2.2.40.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
2.2.40.11. Wi-Fi;
2.2.40.12. Adaptadores de rede externos;
2.2.40.13. Dispositivos MP3 ou smartphones;
2.2.40.14. Dispositivos Bluetooth;
2.2.40.15. Câmeras e Scanners.
2.2.41. 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;
2.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
2.2.43. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
2.2.45. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;
2.2.46. 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);
2.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
2.2.49. 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;
2.2.50. 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.
3. Estações Mac OS X
3.1. Compatibilidade:
3.2.Mac OS X 10.11 (El Capitan);
3.3.Mac OS X 10.10 (Yosemite);
3.4.Mac OS X 10.9 (Mavericks).
3.5.Mac OS X 10.8 (Mountain Lion)
3.6.Mac OS X 10.7 (Lion)
3.7. Características:
3.7.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.7.2.Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.7.3.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;
3.7.4. Deve possuir suportes a notificações utilizando o Growl;
3.7.5. 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);
3.7.6. Capacidade de voltar para a base de dados de vacina anterior;
3.7.7.Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
3.7.8.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;
3.7.9.Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.7.10. 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;
3.7.11. Capacidade de verificar somente arquivos novos e alterados;
3.7.12. Capacidade de verificar objetos usando heurística;
3.7.13. Capacidade de agendar uma pausa na verificação;
3.7.14. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.7.14.1. Perguntar o que fazer, ou;
3.7.14.2. Bloquear acesso ao objeto;
3.7.14.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.7.14.2.2. Caso positivo de desinfecção:
3.7.14.2.2.1. Restaurar o objeto para uso;
3.7.14.2.3. Caso negativo de desinfecção:
3.7.14.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
3.7.15. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.7.16. Capacidade de verificar arquivos de formato de email;
3.7.17. 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;
3.7.18. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
4. Estações de trabalho Linux
4.1. Compatibilidade:
4.1.1. Plataforma 32-bits:
4.1.1.1. Canaima 3;
4.1.1.2. Red Flag Desktop 6.0 SP2;
4.1.1.3. Red Hat Enterprise Linux 5.8 Desktop;
4.1.1.4. Red Hat Enterprise Linux 6.2 Desktop;
4.1.1.5. Fedora 16;
4.1.1.6. CentOS-6.2;
4.1.1.7. SUSE Linux Enterprise Desktop 10 SP4;
4.1.1.8. SUSE Linux Enterprise Desktop 11 SP2;
4.1.1.9. openSUSE Linux 12.1;
4.1.1.10. openSUSE Linux 12.2;
4.1.1.11. Debian GNU/Linux 6.0.5;
4.1.1.12. Mandriva Linux 2011;
4.1.1.13. Ubuntu 10.04 LTS;
4.1.1.14. Ubuntu 12.04 LTS.
4.1.2. Plataforma 64-bits:
4.1.2.1. Canaima 3;
4.1.2.2. Red Flag Desktop 6.0 SP2;
4.1.2.3. Red Hat Enterprise Linux 5.8;
4.1.2.4. Red Hat Enterprise Linux 6.2 Desktop;
4.1.2.5. Fedora 16;

4.1.2.6. CentOS-6.2;
4.1.2.7. SUSE Linux Enterprise Desktop 10 SP4;
4.1.2.8. SUSE Linux Enterprise Desktop 11 SP2;
4.1.2.9. openSUSE Linux 12.1;
4.1.2.10. openSUSE Linux 12.2;
4.1.2.11. Debian GNU/Linux 6.0.5;
4.1.2.12. Ubuntu 10.04 LTS;
4.1.2.13. Ubuntu 12.04 LTS.
4.2. Características:
4.2.1. Deve prover as seguintes proteções:
4.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4.2.2.Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
4.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.2.2.2. 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;
4.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
4.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
4.2.5. 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;
4.2.6. Capacidade de verificar objetos usando heurística;
4.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
4.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
4.2.9.Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
5. Servidores Windows
5.1. Compatibilidade:
5.2. Plataforma 32-bits:
5.2.1.Microsoft Windows Server 2003 Standard / Enterprise (SP2);
5.2.2.Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);

5.2.3.Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.2.4.Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
5.3.Plataforma 64-bits:
5.3.1.Microsoft Windows Server 2003 Standard / Enterprise (SP2);
5.3.2.Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
5.3.3.Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.3.4.Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
5.3.5.Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.3.6.Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
5.3.7.Microsoft Windows Storage Server 2008 R2;
5.3.8.Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
5.3.9.Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
5.3.10. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
5.3.11. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
5.3.12. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
5.3.13. Microsoft Windows Storage Server 2012 (Todas edições);
5.3.14. Microsoft Windows Storage Server 2012 R2 (Todas edições);
5.3.15. Microsoft Windows Hyper-V Server 2012;
5.3.16. Microsoft Windows Hyper-V Server 2012 R2.
5.4. Características:
5.4.1. Deve prover as seguintes proteções:
5.4.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
5.4.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.4.1.3. Firewall com IDS;
5.4.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.4.2.Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.4.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.4.4.Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.4.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.4.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.4.4.3. Leitura de configurações;
5.4.4.4. Modificação de configurações;
5.4.4.5. Gerenciamento de Backup e Quarentena;

5.4.4.6. Visualização de relatórios;
5.4.4.7. Gerenciamento de relatórios;
5.4.4.8. Gerenciamento de chaves de licença;
5.4.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.4.5.O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.4.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.4.5.2. 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.
5.4.6.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;
5.4.7.Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.4.8.Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
5.4.9.Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.4.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.4.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.4.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.4.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.4.14. 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;
5.4.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.4.16. 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;
5.4.17. Capacidade de verificar somente arquivos novos e alterados;
5.4.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.4.19. Capacidade de verificar objetos usando heurística;
5.4.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.4.21. Capacidade de agendar uma pausa na verificação;
5.4.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for

iniciado;
5.4.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.4.23.1. Perguntar o que fazer, ou;
5.4.23.2. Bloquear acesso ao objeto;
5.4.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.4.23.2.2. Caso positivo de desinfecção:
5.4.23.2.2.1. Restaurar o objeto para uso;
5.4.23.2.3. Caso negativo de desinfecção:
5.4.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.4.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.4.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.4.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.4.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
6. Servidores Linux
6.1. Compatibilidade:
Plataforma 32-bits:
6.1.1.Red Hat Enterprise Linux Server 5.x;
6.1.2.Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
6.1.3.CentOS 6.x (6.0 - 6.6);
6.1.4.SUSE® Linux Enterprise Server 11 SP3;
6.1.5.Ubuntu Server 12.04 LTS;
6.1.6.Ubuntu Server 14.04 LTS;
6.1.7.Ubuntu Server 14.10;
6.1.8.Oracle Linux 6.5;
6.1.9.Debian GNU/Linux 7.5, 7.6, 7.7;
6.1.10. openSUSE 13.1.
6.1.11. Plataforma 64-bits:
6.1.12. Red Hat Enterprise Linux Server 5.x;
6.1.13. Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
6.1.14. Red Hat Enterprise Linux Server 7;
6.1.15. CentOS-6.x (6.0 - 6.6);
6.1.16. CentOS-7.0;
6.1.17. SUSE Linux Enterprise Server 11 SP3;
6.1.18. SUSE Linux Enterprise Server 12;
6.1.19. Novell Open Enterprise Server 11 SP1;
6.1.20. Novell Open Enterprise Server 11 SP2;
6.1.21. Ubuntu Server 12.04 LTS;
6.1.22. Ubuntu Server 14.04 LTS;
6.1.23. Ubuntu Server 14.10;
6.1.24. Oracle Linux 6.5;
6.1.25. Oracle Linux 7.0;

6.1.26. Debian GNU/Linux 7.5, 7.6, 7.7;
6.1.27. openSUSE® 13.1.
6.1.28.
6.2. Características:
6.2.1. Deve prover as seguintes proteções:
6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, antimalware, 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).
8. Smartphones e tablets
8.1. Compatibilidade:
8.1.1. Apple iOS 7.0 – 8.X;
8.1.2.Windows Phone 8.1;
8.1.3.Android OS 2.3 – 5.1.
8.2.Características:
8.2.1.Deve prover as seguintes proteções:
8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
8.2.1.1.1. 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;
8.2.1.1.2. Arquivos abertos no smartphone;
8.2.1.1.3. Programas instalados usando a interface do smartphone
8.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
8.2.2. Deverá isolar em área de quarentena os arquivos infectados;
8.2.3. Deverá atualizar as bases de vacinas de modo agendado;
8.2.4. Deverá bloquear spams de SMS através de Black lists;
8.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
8.2.6.Capacidade de desativar por política:
Wi-fi;
Câmera;
Bluetooth.
8.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
8.2.8.Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
8.2.9.
8.2.10. Deverá ter firewall pessoal (Android);
8.2.11. Capacidade de tirar fotos quando a senha for inserida incorretamente;
8.2.12. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
8.2.13. Capacidade de enviar comandos remotamente de:
 Localizar;
 Bloquear.
8.2.14. Capacidade de detectar Jailbreak em dispositivos iOS;
8.2.15. Capacidade de bloquear o acesso a site por categoria em dispositivos;
8.2.16. Capacidade de bloquear o acesso a sites phishing ou malicioso;
8.2.17. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
8.2.18. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
8.2.19. Capacidade de configurar White e blacklist de aplicativos;
8.2.20. Capacidade de localizar o dispositivo quando necessário;
8.2.21. Permitir atualização das definições quando estiver em “roaming”;
8.2.22. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
8.2.23. Capacidade de enviar URL de instalação por e-mail;
8.2.24. Capacidade de fazer a instalação através de um link QRCode;
8.2.25. Capacidade de executar as seguintes ações caso a desinfecção falhe:
 Deletar;
 Ignorar;
 Quarentenar;
 Perguntar ao usuário.
9. Gerenciamento de dispositivos móveis (MDM)
9.1. Compatibilidade:

9.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync:
9.1.1.1. Apple iOS;
9.1.1.2. Windows Phone;
9.1.1.3. Android.
9.1.2. Dispositivos com suporte ao Apple Push Notification (APNs).
9.1.2.1. Apple iOS 3.0 ou superior.
9.2. Características:
9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
9.2.2. Capacidade de ajustar as configurações de:
9.2.2.1. Sincronização de e-mail;
9.2.2.2. Uso de aplicativos;
9.2.2.3. Senha do usuário;
9.2.2.4. Criptografia de dados;
9.2.2.5. Conexão de mídia removível.
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS.