

Estudo Técnico Preliminar 21/2024

1. Informações Básicas

Número do processo: 23479.001447/2024-61

2. Descrição da necessidade

Em um mundo cada vez mais digital, a segurança cibernética se torna um pilar fundamental para a proteção de dados e sistemas de qualquer organização. As Soluções de *Endpoint* assumem um papel crucial nesse cenário, atuando como uma linha de defesa essencial contra as diversas ameaças que surgem constantemente.

Os ataques cibernéticos, também conhecidos como *Cyber Attacks*, representam um dos maiores desafios de segurança da atualidade, impactando significativamente as organizações. O aumento exponencial das violações de dados ao longo dos anos evidencia a necessidade de medidas robustas para proteção dos sistemas e informações.

As Soluções de *Endpoint* são ferramentas essenciais para a segurança cibernética de qualquer organização, oferecendo proteção abrangente contra diversas ameaças, gerenciamento eficiente da segurança, detecção e resposta rápida a incidentes, além de diversos outros benefícios.

O design das soluções de *Endpoint* presentes no mercado exige a comunicação constante do software com o banco de dados da empresa fabricante. Essa comunicação, viabilizada pelas licenças, garante a atualização contínua das proteções contra as novas ameaças que surgem diariamente.

A indisponibilidade do software antivírus pode ocasionar graves impactos, como:

- **Interrupção do funcionamento das estações de trabalho:** Sem a proteção adequada, os computadores ficam vulneráveis a ataques cibernéticos, podendo comprometer a produtividade e o funcionamento da instituição.
- **Perda de dados confidenciais:** Ataques de *ransomware*, por exemplo, podem criptografar dados importantes, causando perdas financeiras e danos à reputação da instituição.
- **Prejuízos à imagem e reputação da instituição:** A falha na proteção dos dados pode gerar perda de confiança por parte dos usuários e stakeholders, impactando negativamente a imagem da instituição.

A presente contratação é crucial para garantir a segurança cibernética da instituição, protegendo seus sistemas e informações contra as mais recentes ameaças. A indisponibilidade da Solução pode ter consequências graves, comprometendo o funcionamento da instituição, causando perdas financeiras e danos à sua imagem.

3. Área requisitante

Área Requisitante	Responsável
Divisão de Redes e Serviços de Internet	JORDELSON SANTIAGO MACIEL

4. Necessidades de Negócio

4.1. A solução a ser contratada precisa necessariamente dar continuidade à solução atualmente em uso de maneira efetiva, apresentando os mesmos requisitos funcionais e demais requisitos presentes na Tabela 1 (descrição detalhada).

Requisito 1: Proteção contra malware e ransomware: A solução deve ser capaz de detectar, prevenir e bloquear malwares e *ransomwares* conhecidos e emergentes.

Requisito 2: Detecção e prevenção de intrusões: A solução deve ser capaz de detectar e prevenir acessos não autorizados, tentativas de invasão e outras atividades maliciosas.

Requisito 3: Gerenciamento de identidade e acesso (IAM): A solução deve fornecer controles robustos de IAM para garantir que apenas usuários autorizados tenham acesso aos endpoints.

Requisito 4: Criptografia de dados: A solução deve criptografar os dados em repouso e em trânsito para proteger contra acesso não autorizado

Requisito 5: Visibilidade centralizada: A solução deve fornecer uma visão centralizada de todos os endpoints da organização, incluindo seu estado de segurança, conformidade e desempenho.

Requisito 6: Gerenciamento remoto: A solução deve permitir que os administradores gerenciem endpoints remotamente, incluindo a instalação de software, a aplicação de patches e a configuração de políticas de segurança.

Requisito 7: Automação: A solução deve ser capaz de automatizar tarefas repetitivas, como varreduras de malware e aplicação de patches, para reduzir a carga de trabalho da equipe de TI.

Requisito 8: Relato e conformidade: A solução deve gerar relatórios detalhados sobre a postura de segurança da organização, que podem ser usados para demonstrar conformidade com os regulamentos

Requisito 9: Impacto mínimo no desempenho: A solução deve ter um impacto mínimo no desempenho dos endpoints, para evitar lentidão ou interrupções.

Requisito 10: Escalabilidade: A solução deve ser escalável para atender às necessidades de uma organização em crescimento.

Requisito 11: Alta disponibilidade: A solução deve estar sempre disponível para proteger os endpoints contra ameaças.

Requisito 12: Interface amigável: A solução deve ter uma interface amigável que seja fácil de usar para administradores de todos os níveis de experiência.

Requisito 13: Suporte multiplataforma: A solução deve suportar vários sistemas operacionais, como Windows, macOS e Linux.

Requisito 14: Integração com outras ferramentas de segurança: A solução deve se integrar com outras ferramentas de segurança existentes, como firewalls e sistemas de detecção de intrusão.

Requisito 15: Continuidade e padronização. A solução a ser contratada precisa necessariamente dar continuidade à solução atualmente em uso de maneira efetiva, apresentando os mesmos requisitos funcionais e demais requisitos presentes na Tabela 1 (descrição detalhada).

5. Necessidades Tecnológicas

Requisito 1: Sistemas operacionais suportados: A solução deve ser compatível com as estações de trabalho e servidores com arquitetura de hardware 32 bits e 64 bits, nas Plataformas Microsoft Windows/ Mac/ Linux.

Requisito 2: Agentes de endpoint: A solução deve incluir agentes de endpoint que podem ser instalados em cada endpoint para fornecer proteção e gerenciamento.

Requisito 3: Console de gerenciamento: A solução deve incluir um console de gerenciamento centralizado que permite aos administradores gerenciar endpoints, aplicar políticas de segurança e monitorar a postura de segurança da organização.

Requisito 4: Atualizações de segurança: A solução deve ser atualizada regularmente com as últimas definições de vírus e malware para garantir que seus endpoints estejam protegidos contra as últimas ameaças.

Requisito 5: Proteção contra ransomware: A solução deve incluir proteção contra ransomware.

Requisito 6: Detecção e resposta a endpoints (EDR): A solução deve incluir recursos de EDR para detectar e responder a ataques em andamento em seus endpoints.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Os serviços de garantia e de manutenção e suporte deverão ser capazes de assegurar o funcionamento da solução de segurança contratada, com todas as suas funcionalidades, durante toda a vigência do contrato, com suporte e manutenção corretiva sob demanda.

7. Estimativa da demanda - quantidade de bens e serviços

As quantidades levantadas se justificam pois a instituição possui essa quantidade de licenças aplicadas em seu servidor, e precisa renovar esse quantitativo além de vislumbrar o eventual crescimento de seu parque de computadores.

Item	Bem / Serviço	CATSER	Quantidade	Unidade
1	Renovação de licenças da solução de segurança para dispositivos fins Kaspersky EndPoint Security for Business Advanced, por um período de 36 (trinta e seis) meses, incluindo suporte.	27502	1000	Licenças

8. Levantamento de soluções

Solução 1: Renovação e ampliação da solução Atual (Kaspersky EndPoint Security for Business Advanced).

Solução 2: Contratar solução equivalente de outros desenvolvedores.

Para analisar as soluções de TIC, os órgãos de governo tem utilizado o Quadrante Mágico da Gartner para tomada de decisão na escolha da solução. O relatório posiciona *vendors* com base em sua "Compleitude de Visão" e "Capacidade de Execução".

Embora o relatório de 2024 ainda não tenha sido divulgado (previsão para agosto), aqui estão alguns destaques da versão 2023 ara Plataformas de Proteção de Endpoints:

Líderes:

- **CrowdStrike:** Líder pelo quarto ano consecutivo, reconhecida por sua inovação e eficácia.
- **Microsoft:** Forte oferta baseada em nuvem com integração nativa com outros serviços Microsoft.
- **SentinelOne:** Solução avançada com foco em prevenção e detecção de ameaças.
- **Trend Micro:** Fornecedor experiente com ampla gama de recursos de segurança.
- **McAfee:** Solução consolidada com foco em proteção multicamadas.
- **Sophos:** Opção popular com forte relação custo-benefício.

Visionários:

- **Cisco:** Oferece segurança integrada com soluções de rede.
- **Palo Alto Networks:** Conhecido por sua tecnologia de prevenção de intrusão.
- **McAfee Enterprise:** Foco em grandes empresas com opções de gerenciamento centralizado.
- **VMware Carbon Black:** Solução avançada com recursos de detecção e resposta estendidos (XDR).

Challengers:

- **Bitdefender:** Oferece opções acessíveis com bom desempenho em detecção de malware.
- **Webroot:** Solução leve baseada em nuvem com foco em simplicidade.
- **Cybereason:** Plataforma focada em prevenção e resposta baseada em inteligência.

Niquelados:

- **AhnLab:** Provedor internacional com recursos específicos para empresas na Ásia.
- **Kaspersky:** Ausente no relatório devido à suspensão de fornecedores russos pela Gartner.

Em 9 de fevereiro de 2024, a Kaspersky não está incluída no Magic Quadrant da Gartner para Plataformas de Proteção de Endpoints. Isso se deve à decisão da Gartner de suspender a avaliação de todos os fornecedores da Rússia em março de 2022.

- **Reconhecimento da Gartner:** Apesar da ausência no Magic Quadrant, a Kaspersky recebeu reconhecimento positivo da Gartner em outras áreas:
- **Gartner Peer Insights:** A Kaspersky foi nomeada "Escolha do Cliente" para Plataformas de Proteção de Endpoints quatro vezes consecutivas (2018-2021). Este prêmio é baseado em avaliações de clientes e reflete a satisfação do usuário com o produto.
- **Gartner Security & Risk Management Summit 2022:** A Kaspersky foi reconhecida como "Cool Vendor" por sua solução Threat Hunting. Este prêmio destaca fornecedores inovadores no mercado de segurança.

9. Análise comparativa de soluções

9.1 A necessidade não pode ser atendida por softwares disponíveis no portal de Software Público Brasileiro, conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações;

10. Registro de soluções consideradas inviáveis

Solução 2: Contratar solução equivalente de outros desenvolvedores.

Considerando que solução do desenvolvedor Karpesky encontra-se implantada, em todas as estações de trabalho da Unifesspa. A aquisição de solução diversa demandaria esforço de trabalho da equipe técnica para instalação e configuração de todo o parque de computadores.

Além disso, a unidade responsável encontra-se com colaboradores em número reduzidos concentrando-se no momento na manutenção dos serviços em produção.

11. Análise comparativa de custos (TCO)

Considerando que todas as soluções consideradas viáveis são softwares proprietários licenciáveis de mercado, o Custo Total de Propriedade será calculado de forma equivalente para todas as opções existentes. Desta forma não há o que se fazer em termos de análise comparativa de custos além do levantamento de estimativa do valor máximo admitido para a contratação.

12. Descrição da solução de TIC a ser contratada

Contratação de renovação de licenças de solução antivírus composta por um conjunto de módulos de software, que funcionam de forma integrada, com o objetivo de proteger as estações de trabalho (Endpoint Protection) contra eventuais ataques cibernéticos.

Item	Descrição	CATSER	Quantidade	Unidade
1	Renovação das licenças da solução de segurança para dispositivos fins Kaspersky EndPoint Security for Business Advanced, por um período de 36 (trinta e seis) meses, incluindo suporte.	27502	1000	Licenças

13. Estimativa de custo total da contratação

Valor (R\$): 134.320,00

Quadro 2 - Estimativas de preços						
ITEM	DENOMINAÇÃO DO ITEM	CATSER	QTDE.	UNIDADE DE FORNECIMENTO	VALOR UNITÁRIO REFERÊNCIA (R\$)	VALOR TOTAL REFERÊNCIA (R\$)
01	Renovação das licenças da solução de segurança para dispositivos fins Kaspersky EndPoint Security for Business Advanced, por um período de 36 (trinta e seis) meses, incluindo suporte.	27502	1000	Licenças	R\$ 145,75	R\$ 145.750,00

14. Justificativa técnica da escolha da solução

Visando a manutenção dos níveis desejáveis de segurança na operação das soluções TIC no âmbito desta universidade, considerando a alocação do datacenter que provê os sistemas críticos que viabilizam todas as atividades administrativas e acadêmicas da Unidades, torna-se de importância vital a utilização de uma solução adequada, baseada nas boas práticas de mercado, como um software antivírus de nível corporativo, avaliado por instituições independentes dedicadas à análise específica destas soluções, que disponha de todas as funcionalidades necessárias para o controle efetivo de ataques que possam degradar os sistemas e/ou as informações neles contidos.

Essa solução irá estabelecer uma barreira inicial contra tentativas de intrusão com objetivos como: extorsão mediante sequestro de informações, uso indevido de recursos de TIC, negação de serviços e outros que ocasionem solução de continuidade das atividades laborais da UNIFESSPA de forma parcial ou plena, com consequências incalculáveis. Com todo o parque de equipamentos sendo monitorado em tempo real, a gestão centralizada da segurança, relatórios de situação, etc, a Divisão de Redes e Serviços de Internet conseguirá cumprir sua missão principal que é ade manter os recursos de TIC disponíveis a todos os colaboradores, dentro dos melhores padrões operacionais existentes.

Considerando que a falta da solução em questão permitirá a ocorrência de eventos catastróficos com impactos negativos incalculáveis para a UNIFESSPA, sua contratação já se caracteriza justificável do ponto de vista econômico já que trará redução de custos imprevistos com mitigação de riscos. Outro fato é que a solução pretendida já está devidamente consagrada como melhor alternativa de mercado para as demandas existentes, justificando-se economicamente também pela grande quantidade de fornecedores que poderão participar do certame com perspectiva de redução dos valores de referência e consequente economia para a administração.

15. Justificativa econômica da escolha da solução

16. Justificativa para o parcelamento ou não

Não há necessidade de parcelamento

17. Benefícios a serem alcançados com a contratação

Manutenção de uma solução de segurança para dispositivos fins contra ameaças cibernéticas e comprometimento de computadores, servidores e dispositivos móveis da Universidade, com garantia de operação de toda a solução por parte da contratada;

Manutenção do gerenciamento centralizado da solução de segurança dos dispositivos móveis, estações de trabalho e servidores institucionais;

Manutenção do monitoramento e rastreamento em tempo real de atividades, arquivos e processos maliciosos na infraestrutura de TI, visando auxiliar o processo de tratamento de incidentes;

Manutenção e elaboração de políticas e controles globais de acesso e uso de recursos de rede, efetuadas em nível de dispositivo;

Redução de incidentes de segurança críticos no ambiente da Universidade.

Melhoria na proteção das informações e dados pessoais e corporativos, atendendo às exigências da Lei geral de Proteção de Dados Pessoais (LGPD).

18. Providências a serem Adotadas

Não há necessidade de adoção de providências.

19. Demonstração do alinhamento estratégico

Alinhamento ao Plano de Desenvolvimento Institucional - PDI.

OE.PDI.10 - Ampliar e adequar a estrutura e a infraestrutura física e tecnológica, com critérios de acessibilidade e sustentabilidade, para garantir o pleno funcionamento da Unifesspa.

Alinhamento ao PDTIC 2022-2024/2025

A037 - Automatizar execução de ferramentas de segurança de rede

Alinhamento ao PAC 2025

Documento de Formalização da Demanda Nº 15/2025

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

Esta equipe de planejamento declara viável esta contratação.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

JORDELSON SANTIAGO MACIEL
INTEGRANTE REQUISITANTE TITULAR

ADRIANO DOS SANTOS BARROS
INTEGRANTE TÉCNICO TITULAR

MARIA ELIANE SOBRINHO
INTEGRANTE ADMINISTRATIVO TITULAR

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - TR31_2024_3_merged_1-26-36.pdf (1.3 MB)



ANEXO II - ESPECIFICAÇÃO TÉCNICA

1. Renovação de licença de software antivírus

1.1 Contratação de renovação da solução de tecnologia da informação para a proteção de computadores contra software malicioso (malware), composta por sistema de software antivírus para ambiente corporativo e serviços de suporte técnico, resumida a seguir é detalhada no restante deste documento (seções 2 e 3):

1.1.1 Sistema de software antivírus com gerenciamento centralizado para ambiente corporativo, incluindo licenças de uso, serviços de instalação e configuração inicial e subscrição de atualizações para o sistema e suas bases de dados de definições de malware pelo período de 36 (trinta e seis) meses;

1.1.2 Serviços de suporte técnico ao sistema do item 1.1.1, na modalidade "24x7" (disponível vinte e quatro horas por dia, sete dias por semana), prestados mensalmente, pelo período de 36 (trinta e seis) meses;

1.2 A tabela a seguir apresenta os quantitativos dos itens que compõem a solução:

Item	Bem / Serviço	CATMAT/CATSER	Quant.	Unidade
1	Renovação das licenças da solução de segurança para dispositivos fins Kaspersky EndPoint Security for Business Advanced, já implementada e em produção na Unifesspa, com 1000 licenças, por um período de 36 (trinta e seis) meses, incluindo suporte.	27502	1000	Licenças

2 Detalhamento

2.1 Sistema de software antivírus

2.1.1 Deverá ser entregue documentação comprobatória do licenciamento do software ofertado nas condições deste Termo de Referência dentro do prazo de 10 (dez) dias úteis a contar da assinatura do contrato.

2.1.2 Todas as ferramentas de software fornecidas devem pertencer a uma solução integrada produzida por um único fabricante/desenvolvedor.

2.1.3 A solução fornecida deverá prover proteção contra software mal-intencionado (malware) para estações de trabalho (desktops e notebooks) com sistemas operacionais Microsoft Windows, Linux e Mac OS X. As versões específicas para compatibilidade e características serão abordadas na seção 3.

2.1.4 A solução fornecida deve possuir um Servidor de Administração e Console Administrativa com compatibilidade e características abordadas na seção 3.5.

3 Compatibilidades e Características

3.1 Estações Windows:

3.1.1 Compatibilidade:

- 3.1.1.1 Microsoft Windows Embedded 8.0 Standard x64;
- 3.1.1.2 Microsoft Windows Embedded 8.1 Industry Pro x64;
- 3.1.1.3 Microsoft Windows Embedded Standard 7* x86 / x64 SP1;
- 3.1.1.4 Microsoft Windows Embedded POSReady 7* x86 / x64;
- 3.1.1.5 Microsoft Windows XP Professional x86 SP3 e superior;
- 3.1.1.6 Microsoft Windows Vista x86 / x64SP2 e posterior;



- 3.1.1.7 Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
- 3.1.1.8 Microsoft Windows 8 Professional/Enterprise x86 / x64;
- 3.1.1.9 Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- 3.1.1.10 Microsoft Windows 10 Pro / Enterprise x86 / x64.

3.1.2 Características

- 3.1.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, ramsonwares, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.1.2.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- 3.1.2.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- 3.1.2.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
- 3.1.2.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- 3.1.2.6 Firewall com IDS;
- 3.1.2.7 Autoproteção (contra-ataques aos serviços/processos do antivírus);
- 3.1.2.8 Controle de dispositivos externos;
- 3.1.2.9 Controle de acesso a sites por categoria;
- 3.1.2.10 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 3.1.2.11 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);
- 3.1.2.12 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 3.1.2.13 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 3.1.2.14 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;
- 3.1.2.15 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;
- 3.1.2.16 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 3.1.2.17 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 3.1.2.18 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;
- 3.1.2.19
- 3.1.2.20 Capacidade de verificar somente arquivos novos e alterados;
- 3.1.2.21 Capacidade de verificar objetos usando heurística;
- 3.1.2.22 Capacidade de agendar uma pausa na verificação;
- 3.1.2.23 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 3.1.2.24 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 3.1.2.25 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 3.1.2.26 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);
- 3.1.2.27 Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- 3.1.2.28 Capacidade de verificar links inseridos em e-mails contra phishings;
- 3.1.2.29 Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;



- 3.1.2.30 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 3.1.2.31 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- 3.1.2.32 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 3.1.2.33 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 3.1.2.34 Deve ter suporte total ao protocolo IPv6;
- 3.1.2.35 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 3.1.2.36 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador;
- 3.1.2.37 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
- 3.1.2.38 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- 3.1.2.39 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 3.1.2.40 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;
- 3.1.2.41
- 3.1.2.42 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- 3.1.2.43 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;
- 3.1.2.44 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);
- 3.1.2.45 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 3.1.2.46 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;
- 3.1.2.47 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 3.1.2.47.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 3.1.2.47.2 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
- 3.1.2.48 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 - 3.1.2.48.1 Discos de armazenamento locais;
 - 3.1.2.48.2 Armazenamento removível;
 - 3.1.2.48.3 Impressoras;
 - 3.1.2.48.4 CD/DVD;
 - 3.1.2.48.5 Drives de disquete;
 - 3.1.2.48.6 Modems;
 - 3.1.2.48.7 Dispositivos de fita;
 - 3.1.2.48.8 Dispositivos multifuncionais;
 - 3.1.2.48.9 Leitores de smart card;
 - 3.1.2.48.10 Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
 - 3.1.2.48.11 Wi-Fi;
 - 3.1.2.48.12 Adaptadores de rede externos;
 - 3.1.2.48.13 Dispositivos MP3 ou smartphones;
 - 3.1.2.48.14 Dispositivos Bluetooth;
 - 3.1.2.48.15 Câmeras e Scanners.



- 3.1.2.49 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;
- 3.1.2.50 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 3.1.2.51 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- 3.1.2.52 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- 3.1.2.53 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;
- 3.1.2.54 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);
- 3.1.2.55 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 3.1.2.56 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;
- 3.1.2.57 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;
- 3.1.2.58 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.

3.2 Estações Mac OS X

3.2.1 Compatibilidade:

- 3.2.1.1 Mac OS X 10.12 (Sierra);
- 3.2.1.2 Mac OS X 10.11 (El Capitan);
- 3.2.1.3 Mac OS X 10.10 (Yosemite);
- 3.2.1.4 Mac OS X 10.9 (Mavericks).
- 3.2.1.5 Mac OS X 10.8 (Mountain Lion)
- 3.2.1.6 Mac OS X 10.7 (Lion)

3.2.2 Características:

- 3.2.2.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.2.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 3.2.2.3 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;
- 3.2.2.4 Deve possuir suportes a notificações utilizando o Growl;
- 3.2.2.5 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);
- 3.2.2.6 Capacidade de voltar para a base de dados de vacina anterior;
- 3.2.2.7 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 3.2.2.8 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;
- 3.2.2.9 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 3.2.2.10 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;

- 3.2.2.11 Capacidade de verificar somente arquivos novos e alterados;
- 3.2.2.12 Capacidade de verificar objetos usando heurística;
- 3.2.2.13 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 3.2.2.14 Capacidade de verificar arquivos de formato de email;
- 3.2.2.15 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;
- 3.2.2.16 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

3.3 Servidores Windows

3.3.1 Compatibilidade:

- 3.3.1.1 Plataforma 32-bits:
 - 3.3.1.1.1 Microsoft Windows Server 2003 Standard / Enterprise (SP2);
 - 3.3.1.1.2 Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
 - 3.3.1.1.3 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 3.3.1.1.4 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
- 3.3.1.2 Plataforma 64-bits:
 - 3.3.1.2.1 Microsoft Windows Server 2003 Standard / Enterprise (SP2);
 - 3.3.1.2.2 Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
 - 3.3.1.2.3 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 3.3.1.2.4 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 3.3.1.2.5 Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 3.3.1.2.6 Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 3.3.1.2.7 Microsoft Windows Storage Server 2008 R2;
 - 3.3.1.2.8 Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
 - 3.3.1.2.9 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
 - 3.3.1.2.10 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
 - 3.3.1.2.11 Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
 - 3.3.1.2.12 Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
 - 3.3.1.2.13 Microsoft Windows Storage Server 2012 (Todas edições);
 - 3.3.1.2.14 Microsoft Windows Storage Server 2012 R2 (Todas edições);
 - 3.3.1.2.15 Microsoft Windows Hyper-V Server 2012;
 - 3.3.1.2.16 Microsoft Windows Hyper-V Server 2012 R2.
 - 3.3.1.2.17 Microsoft Windows Server 2016 x64.

3.3.2 Características:

- 3.3.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.3.2.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;
- 3.3.2.3 Firewall com IDS;
- 3.3.2.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 3.3.2.5 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 3.3.2.6 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;



- 3.3.2.7 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- 3.3.2.7.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 3.3.2.7.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 3.3.2.7.3 Leitura de configurações;
 - 3.3.2.7.4 Modificação de configurações;
 - 3.3.2.7.5 Gerenciamento de Backup e Quarentena;
 - 3.3.2.7.6 Visualização de relatórios;
 - 3.3.2.7.7 Gerenciamento de relatórios;
 - 3.3.2.7.8 Gerenciamento de chaves de licença;
 - 3.3.2.7.9 Gerenciamento de permissões (adicionar/excluir permissões acima);
 - 3.3.2.7.10 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 3.3.2.7.10.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 3.3.2.7.10.2 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 a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 3.3.2.8 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
- 3.3.2.9 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
- 3.3.2.10 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
- 3.3.2.11 Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 3.3.2.12 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- 3.3.2.13 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- 3.3.2.14 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- 3.3.2.15 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 3.3.2.16 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 3.3.2.17 Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 3.3.2.18 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 3.3.2.19 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;
- 3.3.2.20 Capacidade de verificar somente arquivos novos e alterados;
- 3.3.2.21 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- 3.3.2.22 Capacidade de verificar objetos usando heurística;
- 3.3.2.23 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 3.3.2.24 Capacidade de agendar uma pausa na verificação;
- 3.3.2.25 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;



- 3.3.2.26 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 3.3.2.27 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 3.3.2.28 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 3.3.2.29 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.4 Servidores Linux:

3.4.1 Compatibilidade:

- 3.4.1.1 CentOS 6.x ou superior;
- 3.4.1.2 Debian GNU/Linux 7.5, 7.6, 7.7 ou superior;
- 3.4.1.3 openSUSE 13.1.
- 3.4.1.4 SUSE Linux Enterprise Server 11 SP3;
- 3.4.1.5 SUSE Linux Enterprise Server 12;
- 3.4.1.6 Ubuntu Server 12.04 LTS ou superior;

3.4.2 Características:

- 3.4.2.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.4.2.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 3.4.2.3 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 3.4.2.3.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 3.4.2.3.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
- 3.4.2.4 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
- 3.4.2.5 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
- 3.4.2.6 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- 3.4.2.7 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 3.4.2.8 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;
- 3.4.2.9 Capacidade de verificar objetos usando heurística;
- 3.4.2.10 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 3.4.2.11 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 3.4.2.12 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

3.5 Servidor de Administração e Console Administrativa

3.5.1 Compatibilidade:

- 3.5.1.1 Microsoft Windows Server 2003 SP2 (Todas edições);
- 3.5.1.2 Microsoft Windows Server 2003 x64 SP2 (Todas edições);
- 3.5.1.3 Microsoft Windows Server 2008 (Todas edições);
- 3.5.1.4 Microsoft Windows Server 2008 x64 SP1 (Todas edições);
- 3.5.1.5 Microsoft Windows Server 2008 R2 (Todas edições);



- 3.5.1.6 Microsoft Windows Server 2012 (Todas edições);
- 3.5.1.7 Microsoft Windows Server 2012 R2 (Todas edições);
- 3.5.1.8 Microsoft Windows Server 2016 x64
- 3.5.1.9 Microsoft Windows Small Business Server 2003 SP2 (Todas edições);
- 3.5.1.10 Microsoft Windows Small Business Server 2008 (Todas edições);
- 3.5.1.11 Microsoft Windows Small Business Server 2011 (Todas edições);
- 3.5.1.12 Microsoft Windows XP Professional SP2 ou superior;
- 3.5.1.13 Microsoft Windows XP Professional x64 SP2 ou superior;
- 3.5.1.14 Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
- 3.5.1.15 Microsoft Windows VistaBusiness / Enterprise / Ultimate SP1 x64 ou posterior;
- 3.5.1.16 Microsoft Windows 7 Professional / Enterprise / Ultimate x86/x64 ou posterior;
- 3.5.1.17 Microsoft Windows 8 Professional / Enterprise x86/x64;
- 3.5.1.18 Microsoft Windows 8.1 Professional / Enterprise x86/x64.
- 3.5.1.19 Microsoft Windows 10 Professional / Enterprise x86/x64.

3.5.2 Suporte às seguintes plataformas virtuais:

- 3.5.2.1 VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0;
- 3.5.2.2 Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
- 3.5.2.3 KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
- 3.5.2.4 Microsoft VirtualPC 6.0.156.0;
- 3.5.2.5 Parallels Desktop 7 e superior;
- 3.5.2.6 Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
- 3.5.2.7 Citrix XenServer 6.1, 6.2.
- 3.5.2.8 Nutanix

3.5.3 Características:

- 3.5.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
- 3.5.3.2 Console deve ser baseada no modelo cliente/servidor;
- 3.5.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- 3.5.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- 3.5.3.5 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;
- 3.5.3.6 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;
- 3.5.3.7 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 3.5.3.8 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;
- 3.5.3.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 3.5.3.10 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- 3.5.3.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- 3.5.3.12 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
- 3.5.3.13 Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
- 3.5.3.14 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- 3.5.3.15 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;



- 3.5.3.16 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 3.5.3.17 Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
- 3.5.3.18 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 3.5.3.19 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 3.5.3.20 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;
- 3.5.3.21 A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- 3.5.3.22 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- 3.5.3.23 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
 - 3.5.3.23.1 Nome do computador;
 - 3.5.3.23.2 Nome do domínio;
 - 3.5.3.23.3 Range de IP;
 - 3.5.3.23.4 Sistema Operacional;
 - 3.5.3.23.5 Máquina virtual.
- 3.5.3.24 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 3.5.3.25 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;
- 3.5.3.26 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- 3.5.3.27 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;
- 3.5.3.28 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
- 3.5.3.29 instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 3.5.3.30 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;
- 3.5.3.31 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 3.5.3.32 Deve fornecer as seguintes informações dos computadores:
 - 3.5.3.32.1 Se o antivírus está instalado;
 - 3.5.3.32.2 Se o antivírus está iniciado;
 - 3.5.3.32.3 Se o antivírus está atualizado;
 - 3.5.3.32.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 3.5.3.32.5 Minutos/horas desde a última atualização de vacinas;
 - 3.5.3.32.6 Data e horário da última verificação executada na máquina;
 - 3.5.3.32.7 Versão do antivírus instalado na máquina;
 - 3.5.3.32.8 Se é necessário reiniciar o computador para aplicar mudanças;
 - 3.5.3.32.9 Data e horário de quando a máquina foi ligada;
 - 3.5.3.32.10 Quantidade de vírus encontrados (contador) na máquina;
 - 3.5.3.32.11 Nome do computador;
 - 3.5.3.32.12 Domínio ou grupo de trabalho do computador;
 - 3.5.3.32.13 Data e horário da última atualização de vacinas;
 - 3.5.3.32.14 Sistema operacional com Service Pack;
 - 3.5.3.32.15 Quantidade de processadores;
 - 3.5.3.32.16 Quantidade de memória RAM;



- 3.5.3.32.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 3.5.3.32.18 Endereço IP;
- 3.5.3.32.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- 3.5.3.32.20 Atualizações do Windows Updates instaladas;
- 3.5.3.32.21 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 3.5.3.32.22 Vulnerabilidades de aplicativos instalados na máquina;
- 3.5.3.33 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 3.5.3.34 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
 - 3.5.3.34.1 Alteração de Gateway Padrão;
 - 3.5.3.34.2 Alteração de subrede;
 - 3.5.3.34.3 Alteração de domínio;
 - 3.5.3.34.4 Alteração de servidor DHCP;
 - 3.5.3.34.5 Alteração de servidor DNS;
 - 3.5.3.34.6 Alteração de servidor WINS;
 - 3.5.3.34.7 Alteração de subrede;
 - 3.5.3.34.8 Resolução de Nome;
 - 3.5.3.34.9 Disponibilidade de endereço de conexão SSL;
- 3.5.3.35 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 3.5.3.36 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 3.5.3.37 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 3.5.3.38 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 3.5.3.39 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 3.5.3.40 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 3.5.3.41 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 3.5.3.42 Capacidade de gerar traps SNMP para monitoramento de eventos;
- 3.5.3.43 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 3.5.3.44 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 3.5.3.45 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
- 3.5.3.46 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 3.5.3.47 Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 3.5.3.48 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 3.5.3.49 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 3.5.3.50 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
 - 3.5.3.50.1 Nome do vírus;



- 3.5.3.50.2 Nome do arquivo infectado;
- 3.5.3.50.3 Data e hora da detecção;
- 3.5.3.50.4 Nome da máquina ou endereço IP;
- 3.5.3.50.5 Ação realizada.
- 3.5.3.51 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- 3.5.3.52 Capacidade de diferenciar máquinas virtuais de máquinas físicas

Identificação e assinatura da equipe de planejamento da contratação

INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO	INTEGRANTE REQUISITANTE
ADRIANO DOS SANTOS BARROS Siape 2139762,	MARIA ELIANE SOBRINHO Siape 3329725	JORDELSON SANTIAGO MACIEL Siape 1390469