Estudo Técnico Preliminar 44/2021

1. Informações Básicas

Número do processo: 23060.001576/2021-18

2. Descrição da necessidade

Aquisição de licença e suporte técnico On-line para uso de software “antivírus” a fim atender os requisitos de Segurança da Informação no âmbito do IFS.

3. Área requisitante

Área Requisitante	Responsável
Integrante Requisitante	Demair de Sá Ramos

4. Necessidades de Negócio

4.1 Detectar rapidamente qualquer nova ameaça que seja baixada pelo usuário;

4.2 Evitar que malwares sejam sequer instalados nos computadores do IFS;

4.3 Prover maior segurança e proteção aos dados;

4.4 Garantir integridade e disponibilidade dos dispositivos computacionais do IFS.

5. Necessidades Tecnológicas

Aquisição de licença e suporte técnico On-line para uso de software “antivírus” a fim atender os requisitos de Segurança da Informação no âmbito do IFS, conforme tabela abaixo:

Item	Descrição	CATMAT	Métrica	Quantidade Mínima	Quantidade Máxima
1	Licença de uso de Software Antivírus para Servidores e Estações de Trabalho, Estações Móveis e Smartphones com atualização continuada por 60 meses.	350949	Licença	1	1600

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

6.1 Requisitos Técnicos: conforme ANEXO I deste ETP;

6.2 Capacitação: Conforme manual de uso a ser entregue pelo fornecedor.

6.3 Temporais: O prazo para o fornecimento do objeto será de 30 (trinta) dias úteis, a partir do recebimento da Ordem de Fornecimento de Bens de TIC.

6.4 Segurança: Não se aplica.

6.5 Requisitos de Segurança da Informação: Obedecer ao Regulamento Geral e as normas de Segurança de Informação do IFS.

6.6 Requisitos de Sustentabilidade:

a) Os serviços serão prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5° da Instrução Normativa n° 1, de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG e do Decreto n° 7.746, de 2012, da Casa Civil, da Presidência da República, no que couber.

b) Cumprir, no que couber, as exigências do inciso XI, art. 7º da Lei 12.305, de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

c) Cumprir, no que couber, as exigências do art. 6º da Instrução Normativa MPOG nº 01, de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Justificativa/Motivação dos Itens e os Respectivos Quantitativo de Serviços Informados: baseado no sistema atual, a Instituição faz uso de 1400 licenças. Diante do recente crescimento da Instituição e perspectiva de inauguração do Campus Poço Redondo e Mudança para novo prédio do campus Glória, estima-se a necessidade de aumentar 200 licenças. Assim totalizam-se 1600.

Objeto: Aquisição de licença e suporte técnico On-line para uso de software “antivírus”		
Unidade do IFS	Métrica	Quantitativo
Reitoria	UND	200
Campus Aracaju	UND	600
Campus Socorro	UND	60
Campus Propriá	UND	60
Campus Tobias Barreto	UND	60
Campus Glória	UND	60
Campus São Cristóvão	UND	200
Campus Poço Redondo	UND	40
Campus Estância	UND	60
Campus Lagarto	UND	160

Campus Itabaiana	UND	100

8. Levantamento de soluções

8.1 Após o estudo das necessidades apontadas no item 1 deste documento, as quais foram extraídas do Plano Diretor de TI (PDTIC) do IFS, inicialmente, verificou-se o Catálogo de Soluções de TIC, conforme previsto na IN SGD/ME nº 1, de 4 de abril de 2019, no entanto, nenhuma solução de antivírus foi encontrada. Em seguida, as alternativas descritas no item 3.1 foram encontradas.

8.2 Identificação das Soluções de TIC

ID	Descrição da Solução
1	Kaspersky Endpoint Security for Business (KESB) Select
2	McAfee Endpoint Protecon Suíte

9. Análise comparativa de soluções

9.1 Análise Comparativa das Soluções de TIC

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da administração pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X

A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

9.2 Análise da Solução 1: Kaspersky Endpoint Security for Business (KESB) Select

Vantagens:

I - As licenças dos produtos Kaspersky Endpoint Security for Business (KESB) já foram adquiridas pelo IFS, sendo necessário apenas a contratação da renovação do suporte técnico on-line e atualização das ferramentas de segurança;

II - O IFS é usuária da solução Kaspersky Endpoint Security for Business (KESB) Select há aproximadamente 9 anos, o que configura experiência e conhecimento da solução pela equipe técnica do IFS;

III - A implementação e uso da ferramenta incluiu as fases de: homologação da solução, testes de funcionamento em rede e adaptações (customizações) para atendimento das especificidades do IFS em termos de sigilo. Nisso, houve um alto investimento financeiro do IFS nas fases acima elencadas que representa um comprometimento de médio/longo prazo de planejamento de utilização do produto e exploração máxima de sua potencialidade em prol das atividades de Defesa Cibernética dos computadores do IFS;

IV - ENDPOINT está instalado em mais de 1.500 Endpoints do IFS que são gerenciados pelo Kaspersky Securirty Center, administrado por pessoal da equipe de sustentação operacional de segurança da informação, treinados e capacitados para essa solução;

V - Até o presente momento, o Kaspersky Endpoint Security for Business (KESB) Select vem atendendo de maneira satisfatória os requisitos mínimos de Segurança da Informação.

VI - Para os computadores clientes o administrador da solução pode instalar os seguintes módulos:

- Prevenção contra ameaças - verifica vírus, spywares, programas indesejados e outras ameaças varrendo itens automaticamente, quando os usuários acessam ou, sob demanda, a qualquer momento.;
- Firewall - monitora a comunicação entre o computador e os recursos da rede e da Internet. E intercepta comunicações suspeitas;
- Controle da Web - exibe classificações e relatórios de segurança para sites durante a navegação ou pesquisa on-line. E permite que o administrador do site bloqueie o acesso a sites com base na classificação de segurança ou no conteúdo.;
- Proteção adaptável contra ameaças — analisa o conteúdo da empresa e decide o que deve ser feito com base na reputação do arquivo, em regras e limites de reputação.

Desvantagens: Licença paga, no entanto, para o cenário, não foi encontrado outra que atenda as especificações técnicas e que seja gratuita.

9.3 Análise da Solução 2: McAfee Endpoint Protecon Suíte

Vantagens:

I - Implementação fácil, pois as opções e recursos da solução são intuitivos para quem já possui experiência no gerenciamento de Endpoint Protecon Plaorm (EPP);

II - A interface da console de gerenciamento e do agente mostrou-se clara no quesito usabilidade, o que facilitou a configuração e criação de regras e tarefas;

III - Não houve problema para realizar a instalação dos agentes nas estações de trabalho;

IV - Com o McAfee permitiu a identificação, visibilidade e controle (podendo até efetuar bloqueios) sobre todos os softwares instalados nas estações de trabalho;

V - Durante a varredura, a solução foi capaz de identificar se os arquivos e/ou pastas já tinham sido modificados desde a última verificação;

VI - A ferramenta, ainda, permite definir o período em que os arquivos serão novamente verificados;

VII - o Antivírus McAfee Endpoint Protecon Suíte representa uma solução de segurança que atende os requisitos mínimos de segurança.

Desvantagens: Licença paga, não obstante, a aquisição desta solução de antivírus implica em custos adicionais necessários de implementação e repasse de conhecimento para todos os profissionais que ficariam responsáveis pela administração da ferramenta em questão.

10. Registro de soluções consideradas inviáveis

McAfee Endpoint Protecon Suíte, a aquisição dessa solução de antivírus implica em custos adicionais necessários de implementação e repasse de conhecimento para os profissionais que ficariam responsáveis pela administração da ferramenta, diferentemente da solução 1 que no máximo será necessário treinar a equipe a afim de atualizar-se com novas versões e\ou atualizações.

É possível visualizar esses custos no edital 11/2021 da UASG 080005, onde o item 3 (implantação) aborda R$16.000,00 por servidor e o item 4 (treinamento) R$2.600,00 por aluno.

11. Análise comparativa de custos (TCO)

11.1 Solução Viável 1: Kaspersky Endpoint Security for Business (KESB)

A estimativa do preço unitário dos itens a serem adquiridos foram obtidos a partir do cálculo da média de três cotações de preço dos itens. O preço total estimado da contratação foi obtido através da multiplicação da quantidade de itens por seus respectivos preços unitários.

Ptotal = Σ(preço estimado do item * quantidade)

MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)						
Solução	Estimativa de TCO ao longo dos anos					Total
	Ano 01	Ano 02	Ano 03	Ano 04	Ano 05	

Solução 01	R$ 116.298,66	R$ 116.298,66	R$ 116.298,66	R$ 116.298,66	R$ 116.298,66	R$ 581.493,33

Obs: Conforme estudo, diante da necessidade do IFS, há apenas uma solução viável.

12. Descrição da solução de TIC a ser contratada

Aquisição de Renovação de licenças, suporte técnico on-line para uso de software “antivírus” Kaspersky Endpoint Security for Business (KESB) a fim atender os requisitos de Segurança da Informação no âmbito do IFS, conforme tabela abaixo:

Item	Descrição	CATMAT	Métrica	Quant. Mínima	Quant. Máxima
1	Renovação de licença de uso do Kaspersky Endpoint Security for Business Advanced Antivírus para Servidores e Estações de Trabalho, Estações Móveis e Smartphones com atualização continuada por 60 meses.	350948	Licença	1	1600

13. Estimativa de custo total da contratação

Valor (R$): 260.352,00

ID	Descrição dos Serviços	Qtd.	Métrica	Valor Unitário	Valor Total
1	Renovação de licença de uso do Kaspersky Endpoint Security for Business Advanced Antivírus para Servidores e Estações de Trabalho, Estações Móveis e Smartphones com atualização continuada por 60 meses	1600	Licença	R$ 162,72	R$ 260.352,00
Valor Total Por Ano					R$ 260.352,00

14. Justificativa técnica da escolha da solução

O IFS é usuária da solução Kaspersky Endpoint Security for Business (KESB) Select há aproximadamente 9 anos, o que configura experiência e conhecimento da solução pela equipe técnica do IFS. Além disso, até o presente momento, essa solução atende de maneira satisfatória os requisitos mínimos de Segurança da Informação da Instituição.

15. Justificativa econômica da escolha da solução

As licenças já foram adquiridas, assim é necessário apenas a contratação da renovação, sem a necessidade de custos e retrabalho para implantação e treinamento.

16. Benefícios a serem alcançados com a contratação

- Garantir a continuidade da prestação de serviços ao negócio da instituição;
- Garantir a continuidade da prestação de serviços à comunidade interna e externa a instituição;
- Melhorar o desempenho da comunicação entre os sistemas informatizados e os seus clientes;
- Garantia de segurança nas estações de trabalho e servidores;
- Redução de tempo despendido em manutenção de softwares comprometidos por ações de malwares;
- Integridade de dados, garantindo a exatidão dos dados para a tomada de decisão e prosseguimento do trabalho administrativo;
- Confidencialidade, garantindo que os dados institucionais não serão expostos por malwares.

17. Providências a serem Adotadas

A Administração tomará as seguintes providências previamente ao contrato:

Definições dos servidores que farão parte da equipe de fiscalização e gestão contratual;
Capacitação dos fiscais e gestores a respeito do tema objeto da contratação;
Definição de planos de trabalho com vistas à boa execução contratual;
Acompanhamento rigoroso das ações previstas nos projetos apresentados.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

O cenário escolhido é o mais viável para o Instituto Federal de Sergipe – IFS, devido ao alcance dos resultados pretendidos e, com isso, cumprimento da missão institucional.

19. Responsáveis

LORENA DE SOUZA SILVA MEDEIROS
Integrante Administrativo

DEMAIR DE SÁ RAMOS
Integrante Requisitante

JOAO SILVIO RIBEIRO DOS SANTOS
Integrante Técnico

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 - Requisitos Técnicos.pdf (212.7 KB)

Anexo I - Requisitos Técnicos.pdf

ANEXO I - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

1.1. SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1.1.1. Compatibilidade:

1.1.1.1. Microsoft Windows Server 2008, e versões superiores.

1.1.1.2. Microsoft Windows Small Business Server 2008, e versões superiores.

1.1.1.3. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64, e versões superiores.

1.1.2. Suporta as seguintes plataformas virtuais:

1.1.2.1. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6.

1.1.2.2. Microsoft Hyper-V: 2008 e licenciamentos e versões superiores

1.1.2.3. Microsoft Virtual PC 6.0.156.0 e versões superiores.

1.1.2.4. Parallels Desktop 7 e versões superiores.

1.1.2.5. Oracle VM VirtualBox 4.0.4 e versões superiores.

1.1.2.6. Citrix XenServer 6.2 e versões superiores.

1.1.3. Características:

1.1.3.1. A console poderá ser On-Premises ou Cloud

1.1.3.2. A console deve ser acessada via WEB (HTTPS) ou MMC.

1.1.3.3. A console deve ser baseada no modelo cliente/servidor.

1.1.3.4. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

1.1.3.5. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

1.1.3.6. Deve permitir incluir usuários do AD para logarem na console de administração.

1.1.3.7. Console deve ser totalmente integrado com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

1.1.3.8. 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.

1.1.3.9. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

1.1.3.10. 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.

1.1.3.11. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

1.1.3.12. Deve armazenar histórico das alterações feitas em políticas.

1.1.3.13. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

1.1.3.14. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

1.1.3.15. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

1.1.3.16. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

1.1.3.17. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android.

1.1.3.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

1.1.3.19. 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.

1.1.3.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus.

1.1.3.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

1.1.3.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

1.1.3.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto.

1.1.3.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

1.1.3.25. 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.

1.1.3.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

1.1.3.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

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

1.1.3.28.1. Nome do computador.

1.1.3.28.2. Nome do domínio.

1.1.3.28.3. Range de IP.

1.1.3.28.4. Sistema Operacional.

1.1.3.28.5. Máquina virtual.

1.1.3.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

1.1.3.30. 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.

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

1.1.3.32. 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.

1.1.3.33. 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.

1.1.3.34. 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.

1.1.3.35. 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.

1.1.3.36. Deve fornecer as seguintes informações dos computadores:

1.1.3.36.1. Se o antivírus está instalado.

1.1.3.36.2. Se o antivírus está iniciado.

1.1.3.36.3. Se o antivírus está atualizado.

1.1.3.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo.

1.1.3.36.5. Minutos/horas desde a última atualização de vacinas.

1.1.3.36.6. Data e horário da última verificação executada na máquina.

1.1.3.36.7. Versão do antivírus instalado na máquina.

1.1.3.36.8. Se é necessário reiniciar o computador para aplicar mudanças.

1.1.3.36.9. Data e horário de quando a máquina foi ligada.

1.1.3.36.10. Quantidade de vírus encontrados (contador) na máquina.

1.1.3.36.11. Nome do computador.

1.1.3.36.12. Domínio ou grupo de trabalho do computador.

1.1.3.36.13. Data e horário da última atualização de vacinas.

1.1.3.36.14. Sistema operacional com Service Pack.

1.1.3.36.15. Quantidade de processadores.

1.1.3.36.16. Quantidade de memória RAM.

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

1.1.3.36.18. Endereço IP.

1.1.3.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

1.1.3.36.20. Atualizações do Windows Updates instaladas.

1.1.3.36.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

1.1.3.36.22. Vulnerabilidades de aplicativos instalados na máquina.

1.1.3.36.23. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

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

1.1.3.37.1. Alteração de Gateway Padrão.

1.1.3.37.2. Alteração de subrede.

1.1.3.37.3. Alteração de domínio.

1.1.3.37.4. Alteração de servidor DHCP.

1.1.3.37.5. Alteração de servidor DNS.

1.1.3.37.6. Alteração de servidor WINS.

1.1.3.37.7. Alteração de subrede.

1.1.3.37.8. Resolução de Nome.

1.1.3.37.9. Disponibilidade de endereço de conexão SSL.

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

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

1.1.3.40. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

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

1.1.3.42. 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.

1.1.3.43. 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.

1.1.3.44. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

1.1.3.45. Capacidade de gerar traps SNMP para monitoramento de eventos.

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

1.1.3.47. Listar em um único local, todos os computadores não gerenciados na rede.

1.1.3.48. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

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

1.1.3.50. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente.

1.1.3.51. 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.

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

1.1.3.53. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador.

1.1.3.54. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

1.1.3.55. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

1.1.3.56. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

1.1.3.57. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

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

1.1.3.58.1. Nome do vírus.

1.1.3.58.2. Nome do arquivo infectado.

1.1.3.58.3. Data e hora da detecção.

1.1.3.58.4. Nome da máquina ou endereço IP.

1.1.3.58.5. Ação realizada.

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

1.1.3.60. Capacidade de listar updates nas máquinas com o respectivo link para download.

1.1.3.61. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.

1.1.3.62. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

1.1.3.63. Capacidade de realizar inventário de hardware de todas as máquinas clientes.

1.1.3.64. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes.

1.1.3.65. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2. ESTAÇÕES WINDOWS

2.2.1. Compatibilidade:

2.2.1.1. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64, , e versões superiores.

2.2.1.2. Microsoft Windows Server 2012 R2 Standard x64, e versões superiores.

2.2.1.3. Microsoft Small Business Server 2011 Standard x64, e versões superiores.

2.2.1.4. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1,ce versões superiores.

2.2.2. Características:

2.2.2.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.2.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.2.2.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.2.2.4. O endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza.

2.2.2.5. Firewall com IDS.

2.2.2.6. Autoproteção (contra-ataques aos serviços/processos do antivírus).

2.2.2.7. Controle de dispositivos externos.

2.2.2.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc.

2.2.2.9. Controle de acesso a sites por horário.

2.2.2.10. Controle de acesso a sites por usuários.

2.2.2.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio.

2.2.2.12. Controle de execução de aplicativos.

2.2.2.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

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

2.2.2.17. 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.

2.2.2.18. 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.

2.2.2.19. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

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

2.2.2.21. 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.

2.2.2.22. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

2.2.2.23. Capacidade de verificar somente arquivos novos e alterados.

2.2.2.24. Capacidade de verificar objetos usando heurística.

2.2.2.25. Capacidade de agendar uma pausa na verificação.

2.2.2.26. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

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

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

2.2.2.28.1. Perguntar o que fazer, ou.

2.2.2.28.2. Bloquear acesso ao objeto.

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

2.2.2.28.2.2. Caso positivo de desinfecção:

2.2.2.28.2.2.1. Restaurar o objeto para uso.

2.2.2.28.2.3. Caso negativo de desinfecção.

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

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

2.2.2.30. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.

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

2.2.2.32. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera.

2.2.2.33. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

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

2.2.2.34.1. Perguntar o que fazer, ou.

2.2.2.34.2. Bloquear o e-mail.

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

2.2.2.34.2.2. Caso positivo de desinfecção:

2.2.2.34.2.2.1. Restaurar o e-mail para o usuário.

2.2.2.34.2.3. Caso negativo de desinfecção:

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

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

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

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

2.2.2.38. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas.

2.2.2.39. Deve ter suporte total ao protocolo Ipv6.

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

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

2.2.2.41.1. Perguntar o que fazer, ou.

2.2.2.41.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou.

2.2.2.41.3. Permitir acesso ao objeto.

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

2.2.2.42.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou.

2.2.2.42.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

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

2.2.2.44. 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.

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

2.2.2.46. 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.

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

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

2.2.2.49. 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.

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

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

2.2.2.50.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

2.2.2.51.1. Discos de armazenamento locais.

2.2.2.51.2. Armazenamento removível.

2.2.2.51.3. Impressoras.

2.2.2.51.4. CD/DVD.

2.2.2.51.5. Modems (3G,4G,5G).

2.2.2.51.6. Dispositivos de fita.

2.2.2.51.7. Dispositivos multifuncionais.

2.2.2.51.8. Leitores de smart card.

2.2.2.51.9. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc).

2.2.2.51.10. Wi-Fi.

2.2.2.51.11. Adaptadores de rede externos.

2.2.2.51.12. Dispositivos MP3 ou smartphones.

2.2.2.51.13. Dispositivo Bluetooth.

2.2.2.51.14. Câmeras e Scanners.

2.2.2.52. 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.

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

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

2.2.2.55. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.

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

2.2.2.57. 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).

2.2.2.58. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.2.2.58.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.2.58.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

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

2.2.2.60. 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.

2.2.2.61. 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.

2.2.2.62. 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.

2.2.2.63. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.2.2.64. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.2.2.65. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.2.2.66. Capacidade de integração com o Windows Defender Security Center.

2.2.2.67. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.2.2.68. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

2.2.2.69. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

2.2.2.70. O módulo deve ser capaz de agir nos seguintes estados:

2.2.2.70.1. Aprendizado: coleta informações sobre as atividades executadas pelo usuário.

2.2.2.70.2. Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

2.2.2.70.3. Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

3.3. ESTAÇÕES MAC OS X:

3.3.1. Compatibilidade:

3.3.1.1. MacOS Catalina 10.15, e versões superiores.

3.3.2. Características:

3.3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

3.3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https.

3.3.2.3. Possuir módulo de bloqueio á ataques na rede.

3.3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.

3.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede.

3.3.2.6. Possibilidade de importar uma chave no pacote de instalação.

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

3.3.2.8. Deve possuir suportes a notificações utilizando o Growl.

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

3.3.2.10. Capacidade de voltar para a base de dados de vacina anterior.

3.3.2.11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.

3.3.2.12. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de

exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

3.3.2.13. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).

3.3.2.14. 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.

3.3.2.15. Capacidade de verificar somente arquivos novos e alterados.

3.3.2.16. Capacidade de verificar objetos usando heurística.

3.3.2.17. Capacidade de agendar uma pausa na verificação.

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

3.3.2.18.1. Perguntar o que fazer, ou.

3.3.2.18.2. Bloquear acesso ao objeto;

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

3.3.2.18.3.1. Caso positivo de desinfecção:

3.3.2.18.3.1.1. Restaurar o objeto para uso.

3.3.2.18.3.2. Caso negativo de desinfecção:

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

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

3.3.2.20. Capacidade de verificar arquivos de formato de email.

3.3.2.21. 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.

3.3.2.22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4.4 ESTAÇÕES DE TRABALHO LINUX

4.4.1. Compatibilidade:

4.4.1.1. Plataforma 32-bits:

4.4.1.1.1. Ubuntu 14.04.5 LTS, e versões superiores.

4.4.1.1.2. Red Hat® Enterprise Linux® 6.9, e versões superiores.

4.4.1.1.3. CentOS-6.9, e versões superiores.

4.4.1.1.4. Debian GNU/Linux 8.10, e versões superiores.

4.4.1.2. Plataforma 64-bits:

4.4.1.2.1. Ubuntu 14.04.5 LTS, e versões superiores.

4.4.1.2.2. Red Hat® Enterprise Linux® 6.9, e versões superiores.

4.4.1.2.3. CentOS-6.9, e versões superiores.

4.4.1.2.4. Debian GNU/Linux 8.10, e versões superiores.

4.4.1.2.5. OracleLinux 7.4, e versões superiores.

4.4.1.2.6. SUSE® Linux Enterprise Server 12 SP3, e versões superiores.

4.4.1.2.7. OpenSUSE® 42.3, e versões superiores.

4.4.2. Características:

4.4.2.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

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

4.4.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.4.2.3.1. Capacidade de criar exclusões por local, máscara e nome da ameaça.

4.4.2.4. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

4.4.2.5. 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.

4.4.2.6. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

4.4.2.7. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

4.4.2.7.1. Alta.

4.4.2.7.2. Média.

4.4.2.7.3. Baixa.

4.4.2.7.4. Recomendado.

4.4.2.8. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

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

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

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

4.4.2.12. 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.

4.4.2.13. Capacidade de verificar objetos usando heurística.

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

4.4.2.15. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados; de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4.5. Servidores Windows:

4.5.1. Compatibilidade:

4.5.1.1. Plataforma 32-bits:

4.5.1.1.1. Windows Server 2008 Standard/Enterprise/Datacenter SP1, e versões superiores.

4.5.1.1.2. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior, e versões superiores.

4.5.1.2. Plataforma 64-bits:

4.5.1.2.1. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter, e versões superiores.

4.5.1.2.2. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter, e versões superiores.

4.5.1.2.3. Microsoft Windows Storage Server 2008 R2, e versões superiores.

4.5.1.2.4. Microsoft Windows Hyper-V Server 2008 R2 SP1, e versões superiores.

4.5.2. Características:

4.5.2.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

4.5.2.2. Autoproteção contra ataques aos serviços/processos do antivírus.

4.5.2.3. Firewall com IDS.

4.5.2.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

4.5.2.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.5.2.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

4.5.2.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

4.5.2.7.3. Leitura de configurações.

4.5.2.7.4. Modificação de configurações.

4.5.2.7.5. Gerenciamento de Backup e Quarentena.

4.5.2.7.6. Visualização de relatórios.

4.5.2.7.7. Gerenciamento de relatórios.

4.5.2.7.8. Gerenciamento de chaves de licença.

4.5.2.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

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

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

4.5.2.8.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome

de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

4.5.2.9. 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.

4.5.2.10. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

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

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

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

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

4.5.2.15. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

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

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

4.5.2.18. 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.

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

4.5.2.20. 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.

4.5.2.21. Capacidade de verificar somente arquivos novos e alterados.

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

4.5.2.23. Capacidade de verificar objetos usando heurística.

4.5.2.24. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

4.5.2.25. Capacidade de agendar uma pausa na verificação.

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

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

4.5.2.27.1. Perguntar o que fazer, ou.

4.5.2.27.2. Bloquear acesso ao objeto.

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

4.5.2.27.3.1. Caso positivo de desinfecção:

4.5.2.27.3.1.1. Restaurar o objeto para uso.

4.5.2.27.3.2. Caso negativo de desinfecção:

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

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

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

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

4.5.2.31. Deve possuir módulo que analisa cada script executado, procurando por sinais de atividade maliciosa.

4.5.2.32. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

4.5.2.33. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

4.5.2.34. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

4.6. Servidores Linux:

4.6.1. Compatibilidade:

4.6.1.1. Plataforma 32-bits:

4.6.1.1.1. Red Hat® Enterprise Linux® 6.9 Server, e versões superiores.

4.6.1.1.2. CentOS-6.9, e versões superiores.

4.6.1.1.3. Ubuntu 14.04.5 LTS, e versões superiores.

4.6.1.1.4. Debian GNU / Linux 8.10, e versões superiores.

4.6.1.2. Plataforma 64-bits:

4.6.1.2.1. Red Hat® Enterprise Linux® 6.9 Server, e versões superiores.

4.6.1.2.2. CentOS-6.9, e versões superiores.

4.6.1.2.3. Ubuntu 14.04.5 LTS, e versões superiores.

4.6.1.2.4. Debian GNU / Linux 8.10, e versões superiores.

4.6.1.2.5. SUSE® Linux Enterprise Server 12 SP3, e versões superiores.

4.6.1.2.6. Oracle Linux 7.4, e versões superiores.

4.6.2. Características:

4.6.2.1. Antivírus de Arquivos residente (antispyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

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

4.6.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.6.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

4.6.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto,

sendo assim possível a restauração de objetos que contenham informações importantes.

4.6.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

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

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

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

4.6.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

4.6.2.7. Capacidade de verificar objetos usando heurística.

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

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

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

4.7. Smartphones e tablets:

4.7.1. Compatibilidade:

4.7.1.1. Dispositivos com os sistemas operacionais:

4.7.1.1.1. Android 5.0, e versões superiores.

4.7.1.1.2. iOS 10.0, e versões superiores.

4.7.2. Características:

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

4.7.2.1.1. Proteção contra adware e autodialers.

4.7.2.1.2. 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.

4.7.2.1.3. Arquivos abertos no smartphone.

4.7.2.1.4. Programas instalados usando a interface do smartphone.

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

4.7.2.2. Deverá isolar em área de quarentena os arquivos infectados.

4.7.2.3. Deverá atualizar as bases de vacinas de modo agendado.

4.7.2.4. Deverá bloquear spams de SMS através de Black lists.

4.7.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo.

4.7.2.6. Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

4.7.2.7. Deverá ter função de limpeza de dados pessoais à distância, em caso de roubo, por exemplo.

4.7.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

4.7.2.9. Deverá ter firewall pessoal (Android).

4.7.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente.

4.7.2.11. Capacidade de enviar comandos remotamente de:

4.7.2.11.1. Localizar.

4.7.2.11.2. Bloquear.

4.7.2.12. Capacidade de detectar Jailbreak em dispositivos iOS.

4.7.2.13. Capacidade de detectar Root em dispositivos Android.

4.7.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos.

4.7.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso.

4.7.2.16. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído.

4.7.2.17. Capacidade de configurar White e blacklist de aplicativos.

4.7.2.18. Capacidade de localizar o dispositivo quando necessário.

4.7.2.19. Permitir atualização das definições quando estiver em "roaming".

4.7.2.20. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

4.7.2.21. Deve permitir verificar somente arquivos executáveis.

4.7.2.22. Deve ter a capacidade de desinfectar o arquivo se possível (Android).

4.7.2.23. Capacidade de agendar uma verificação (Android).

4.7.2.24. Capacidade de enviar URL de instalação por e-mail.

4.7.2.25. Capacidade de fazer a instalação através de um link QRCode.

4.7.2.26. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

4.7.2.26.1. Deletar.

4.7.2.26.2. Ignorar.

4.7.2.26.3. Quarentenar.

4.7.2.26.4. Perguntar ao usuário.

4.8. Gerenciamento de dispositivos móveis:

4.8.1. Compatibilidade:

4.8.1.1. Dispositivos com os sistemas operacionais:

4.8.1.1.1. Android 5.0, e versões superiores.

4.8.1.1.2. iOS 10.0, e versões superiores.

4.8.2. Softwares de gerência de dispositivos

4.8.2.1. VMWare Workspace ONE UEM 1905, e versões superiores.

4.8.2.2. MobileIron 10. , e versões superiores.

4.8.2.3. IBM Maas360 10.74, e versões superiores.

4.8.2.4. SOTI MobiControl 14.4, e versões superiores.

4.8.3. Características:

4.8.3.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange.

4.8.3.2. Capacidade de ajustar as configurações de:

4.8.3.2.1. Sincronização de e-mail.

4.8.3.2.2. Uso de aplicativos.

4.8.3.2.3. Senha do usuário.

4.8.3.2.4. Criptografia de dados;

4.8.3.2.5. Conexão de mídia removível.

4.8.3.3. Capacidade de instalar certificados digitais em dispositivos móveis.

4.8.3.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

4.8.3.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS.

4.8.3.6. Capacidade de, remotamente, bloquear um dispositivo iOS.

4.8.3.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

4.8.3.8. Permitir sincronização com perfil do "Touch Down".

4.8.3.9. Capacidade de desinstalar remotamente o antivírus do dispositivo.

4.8.3.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

4.8.3.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

4.9. Criptografia:

4.9.1. Compatibilidade:

4.9.1.1. Microsoft Windows 7 Ultimate SP1 e licenciamentos e versões superiores x86/x64.

4.9.2. Características:

4.9.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.

4.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits.

4.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.

4.9.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.

4.9.2.5. Permitir criar vários usuários de autenticação pré-boot.

4.9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.

4.9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

4.9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.

4.9.2.7.2. Criptografar todos os arquivos individualmente.

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

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

4.9.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.

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

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

4.9.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia.

4.9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia.

4.9.2.13. Bloqueia o reuso de senhas.

4.9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas.

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

4.9.2.16. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo.

4.9.2.17. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do Outlook".

4.9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas.

4.9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do Office, Document, arquivos de audio, etc.

4.9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados.

4.9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações.

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

4.9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia.

4.9.2.24. Capacidade de criptografar somente o espaço em disco utilizado.

4.9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador.

4.9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados.

4.9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc.

4.9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft.

4.9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker.

4.9.2.30. Capacidade de fazer "Hardware encryption".

4.10. Gerenciamento de Sistemas:

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

4.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens.

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

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

4.10.5. Capacidade de gerenciar licenças de softwares de terceiros.

4.10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

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

4.10.8. Possibilita fazer distribuição de software de forma manual e agendada.

4.10.9. Suporta modo de instalação silenciosa.

4.10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis.

4.10.11. Possibilita fazer a distribuição através de agentes de atualização.

4.10.12. Utiliza tecnologia multicast para evitar tráfego na rede.

4.10.13. Possibilita criar um inventário centralizado de imagens.

4.10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário.

4.10.15. Suporte a WakeOnLan para deploy de imagens.

4.10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches.

4.10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento.

4.10.18. Capacidade de gerar relatórios de vulnerabilidades e patches.

4.10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração.

4.10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador.

4.10.21. Permite baixar atualizações para o computador sem efetuar a instalação.

4.10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas.

4.10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade.

4.10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento.

4.10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

4.10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos.

4.10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador.

4.10.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades.

4.10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas.

4.10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

4.10.31. Verificar se a contratada indicou formalmente o preposto que irá representá-la durante a vigência contratual.

5. SUPORTE TÉCNICO

5.1. O Suporte Técnico deverá ser prestado pela CONTRATADA durante o tempo de contrato e ficando a cargo da CONTRATANTE;

5.2 A CONTRATADA deverá disponibilizar canais para abertura de chamados, tais como telefone, e-mail ou sistema web, para atender as solicitações de suporte da CONTRATANTE.

5.3 O Suporte Técnico prestado pela CONTRATADA deverá ser realizado em idioma português, em regime comercial (8 horas x 5 dias da semana), remotamente, 4h mensal, não cumulativo.

5.5. Sendo a CONTRATADA representante da FABRICANTE, deverá disponibilizar ligação através de 0800 ou equivalente à ligação local para abertura e acompanhamento de chamados.

5.5 O prazo para a CONTRATADA iniciar o atendimento via suporte telefônico para diagnosticar o problema é de, no máximo 24 (vinte e quatro) horas, contado a partir da abertura do chamado e dentro do período de disponibilidade.

5.6. As requisições de serviços serão encaminhadas à Central de Serviços, por meio de um chamado, no qual constará:

5.6.1. Identificação do requisitante;

5.6.2. Identificação do Gestor do contrato;

5.6.3. Descrição do serviço;

5.6.4. A partir da data de recebimento da solicitação de serviço, a CONTRATADA, no prazo máximo de 06 (seis) horas úteis, deverá realizar o atendimento**.**