Coordenação de Administração
de Contratos / CGCC
Fls._____

Processo nº **48000.001679/2016-56**

CONTRATO Nº 30/2016-MME

PARA AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA, QUE ENTRE SI CELEBRAM A UNIÃO POR INTERMÉDIO DO MINISTÉRIO DE MINAS E ENERGIA E A EMPRESA INFOSEC TECNOLOGIA DA INFORMAÇÃO LTDA.

A **União**, por intermédio do **MINISTÉRIO DE MINAS E ENERGIA,** inscrito no CNPJ sob n.º 37.115.383/0001-53, localizado na Esplanada dos Ministérios, Bloco "U", CEP: 70065-900 cidade de Brasília-DF, neste ato representado por seu **Subsecretário de Planejamento, Orçamento e Administração**, Senhor **Orlando Henrique Costa de Oliveira**, portador da Cédula de Identidade n.º 0388679581-SSP/BA e CPF nº 735.410.875-87, com fundamento no inciso VII do artigo 45 do Regimento Interno da Secretaria Executiva/MME aprovado pela Portaria GM/MME nº 89, de 27 de fevereiro de 2014, publicada no Diário Oficial da União de 28 de fevereiro de 2014, doravante denominado simplesmente **Contratante**, e de outro lado, a empresa **INFOSEC Tecnologia da Informação Ltda.**, inscrita no CNPJ sob n.º 11.266.883/0001-00, estabelecida na SCN Quadra 05 Torre Sul, Sala 1212, Ed. Brasília Shopping, Asa Norte - CEP: 70715-900 - Brasília – DF, neste ato representada pelo seu Representante Legal, o Senhor **Leonardo Garcia Rocha**, portador da RG n.º 2.332.793 –SSP/DF e CPF n.º 001.496.351-50, daqui por diante denominada **Contratada**, têm entre si, justo e avençado e **celebram o presente Contrato para aquisição de solução de segurança,** que tem seu respectivo fundamento e finalidade na consecução do objeto contratado, descrito abaixo, constante da **Ata de Registro de Preços nº 22/2015-MAPA**, originária do **Pregão Eletrônico nº 21/2015-MAPA**, constante do Processo Administrativo nº 21000.007816/2014-48, e em observância às disposições contidas, com fundamento na Lei nº 10.520, de 17 de julho de 2002, publicada no D.O.U., de 18 de julho de 2002, no Decreto n.º 3.555, de 08 de agosto de 2000, publicado no D.O.U., de 09 de agosto de 2000 e, subsidiariamente, no Decreto nº 5.450 de 31/05/2005, publicado no D.O.U., de 01 de junho de 2005, e pela Lei nº 8.666, de 21 de junho de 1993, publicada no D.O.U., de 22 de junho de 1993, e alterações, e no que consta do Processo n.º 48000.001679/2016-56-MME, mediante as cláusulas e condições mediante os termos e condições estabelecidos nas seguintes Cláusulas:

CLÁUSULA PRIMEIRA - OBJETO

1.1 Aquisição de solução de segurança integrada para estações de trabalho e ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades do Ministério de Minas e Energia.

1.2 Este Termo de Contrato vincula-se ao Edital de Pregão Eletrônico nº 21/2015-MAPA e de seus Anexos, da legislação vigente e da minuta aprovada pela Consultoria Jurídica por meio do Parecer nº 0710/2016/CONJUR-MME/CGU/AGU, bem como a proposta da Contratada, datada de 10/11/2016, os quais se encontram vinculados direta ou indiretamente ao presente Contrato e passam a fazer parte integrante deste instrumento, independentemente de sua transcrição.

CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES E CARACTERÍSTICAS

2.1. BENS E/OU SERVIÇOS

Os serviços contratados compreenderão as atividades de:

I. Aquisição de licenças.
II. Suporte técnico 24x7 on-site por um período de 12 (doze) meses;

O Prazo de entrega, instalação, configuração e ativação dos sistemas e softwares não será superior a 30 dias corridos.

O prazo de entrega a que se refere o Subitem acima poderá ser prorrogado uma única vez e por igual período, mediante justificativa devidamente fundamentada pela Contratada, por escrito, até 24h (vinte e quatro horas) antes da data fixada.

A Contratada efetuará a instalação, configuração e ativação dos sistemas e softwares, atendendo integralmente às características e às necessidades do Contratante e responsabilizando-se por todas as conexões, materiais, acessórios e mão de obra necessária para o seu bom funcionamento.

Os sistemas e softwares deverão ser acompanhados de manuais de instalação, operação e manutenção, quando de sua entrega, bem como de todos os acessórios necessários ao seu pleno funcionamento.

Adicionalmente serão realizados os seguintes serviços:

- Serviços de instalação e customização dos produtos;
- Serviços de suporte técnico *on-site* na modalidade 24x7 (vinte e quatro horas por dia e sete dias por semana).

Considerando a situação atual do Contratante descrita neste Contrato, a quantidade de licença a ser contratada encontra-se detalhada na tabela abaixo:

Lote	Item	Descrição	Unidade	Quant.
1	8	**Aquisição de Solução para Prevenção de Ataques Direcionados, Symantec Advanced Threat Protection – Usuários**	Unidade	1200

2.2. REQUISITOS TECNOLÓGICOS

Lote 01: Solução para Proteção, Monitoração e Manutenção da Autenticidade da Informação

- Solução de Segurança, Symantec Protection Suite Enterprise Edition 4.0 ou superior, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução de Proteção, Segurança e Controle de Dispositivos Móveis, Symantec Mobile Suíte, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução de Proteção, Segurança e Controle dos Dados, Symantec Data Loss Prevention 12.5 ou superior, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para Sigilo, Confidencialidade, Symantec Encryption, incluindo

licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;

- Solução do Gerenciamento da Segurança, Symantec IT Management Suite, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para Proteção Avançada de Servidores, Symantec Data Center Security Server Advanced, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Segurança Proativa com Inteligência de Detecção, Symantec Deepsight, incluindo licenças de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para Prevenção de Ataques Direcionados, Symantec Advanced Threat Protection, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para a Gestão e Análise de Ambiente Infraestrutura, Symantec Control Compliance Suite, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para a Gestão e Análise de Ambiente Usuários, Symantec Control Compliance Suite, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução para validação de autenticação forte OTP, Symantec Validation and ID Protection Service, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;
- Solução de Portal para Autenticação Única, Symantec Identity Access Manager, incluindo licenças definitivas de uso, garantia de software e substituição da Solução de Proteção atual;

LOTE 1: Solução Symantec para Proteção, Monitoração e Manutenção da Autenticidade da Informação

Proteção da Informação

2.2.1. Gerenciamento e Características Gerais da Solução

2.2.1.1. Administração centralizada por console de gerenciamento única das soluções;

2.2.1.2. As configurações e gerenciamento do Antivírus, Anti-spyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para maquinas físicas e virtuais através da mesma console;

2.2.1.3. Toda a solução padrão deverá funcionar com agente único na estação de trabalho e servidores físicos e virtuais a fim de diminuir o impacto ao usuário final.

2.2.1.4. Console de gerenciamento via tecnologia Web (HTTP e HTTPS);

2.2.1.5. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

2.2.1.6. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2003 R2, SP1 ou superior e Microsoft Windows Server 2008, 2008 R2 ou

superior;

2.2.1.7. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32-bit e 64-bit suportando ambiente virtual XEN, VMWARE e Microsoft;

2.2.1.8. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;

2.2.1.9. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

2.2.1.10. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

2.2.1.10.1. IP e range de IP;
2.2.1.10.2. Endereço de Servidores de DNS, DHCP e WINS;
2.2.1.10.3. Conexão com o servidor de gerência;
2.2.1.10.4. Conexões de rede como VPN, Ethernet, Wireless e Modem;

2.2.1.11. Possibilidade de aplicar regras diferenciadas por grupos de usuários e maquinas;

2.2.1.12. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2005 e 2008;

2.2.1.13. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover.

2.2.1.14. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);

2.2.1.15. Possibilidade de instalação dos clientes em servidores, estações de trabalho e maquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;

2.2.1.16. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;

2.2.1.17. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;

2.2.1.18. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicos e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

2.2.1.19. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

2.2.1.20. Instalação e atualização do software sem a intervenção do usuário;

2.2.1.21. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;

2.2.1.22. Suportar redirecionamentos dos logs para um servidor de Syslog;

2.2.1.23. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;

2.2.1.24. Deve ter a capacidade de integração com solução de Data Loss Prevention, para os e-mails de saída, possibilitando utilização de mais de um servidor de DLP, para um mesmo Gateway de SMTP;

2.2.1.25. Deve ter a capacidade de priorização dos servidores de DLP utilizados na integração com o Gateway de SMTP, possibilitando balancear o tráfego a ser analisado;

2.2.1.26. Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do órgão;

2.2.1.27. Deve ter capacidade de integração com servidor de criptografia, para criptografar mensagens e anexos;

2.2.1.28. Deve ter a capacidade de permitir ou não endereços de e-mail com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8-bit;

2.2.1.29. Deve ter a capacidade de rejeitar conexões que tentem serem abertas pelos comandos "HELO" e "EHLO", sem que existam gravados seus endereços de "MX" e "A" nos servidores de DNS;

2.2.1.30. Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;

2.2.1.31. Deve ter a capacidade de implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual;

2.2.1.32. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado;

2.2.1.33. Deve possuir integração com Active Directory, para autenticação de usuários da solução;

2.2.1.34. O servidor de gerenciamento contra a fuga de informações deverá utilizar, no mínimo, banco de dados relacional Oracle, por possibilitar sua criptografia;

2.2.1.35. Deve ter a capacidade de instalar de servidores de gerenciamento, monitores e scanners adicionais, fornecendo assim a possibilidade de trabalhar em Load Balance e Failover;

2.2.1.36. Deve ter a capacidade de realizar atualização de versão e patches nos componentes da solução através da console de gerenciamento;

2.2.1.37. Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação;

2.2.1.38. Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;

2.2.1.39. Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;

2.2.1.40. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;

2.2.1.41. Deve permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);

2.2.1.42. Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;

2.2.1.43. Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;

2.2.1.44. Deve ter a capacidade de indexação off-line de dados armazenados em sistemas em redes isoladas, sem conectividade pelo DLP;

2.2.1.45. Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados;

2.2.1.46. Deve possuir logs detalhados de auditoria de alterações de políticas;

2.2.1.47. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;

2.2.1.48. Deve ter suporte a servidores com hardware x86 e sistema operacional Windows e Linux, não requerendo a utilização de appliance;

2.2.1.49. A solução deve ser do tipo cliente/servidor, onde a parte servidora mantém todas as configurações definidas pelo administrador e a parte cliente busca ou recebe essas configurações do servidor. O software cliente é instalado em estações de trabalho e outros clientes, como tablets. O software de gerenciamento (parte servidora) é instalado em um ou mais servidores dedicados e dimensionados para esse fim, denominado, neste documento, de Servidores de Gerenciamento;

2.2.1.50. Permitir a instalação de Servidores de Gerenciamento adicionais, fornecendo assim a possibilidade de trabalho em redundância onde, no caso de falha de um dos servidores, o outro assume todas as funções da solução, sem provocar indisponibilidade para os endpoints;

2.2.1.51. Permitir o gerenciamento de clientes, incluindo inventário de software e hardware, com, no mínimo, os seguintes sistemas operacionais:

2.2.1.51.1. Windows Server 2003 e superior;
2.2.1.51.2. Windows Server 2008 e superior, 32 e 64 bits;
2.2.1.51.3. Windows XP;
2.2.1.51.4. Windows 7, 32 e 64 bits;
2.2.1.51.5. MacOS Lion 10 e superior;
2.2.1.51.6. iPhone 3G, 3GS, 4;
2.2.1.51.7. iPad 1 e 2 ;
2.2.1.51.8. iOS 4.1 e versões;
2.2.1.51.9. iOS 5 e superior;
2.2.1.51.10. Android 2.2 e superior;
2.2.1.51.11. Windows Phone 7, Windows Mobile 6.1, 6.5;
2.2.1.51.12. Blackberry OS 4.3 e superior;
2.2.1.51.13. WebOS 1.4.5 e superior;
2.2.1.51.14. Symbian v5.0.50;

2.2.1.52. Permitir a instalação em máquinas virtuais sem impor nenhuma restrição ao funcionamento e aos recursos e funcionalidades;

2.2.1.53. Caso a solução ofertada utilize SGBD – Sistema Gerenciadores de Bancos de Dados, este deverá ser fornecido como bundle, ou seja, já

embutido no custo da na solução;

2.2.1.54. Possibilitar o estabelecimento de alvos de políticas por filtros baseados em qualquer informação disponível sobre os clientes. Exemplos: configurações de sistema operacional, hardware, componentes, softwares e versões;

2.2.1.55. Clientes devem ser atualizados automaticamente nos grupos de políticas conforme a inclusão ou exclusão de clientes ou da mudança de suas configurações;

2.2.1.56. Implementar, na própria solução, código único para clientes, garantindo consistência para a base de dados mesmo com mudanças de hostname, endereço MAC da placa de rede, endereço IP ou outras informações nos clientes evitando a criação de registros duplicados;

2.2.1.57. Permitir forçar comunicação dos clientes a partir da console para atualizar as políticas e inventário;

2.2.1.58. Permitir a ativação e desativação do software cliente por meio da console de gerenciamento, sem necessidade de reinicialização do endpoint;

2.2.1.59. Permitir integração da solução com o Microsoft Active Directory, possibilitando, no mínimo, as seguintes tarefas:

2.2.1.59.1. Importação e sincronização de usuários, computadores, sites, unidades organizacionais e grupos do AD;

2.2.1.59.1.1. Permitir ao administrador criar agendamentos e definir horários ou frequência de importação;

2.2.1.59.1.2. Permitir a importação e sincronização diferencial, ou seja, apenas dos dados que apresentarem modificações em relação à última sincronização realizada, mantendo a alteração mais recente;

2.2.1.59.1.3. Permitir autenticação de usuários da solução, permitindo atribuir papeis na utilização da console de gerência;

2.2.1.60. Aplicação de políticas baseadas em grupos de AD;

2.2.1.61. Instalação automática do software cliente em computadores de grupos pré-definidos do AD que ainda não estejam sendo gerenciados;

2.2.1.62. Permitir o agendamento de instalação, atualização e desinstalação do software cliente via políticas no servidor a partir da console de gerenciamento da solução sem necessidade de reinício (boot) dos endpoints e de forma silenciosa, ou seja, sem interação com usuário;

2.2.1.63. Flexibilidade para definição da frequência de comunicação cliente-servidor;

2.2.1.64. Controlar banda de rede utilizada pelo cliente na sua comunicação com o servidor utilizando:

2.2.1.65. Configurações diferenciadas por faixa de horário.

2.2.1.66. Permitir configurar exceções para políticas;

2.2.1.67. Bloquear a comunicação por faixa de horário com as seguintes opções:

2.2.1.67.1. Comunicação total entre cliente-servidor e download;

2.2.1.68. Gerenciar a comunicação cliente-servidor com computadores:

2.2.1.68.1. Na LAN e/ou WAN;
2.2.1.68.2. Na Internet com VPN;
2.2.1.68.3. Na Internet;

2.2.1.69. Suporte a múltiplos domínios independente de sua estrutura ou relacionamento de confiança;

2.2.1.70. Deverá prover funcionalidade de envio de logs a servidor do tipo syslog;

2.2.1.71. Deverá permitir a definição de política geral que se aplique aos usuários que não estejam conectados à rede gerenciada pela instituição, para no mínimo:

2.2.1.72. Prover capacidade de habilitar somente os aplicativos homologados pela instituição, enquanto conectados à rede gerenciada;

2.2.1.73. Prover capacidade de separar a utilização dos aplicativos privados dos corporativos homologados;

2.2.1.74. A solução deverá possuir ferramenta de workflow nativa, devendo permitir customização dos processos;

2.2.1.75. A customização deve ser realizada em interface que permita arrastar-e-soltar;

2.2.1.76. Deverá apresentar lista de tarefas para prover uma visão de portal para usuário final, permitindo que visualizem quais atividades requerem ação e processem atividades como parte do workflow;

2.2.1.77. Deverá possuir portal para gerenciamento de processos que provê visibilidade de todos os processos para administradores.

2.2.1.78. Deve ter a capacidade de delegar o gerenciamento com procedimentos "Self-Healing", diminuindo tempo de suporte com tarefas padronizadas;

2.2.1.79. Deve ter a capacidade de executar de forma automática, sem a necessidade nenhum script e agentes externos ao software, a reparação, correção e falta de aplicações nos dispositivos móveis gerenciados;

2.2.1.80. Criptografia de Armazenamento Removível Baseada em Volúmes;

2.2.1.81. Serviços de criptografia e funções de interação do usuário suportados para máquinas que não são integrantes do domínio;

2.2.1.82. A solução deve proteger dados gravados em dispositivos USB, fire-wire, pen-drives, CD/DVDs, discos rígidos externos, cartões digitais protegidos, ipods, câmeras digitais, e em dispositivos, mesmo quando não identificados como "removíveis";

2.2.2. Atualização de Vacinas

2.2.2.1. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus mecanismo de verificação (Engine) dos clientes da rede;

2.2.2.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;

2.2.2.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda,

quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

2.2.2.4. Atualização remota e incremental da versão do software cliente instalado;

2.2.2.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la.

2.2.2.6. Atualização automática das assinaturas do servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

2.2.2.7. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;

2.2.2.8. Um único e mesmo arquivo de vacina de Vírus para todas as plataformas Windows e versões do antivírus.

2.2.2.9. Quarentena

2.2.2.10. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

2.2.2.11. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

2.2.3. Cliente Gerenciado

2.2.3.1. Suportar máquinas com arquitetura 32-bit e 64-bit;

2.2.3.2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com os sistemas operacionais XP, 2003, Vista, 2008, 2008 R2 e 7;

2.2.3.3. Possuir certificação FIPS 140-2;

2.2.3.4. Possuir certificação Common Criteria (CC) EAL2+;

2.2.3.5. O fabricante deverá possuir certificação ICSA Labs no mínimo nas plataformas Windows XP, Windows Vista e Windows 7;

2.2.4. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades

2.2.4.1. Suporte aos protocolos TCP, UDP e ICMP;

2.2.4.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;

2.2.4.3. Possuir proteção contra exploração de buffer overflow;

2.2.4.4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;

2.2.4.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

2.2.4.6. Possibilidade de agendar a ativação da regra de Firewall;

2.2.4.7. Possibilidade de criar regras diferenciadas por aplicações;

2.2.4.8. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;

2.2.4.9. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;

2.2.4.10. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;

2.2.4.11. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;

2.2.4.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;

2.2.4.13. Gerenciamento integrado à console de gerência da solução;

2.2.5. Funcionalidade de Antivírus e Anti-Spyware as funcionalidades:

2.2.5.1. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.

2.2.5.2. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;

2.2.5.3. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;

2.2.5.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);

2.2.5.5. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixo, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;

2.2.5.6. Permitir que verificação das ameaças da maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;

2.2.5.7. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;

2.2.5.8. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Notes e POP3/SMTP;

2.2.5.9. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);

2.2.5.10. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

2.2.5.11. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;

2.2.5.12. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e

Microsoft, para no mínimo:

2.2.5.12.1. Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;

2.2.5.12.2. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:

2.2.5.12.2.1. Proteção de antivírus e anti-spyware;
2.2.5.12.2.2. Proteção de heurística e reputação de arquivos em tempo real (real-time);
2.2.5.12.2.3. Proteção de IPS de rede e "host";
2.2.5.12.2.4. Controle de dispositivos e aplicações;

2.2.5.12.3. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;

2.2.5.12.4. Capacidade de verificar "templates" de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (template);

2.2.5.13. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;

2.2.5.14. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;

2.2.5.15. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

2.2.5.15.1. Origem confiável;
2.2.5.15.2. Origem não confiável;
2.2.5.15.3. Tempo de existência do arquivo na internet;
2.2.5.15.4. Comportamento do arquivo;
2.2.5.15.5. Quantidade mínima de usuários que baixaram o arquivo da internet;

2.2.5.16. Capacidade de implementar regras distintas por grupo (ex. Departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;

2.2.5.17. Deve ter a capacidade de executar backup de forma manual, assim como, o agendamento dos backups, facilitando assim a criação dos pontos de recuperação;

2.2.5.18. Deve ter a capacidade de explorar arquivos de um ponto de recuperação, atribuindo uma letra de unidade visível no Windows Explorer, podendo executar no mínimo as seguintes tarefas:

2.2.5.18.1. Executar o ScanDisk ou CHKDSK;

2.2.5.18.2. Executar uma verificação de vírus;

2.2.5.18.3. Copiar pastas ou arquivos em um local alternativo;

2.2.5.18.4. Exibir informações do disco sobre a unidade tal como espaço usado e o espaço livre;

2.2.5.19. Deve ter a capacidade de configurar a taxa máxima de transmissão utilizada via rede durante a criação do ponto de recuperação quando salvo na rede;

2.2.5.20. Deve ter a capacidade de especificar quais mensagens da solução (erros, avisos e informações) serão registradas conforme ocorrerem, determinar onde o arquivo é armazenado, fornecer informações úteis sobre o status dos jobs de backups, dos eventos relacionados, podendo ainda configurar emissão de alertas via e-mail;

2.2.5.21. Deve ter a capacidade de executar comandos durante, no mínimo, um dos seguintes estágios da criação de um ponto de recuperação:

2.2.5.21.1. Antes da captura dos dados;

2.2.5.21.2. Depois da captura dos dados;

2.2.5.21.3. Depois da criação de pontos de recuperação;

2.2.5.22. Deve ter a capacidade de usar senha e criptografia AES de 128, 192 ou 256 bits para proteger o ponto de recuperação contra acesso e uso não autorizados;

2.2.5.23. Deve ter a capacidade de identificar discos externos pelo seu GUID (Globally Unique IDentifier), indiferentemente da letra do drive assinalada pelo Windows, mesmo que a letra do disco seja alterada, o backup deverá ser concluído com sucesso;

2.2.5.24. Deve permitir restaurar um computador a partir de um local remoto, utilizando a opção de "inicialização do ambiente de recuperação" no menu de inicialização do Windows;

2.2.5.25. Deverá permitir copiar sistema operacional, aplicativos e dados de uma unidade de disco rígido para outra unidade;

2.2.5.26. Deverá integra-se com mecanismo de busca (Google Desktop e Microsoft Windows Search) gerando assim um catálogo de todos os arquivos contidos dentro do ponto de recuperação facilitando a pesquisa de arquivos inclusos no ponto de recuperação;

2.2.5.27. Deve permitir restaurar os pontos de recuperação para ambientes virtualizados, suportando no mínimo:

2.2.5.27.1. VMware Workstation 5, e 6;
2.2.5.27.2. VMware ESX Server 3.5 e 4.0;
2.2.5.27.3. VMware ESXi Server 3.5 e 4.0;
2.2.5.27.4. VMware Server 10 e 2.0;
2.2.5.27.5. Vmware Vsphere 4;
2.2.5.27.6. Microsoft Hyper-V;
2.2.5.27.7. Citrix Xen Server 4 e 5;

2.2.6. Funcionalidade de detecção Proativa de reconhecimento de novas ameaças com as funcionalidades

2.2.6.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

2.2.6.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;

2.2.6.3. Capacidade de detecção keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade

distintas da detecção;

2.2.6.4. Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;

2.2.6.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;

2.2.6.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Pró-Ativa com a base de reputação do fabricante;

2.2.6.7. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

2.2.6.8. Possibilidade de agendar o escaneamento da detecção Pró-Ativa com periodicidade mínima por minuto e em todos os novos processos;

2.2.6.9. Possibilidade de agendar o escaneamento da detecção Pró-Ativa com periodicidade mínima por minuto e em todos os novos processos;

2.2.7. Funcionalidade de Controle de Dispositivos e Aplicações

2.2.7.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

2.2.7.2. Controlar o uso de dispositivos com comunicação infravermelho, firewire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;

2.2.7.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;

2.2.7.4. Gerenciamento integrado à console de gerência da solução;

2.2.7.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;

2.2.7.6. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

2.2.8. Relatórios e Monitoramentos com as funcionalidades

2.2.8.1. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

2.2.8.1.1. As 10 máquinas com maior ocorrência de códigos maliciosos;

2.2.8.1.2. Os 10 usuários com maior ocorrência de códigos maliciosos;

2.2.8.1.3. Localização dos códigos maliciosos;

2.2.8.1.4. Sumários das ações realizadas;

2.2.8.1.5. Número de infecções detectadas diário, semanal e mensal;

2.2.8.1.6. Códigos maliciosos detectados.

2.2.9. Suporte a clientes Mac OS X

2.2.9.1. O cliente para instalação em estações de trabalho e servidores deverá

possuir compatibilidade com o sistema operacional Mac OS X para as funcionalidades de antivírus e anti-spyware.

2.2.9.2. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais Apple Mac OS X 10.5 (Leopard) e 10.6 (Snow Leopard), Mac Os X Server 10.5 e 10.6 em processadores 32 e 64 bits;

2.2.9.3. Suporte ao Apple Remote Desktop para instalação e atualização remota da solução;

2.2.9.4. Gerenciamento integrado à console de gerência da solução;

2.2.9.5. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.

2.2.9.6. Permitir que verificação das ameaças da maneira manual e agendada;

2.2.9.7. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

2.2.9.8. Permitir a ações de reparar arquivo ou quarentenar em caso de infeções a arquivos;

2.2.10. Console avançada de distribuição e relatórios

2.2.10.1. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;

2.2.10.2. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas versões;

2.2.10.3. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:

2.2.10.3.1. CA
2.2.10.3.2. ESET
2.2.10.3.3. F-Secure
2.2.10.3.4. Kaspersky
2.2.10.3.5. McAfee
2.2.10.3.6. Sophos
2.2.10.3.7. Symantec
2.2.10.3.8. Trend Micro

2.2.10.4. Permitir a remoção de outros softwares não desejados;

2.2.10.5. Criar tarefas de migração baseadas no resultado do inventário de antivírus;

2.2.10.6. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;

2.2.10.7. Possibilidade de recuperar instalação em clientes em caso de falha;

2.2.10.8. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot.

2.2.10.9. Os seguintes cubos devem ser disponibilizados para criação de relatórios:

2.2.10.9.1. Alertas;
2.2.10.9.2. Clientes;
2.2.10.9.3. Políticas;
2.2.10.9.4. Rastreamento;

2.2.10.10. Possibilidade de criação de indicadores de performance para medir

eficácia da solução de segurança;

2.2.10.11. Exportar os relatórios criados nos formados xls, pdf e html;

2.2.11. Funcionalidades do Controle de Acesso à Rede

2.2.11.1. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

2.2.11.1.1. Computador deve possuir antivírus, atualizados e ativo;
2.2.11.1.2. Computador deve possuir firewall ativo;
2.2.11.1.3. Computador deve possuir anti-spyware, atualizado e ativo;
2.2.11.1.4. Computador deve possuir patches instalados, ativos e atualizados;

2.2.11.2. Deve ter a capacidade de iniciar à auto-remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

2.2.11.3. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso a rede;

2.2.11.4. Deve possibilitar a verificação se o firewall pessoal esta instalado e inicializado na máquina;

2.2.11.5. Deve possibilitar as verificações customizadas, minimamente com operadores lógicos, "IF", "ELSE", "THEN", "AND", "OR e NOT", para no mínimo, os seguintes critérios:

2.2.11.5.1. Pesquisa de Chave de Registro (Chave e DWORD);
2.2.11.5.2. Versão do Sistema Operacional;
2.2.11.5.3. Idioma do Sistema Operacional;
2.2.11.5.4. Patch instalado;
2.2.11.5.5. Comparar versão, data, tamanho e "fingerprint" de arquivos;
2.2.11.5.6. Além dos quesitos onde mencionam verificações de Firewall e Antivírus nos itens e subitens acima;

2.2.11.6. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não utilizam o agente (Máquinas não gerenciadas);

2.2.11.7. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre maquinas que não estiverem em conformidade com as políticas do controle de acesso à rede;

2.2.12. Proteção na Mensageria

2.2.12.1. Deve ser compatível com os sistemas operacionais Windows Server 2003 e Windows Server 2008, ambos em 32bits e 64bits;

2.2.12.2. Deve suportar Cluster Ativo/passivo da solução Exchange;

2.2.12.3. Deve ser compatível com Exchange Server 2007, 2010 e 2013;

2.2.12.4. Deve ser compatível com VSAPI versões 2.0, 2.5 e 2.6;

2.2.12.5. Deve ser compatível com ambientes virtuais Vmware e Hyper-V;

2.2.12.6. Deve permitir instalação remota;

2.2.12.7. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para especifica mensagem, sem necessidade de integração com produtos de terceiros ou "open source";

2.2.12.8. Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior, em todos os appliances /equipamentos da solução ofertada;

2.2.12.9. Deve permitir realizar o rastreamento da mensagem, conforme citado anteriormente, utilizando caracteres double-byte para líguas estrangeiras;

2.2.12.10. Deve possuir funcionalidade de criação de Alias e Mascaramento de endereço;

2.2.12.11. Deve ser possível realizar notificação do administrador por email caso os filtros antispam não recebam atualizações por um determinado período de tempo;

2.2.12.12. Deve ser capaz de integração com LDAP Microsoft Active Directory 2003, Microsoft Active Directory 2008 e Lotus Domino 6.5 ou superior para sincronização e autenticação;

2.2.12.13. Deve permitir a criação de políticas diferenciadas para tratamento de SPAM, Virus, Filtragem de Conteúdo e Controle de reputação (traffic shaping), de acordo com o destinatário da mensagem e reputação de origem;

2.2.12.14. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento do usuários válidos e ações de Virus, Spam e Filtragem de Conteúdo diferenciadas por grupo do LDAP;

2.2.12.15. Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico, sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;

2.2.12.16. Deve possuir mecanismos de backup/restore da configuração existente na solução;

2.2.12.17. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;

2.2.12.18. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:

- **2.2.12.18.1.** Apagar mensagem;
- **2.2.12.18.2.** Enviar para Quarentena;
- **2.2.12.18.3.** Encaminhar mensagem;
- **2.2.12.18.4.** Encaminhar em BCC;
- **2.2.12.18.5.** Gravar mensagem em disco;
- **2.2.12.18.6.** Gravar em pasta de conformidade;
- **2.2.12.18.7.** Modificar o assunto;
- **2.2.12.18.8.** Adicionar informações ao cabeçalho;
- **2.2.12.18.9.** Deferir a mensagem;

2.2.12.18.10. Rejeitar a mensagem;

2.2.12.19. Deve ter a capacidade de verificação em tempo real de SMTP;

2.2.12.20. Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;

2.2.12.21. Deve ter a capacidade de verificação manual dos message stores;

2.2.12.22. Deve ter a capacidade de verificação agendada dos message stores;

2.2.12.23. Deve permitir verificar mailbox stores e public foldes;

2.2.12.24. Deve permitir definir a "idade mínima" das mensagens a serem verificadas;

2.2.12.25. Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:

2.2.12.25.1. Tempo máximo de verificação;

2.2.12.25.2. Número máximo de decomposição de arquivos compactados recursivamente;

2.2.12.25.3. Tamanho máximo do arquivo descompactado;

2.2.12.26. Número máximo de arquivos descompactados;

2.2.12.27. Deve ser capaz de quando a mensagem for gravada em pasta de conformidade, permitir definir ações distintas para as mensagens aprovadas e reprovadas;

2.2.12.28. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;

2.2.12.29. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);

2.2.12.30. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);

2.2.12.31. Deve possuir centro especializado, 24x7, com monitoramento de mais de 2 milhões de mailboxes, para processamento de SPAMs recebidos e criação automática de novos filtros/assinaturas;

2.2.12.32. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;

2.2.12.33. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;

2.2.12.34. Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);

2.2.12.35. Deve ter a capacidade de reconhecimento de ameaças Dia-Zero, com assinatura de suspeitos de vírus;

2.2.12.36. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:

2.2.12.36.1. Assinaturas para corpo da mensagem e anexos;

2.2.12.36.2. Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;

2.2.12.36.3. Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramente do fornecedor da solução);

2.2.12.36.4. Identificação de idiomas;
2.2.12.36.5. Filtros de URLs;
2.2.12.36.6. Filtros anti-phishing;

2.2.12.37. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;

2.2.12.38. Deve permitir a criação de "compliance folders", para armazenagem de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo Administrador;

2.2.12.39. Deve possuir tecnologia para detecção de ataques de Spam, Vírus e Diretório (Usuários Inválidos);

2.2.12.40. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;

2.2.12.41. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o controle do percentual de mensagens que serão recusadas;

2.2.12.42. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;

2.2.12.43. Deve possuir tecnologia para prevenção de ataques de "Bounce Messages";

2.2.12.44. Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;

2.2.12.45. Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;

2.2.12.46. Deve possuir a capacidade para criação de regras baseada na detecção por "Wildcard";

2.2.12.47. Deve possuir a capacidade para criação de regras baseada na detecção por expressões regulares;

2.2.12.48. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);

2.2.12.49. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;

2.2.12.50. Deve ter capacidade de detecção a pelo menos 10 idiomas (incluindo Português), permitindo o bloqueio de mensagens escritas nos idiomas não desejados;

2.2.12.51. Deve possuir capacidade de criar uma lista de IP's confiáveis baseado no comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;

2.2.12.52. Deve possuir a capacidade de atualização automática periódica da lista de IP's confiáveis, citada no item anterior;

2.2.12.53. Deve ter a capacidade de deleção total de mensagens enviadas por "Mass-Mailing Worms", com opção de ações diferenciadas por tráfego de entrada e saída;

2.2.12.54. Deve ter a capacidade de reconhecimento de Spywares e Adwares;

2.2.12.55. Deve possuir recurso para detecção dos ataques de duas escalas para Vírus e Diretório (LDAP), capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;

2.2.12.56. Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;

2.2.12.57. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo;

2.2.12.58. Deve ter a capacidade de implementar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;

2.2.12.59. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena (digest);

2.2.12.60. Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

2.2.12.61. Deve permitir que o usuário cadastre endereços de e-mail em listas negras/listas brancas pessoais;

2.2.13. Solução de Proteção, Segurança e Controle de Smartphones e Tablets e Aplicações em Mobile

2.2.13.1. A solução deve ter integração nativa entre os módulos de "MDM – Mobile Device Management" e "MAM – Mobile Application Management", possibilitando segurança do dispositivo, aplicações e proteção de dados em um único ponto;

2.2.13.2. O licenciamento da solução de mobilidade deve ser realizado por usuário independente do quantitativo de dispositivos, caso o licenciamento não possibilite este tipo de contabilidade deverá prever uma utilização média de 5 dispositivos por usuário de rede;

2.2.13.3. A solução deve ter a capacidade de entregar políticas e conteúdos de forma dinâmica, sem a necessidade de reinstalação das aplicações e aplicativos;

2.2.13.4. Deve ter a capacidade de a partir de um único ponto e de uma única conta de administração da solução, executar tarefas de administração do software, distribuição de aplicações e aplicativos;

2.2.13.5. A solução deve ter a capacidade de implementar funcionalidades de segurança na navegação através de uma proteção no navegador (Web Browser Protection) e Firewall Statefull, coibindo a navegação em sites fraudulentos;

2.2.13.6. A solução deverá ter a capacidade de implementar, no mínimo:

2.2.13.7. Gerenciamento de dispositivos;

2.2.13.8. Protecão de Dados e Aplicativos;

2.2.13.9. Proteção contra ameaças;

2.2.13.10. Gerenciamento de Acesso de usuários e aplicações;

2.2.13.11. A solução deve prover de forma nativa segurança de e-mail para iOS e Android, provendo no mínimo:

2.2.13.11.1. Separação dos dados privados de dados corporativos para cada usuário;

2.2.13.11.2. Bloqueando tarefas de cópia e cola entre aplicações de e-mails e também para outras aplicações;

2.2.13.11.3. Ter capacidade de implementar à funcionalidade, com e sem, a necessidade de agente;

2.2.13.11.4. Capacidade de permitir e restringir que anexos seja abertos em aplicativos sem autorização;

2.2.13.11.5. Limpeza seletiva dos dados contidos no e-mail seguro;

2.2.13.11.6. Controlar o tamanho dos anexos nas mensagens;

2.2.13.11.7. Possibilitar criptografia no mínimo AES-256, para todos os dados incluindo cartões de memória;

2.2.13.12. A funcionalidade de segurança no e-mail deve ter capacidade de gerenciamento de senha, para no mínimo:

2.2.13.12.1. Tamanho da senha;

2.2.13.12.2. Exigir complexidade de senha;

2.2.13.12.3. Não permitir a reutilização de senhas recentes ;

2.2.13.12.4. Controlar o tempo de validade das senhas;

2.2.13.12.5. Bloqueio;

2.2.13.13. A solução deve ter a capacidade de distribuir seus agentes de forma nativa, sem a necessidade de módulos complementares, possibilitando o auto-atendimento por parte dos usuários finais;

2.2.13.14. Deve ter a capacidade de executar procedimentos "Self-Healing", com o intuito de minimizar as tarefas administrativas, diminuindo tempo de suporte com tarefas padronizadas;

2.2.13.15. Deve ter a capacidade de executar de forma automática, sem a necessidade nenhum script e agentes externos ao software, a reparação, correção e falta de aplicações nos dispositivos móveis gerenciados;

2.2.13.16. Deve ter a capacidade de executar procedimentos para gerenciamento de configuração, para no mínimo:

2.2.13.16.1. Contas de E-mail;

2.2.13.16.2. VPN;

2.2.13.16.3. Wi-Fi;

2.2.13.17. Deve ter a capacidade de gerir políticas de senhas, forçado a aplicação de senha forte, contendo letras, números e caracteres;

2.2.13.18. Deve ter a capacidade de restringir o acesso por parte do usuário às políticas aplicadas no dispositivo móvel;

2.2.13.19. Deve ter a capacidade de limpar (Wipe) os dados dos dispositivos móveis, para no mínimo:

2.2.13.19.1. Limpeza somente de dados corporativos;

2.2.13.19.2. Limpeza completa de dados;

2.2.13.19.3. Limpeza dos cartões de memória dos dispositivos móveis;
2.2.13.19.4. Limpeza dos contatos;
2.2.13.19.5. Limpeza dos SMS;
2.2.13.19.6. Limpeza do histórico de navegação;
2.2.13.19.7. Limpeza dos marcadores de navegação;
2.2.13.19.8. Limpeza do histórico de chamadas;

2.2.13.20. Deve ter a capacidade debloqueio caso acuse a remoção do cartão SIM;

2.2.13.21. Deve ter a capacidade de bloquear de forma granular as ligações e mensagens SMS indesejáveis, mantendo o fluxo normal de chamadas e mensagens para aquelas fora da lista;

2.2.13.22. Deve ter a capacidade de identificar uma não conformidade com as políticas de configurações estabelecidas e consequentemente acarretar em um impedimento de acesso a rede gerenciada da instituição;

2.2.13.23. Deve ter a capacidade de identificar se o dispositivo sofreu alterações em suas configurações padrão ("Jailbreak") e executar uma ação de limpeza do dispositivo;

2.2.13.24. Deve permitir o acesso a rede gerenciada, somente de aparelhos em conformidade com as políticas da instituição;

2.2.13.25. Deve ter a capacidade de bloquear endereços URL's determinados pelas políticas pré-estabelecidas pela instituição;

2.2.13.26. Deve ter a capacidade de bloquear a utilização da câmera e cartões de memórias, conforme determinado pelas políticas pré-estabelecidas pela instituição;

2.2.13.27. Deve ter a capacidade de se integrar com certificados digitais padrão X-509;

2.2.13.28. Deve ter a capacidade de implementar autenticação de duplo fator para acesso a conexões de VPN e Wi-Fi;

2.2.13.29. Deve ter a capacidade de enviar informações para auditoria;

2.2.13.30. Deve ter a capacidade de integrar-se a ferramentas de Workflow;

2.2.13.31. Deve ter a capacidade de ser agnóstico ao serviço de e-mail, para no mínimo:

2.2.13.31.1. Microsoft Exchange 2003 / 2007 / 2010;
2.2.13.31.2. Lotus Notes;
2.2.13.31.3. Gmail;

2.2.13.32. Deve ter a capacidade de gerir no mínimo 20.000 dispositivos em um mesmo servidor de gerência;

2.2.13.33. Deve ter a capacidade de prover assistência remota;

2.2.13.34. Deve ter a capacidade de implementar, no mínimo, as seguintes funcionalidades:

2.2.13.34.1. Segurança com Conformidade;
2.2.13.34.2. Implementar senha forte;
2.2.13.34.3. Wipe remoto;
2.2.13.34.4. Gestão de Aplicações;
2.2.13.34.5. Gestão de Configuração;
2.2.13.34.6. Autenticação de Usuários por OTP (One-Time Password);
2.2.13.34.7. Autenticação de Dispositivo via infraestrutura de chaves

públicas (PKI - Public Key Infrastructure);

2.2.13.34.8. Autenticação de Aplicativos;

2.2.13.34.9. Segurança de Mensagens;

2.2.13.34.10. Proteção contra Ameaças;

2.2.13.34.11. Gestão de Endpoints;

2.2.13.34.12. Service Desk;

2.2.13.34.13. Processos de Negócios;

2.2.13.34.14. Controle de Software e Funções;

2.2.13.34.15. Criptografia de E-Mail;

2.2.13.34.16. DLP de E-mail;

2.2.13.34.17. Segurança de Conteúdo;

2.2.14. Características Técnicas de Segurança nas Aplicações

2.2.14.1. Deve ter a capacidade de criar uma sessão de navegador seguro para aplicativos web corporativos. Entende-se por sessão de navegador seguro:

2.2.14.1.1. O cache, se houver, será criptografado;

2.2.14.1.2. Não será permitido o compartilhamento de dados entre o navegador e outros aplicativos, seja via copiar/colar e envio de arquivos;

2.2.14.2. Deve impedir que dados de aplicativos protegidos sejam enviados e adquiridos por dispositivos externos, incluindo cabo USB e cartões de memória;

2.2.14.3. Deve ter a capacidade de implementar restrições de copia, onde, a cópia de algum dado considerado como restrito, pode ser substituído por uma mensagem de advertência;

2.2.14.4. Deve ter a capacidade de aplicar restrições no compartilhamento de documentos;

2.2.14.5. Deve ter a capacidade de solicitar autenticação Online e Off-line para acesso aos aplicativos e conteúdos protegidos;

2.2.14.6. Deve ter a capacidade de destruir os dados, assim como, desabilitar a aplicação, no caso de bloqueio de conta;

2.2.14.7. Deve ter a capacidade de criptografar a área de armazenamento dos aplicativos e conteúdo protegidos, assim como, limpar os dados quando a aplicação é fechada;

2.2.14.8. Deve ter a capacidade de implementar restrições de uso, para no mínimo, bloqueio no compartilhamento de documentos;

2.2.14.9. Deve ter a capacidade de destruir dados e desabilitar aplicativos, quando identificadas anomalias nos sistemas operacionais dos dispositivos, para no mínimo, "Jailbroken" em iOS e "Rooted" em Android;

2.2.14.10. A solução deve prover funcionalidades de prevenção de perda de dados, criptografia e autenticação forte, aplicadas na camada de aplicação;

2.2.14.11. A solução deve prover políticas avançadas de proteção aplicativo, tais como:

2.2.14.11.1. Conectividade segura de aplicativos;

2.2.14.11.2. Autenticação de usuário;

2.2.14.11.3. Criptografia de dados;
2.2.14.11.4. Gravação de dados para o armazenamento local;
2.2.14.11.5. Compartilhamento de documentos;
2.2.14.11.6. Copiar e colar documentos;
2.2.14.11.7. Controle de acesso off–line;

2.2.14.12. A solução deve ter a capacidade de distribuir e identificar o dispositivo através de certificados, possibilitando implementar 802.1x aderente ao domínio de gerência, garantindo desta forma, que o dispositivo que receber o direito de navegar é um dispositivo confiável;

2.2.14.13. A solução deve ser capaz de, após identificado o dispositivo como confiável, conforme descrito no item anterior, identificar também o usuário deste dispositivo, utilizando para isto um duplo fator de autenticação, para no mínimo usuário e senha de domínio em conjunção com certificado digital ou autenticação através de dispositivo OTP;

2.2.14.14. A solução deve ter a capacidade de identificar aplicações corporativas que sejam confiáveis, permitindo o acesso aos dados corporativos e possibilitar desta forma, o bloqueio de aplicações;

2.2.14.15. O software deve ter a capacidade de implementar uma loja virtual de aplicativos de forma nativa, para no mínimo:

2.2.14.15.1. iOS com arquivos *.IPA
2.2.14.15.2. Android com arquivos *.APK
2.2.14.15.3. Blackberry com arquivos *.ZIP

2.2.14.16. Caso o cliente seja removido, deve destruir os dados e aplicativos protegidos;

2.2.14.17. Deve ter a capacidade de destruir os dados e desabilitar a aplicação, caso o servidor de gerencia não esteja conectado na rede corporativa, a ser determinado pelo administrador do produto;

2.2.14.18. Deve ter a capacidade de suportar iOS, Android e BlackBerry;

2.2.14.19. Deve ter a capacidade de implementar níveis diferente de acesso a console, para no mínimo, Administradores com permissão total e Gerentes, Desenvolvedores e Editores de aplicação, onde cada um tem permissão específica ao que for associado ao seu papel;

2.2.14.20. Deve ter a capacidade de implementar permissionamento baseado em usuários, grupo de usuários e papeis;

2.2.14.21. Deve ter a capacidade de bloquear o usuário caso ocorra o cruzamento de quantidade de tentativas em um determinado intervalo de tempo, ambos com possibilidade de configuração pelo administrador do produto;

2.2.14.22. Deve ter a capacidade de implementar políticas de senhas com no mínimo, tamanho mínimo de senha, tempo de troca de senha, histórico de últimas senhas, proibição de utilização dos nomes de usuário e e-mail na composição da senha, utilização de no mínimo um caractere maiúsculo, minúsculo, numeral, caractere especial e requerer que no mínimo os três primeiros caracteres sejam únicos na composição da senha;

2.2.14.23. Deve ter a capacidade de montar uma loja de aplicativos corporativos, os quais podem ser agrupados por categorias lógicas;

2.2.14.24. Deve ter a capacidade de possibilitar ao usuário acesso as aplicações endereçadas a ele;

2.2.14.25. Deve ter a capacidade de limpar somente os dados corporativos;

2.2.14.26. Deve ter a capacidade de habilitar políticas corporativas para utilização das aplicações sejam elas proprietárias, de terceiros e existentes nas lojas dos fabricantes dos dispositivos, para no mínimo, autenticação de usuários, criptografia de dados da aplicação, acesso off-line e compartilhamento de documentos, habilitar armazenamento local no dispositivo, restringir conexões de rede, sem a necessidade de utilização da SDK da aplicação para integração das funcionalidades com suas aplicações já desenvolvidas e em desenvolvimento;

2.2.14.27. Deve ter a capacidade de habilitar a coexistência de aplicações pessoais e aplicações corporativas, possibilitando a utilização de ambas ao mesmo instante, aplicando todas as diretivas de segurança que forem necessárias nas aplicações corporativas;

2.2.14.28. Deve ter a capacidade de proteger a aplicação e o seu conteúdo;

2.2.15. Solução para Investigação e Prevenção de Fuga das Informações

2.2.15.1. Deverá ser fornecido em formato de hardware dedicado (Appliance) ou Virtual Appliance;

2.2.15.2. Deve possuir módulos de detecção distintos, licenciados de forma independente, gerenciados por console única, para:

2.2.15.2.1. Localizar dados confidenciais armazenados em servidores de arquivos, intranets e bancos de dados;

2.2.15.2.2. Localizar dados confidenciais armazenados em desktops e laptops;

2.2.15.2.3. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP, capturando tráfego em modo promíscuo;

2.2.15.3. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas;

2.2.15.4. Toda política criada na solução deve ser única, compatível e válida para aplicação em qualquer um dos módulos (agente, monitor de rede, scanner de dado armazenado)

2.2.15.5. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:

2.2.15.5.1. Conteúdo detectado em arquivos e tráfego de rede (protocolos);

2.2.15.5.2. Remetente e destinatário de correio;

2.2.15.5.3. Tipo real (baseado em cabeçalho, não extensão), nome e tamanho do arquivo;

2.2.15.5.4. Protocolo de comunicação utilizado;

2.2.15.6. Deve permitir alterar a criticidade do incidente, baseado em valores de referência e limites configuráveis para, no mínimo:

2.2.15.6.1. Quantidade de dados expostos;

2.2.15.6.2. Dados específicos expostos;

2.2.15.6.3. Arquivos específicos expostos;

2.2.15.6.4. Remetente de correio específico;
2.2.15.6.5. Destinatário de correio específico;
2.2.15.6.6. Protocolo de comunicação utilizado;

2.2.15.7. Deve criar regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo serviço de diretório, seja AD (Active Directory) quanto LDAP;

2.2.15.8. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:

2.2.15.8.1. SOX;
2.2.15.8.2. PCI;
2.2.15.8.3. HIPAA;

2.2.15.9. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:

2.2.15.9.1. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR);
2.2.15.9.2. CAD (DWG, DXF, VSD, DGN);
2.2.15.9.3. Planilhas (XLS, XLSX, 123, SXC, ODS);
2.2.15.9.4. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
2.2.15.9.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);
2.2.15.9.6. Outros (PDF, MDB);
2.2.15.9.7. Deve ter a capacidade de criar um novo formato "TrueType", com base no cabeçalho do arquivo, para detectar um arquivo não compatível com a ferramenta;
2.2.15.9.7.1. Deve ser entregue pelo fornecedor ferramentas e metodologia para extração de cabeçalho com base em amostragem de arquivos;
2.2.15.9.7.2. As ferramentas e metodologia entregues, conforme item anterior, deve ser suficiente para que o Contratante execute de forma autônoma a criação do novo formato "TrueType", não será admitida, desta forma, a intervenção do fornecedor e fabricante;

2.2.15.10. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo;

2.2.15.11. Deve ter a capacidade de indexar através de impressão digital (hash) para dados estruturados e não-estruturados;

2.2.15.12. Deve ter a capacidade de definir o percentual do documento indexado para validar a detecção (por exemplo, 10% do documento indexado);

2.2.15.13. Deve ter a capacidade de normalizar todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "123-45-6789", "123456789", "123.45.6789", etc.);

2.2.15.14. Deve ter a capacidade de implementar a funcionalidade de discover tanto nas plataformas Windows como MacOS;

2.2.15.15. A comunicação entre os clientes e servidores de gerencia dos módulos de "Investigação e Prevenção de Fuga das

Informações" deve ser implementada via certificação digital;

2.2.15.16. A solução de "Investigação e Prevenção de Fuga das Informações" deve ser capaz de implementar monitoração e bloqueio de informações sensíveis sob a plataforma OWA – Outlook Web Access;

2.2.15.17. A solução de Deve possuir capacidade de detecção usando palavras e frases-chave totalmente configuráveis;

2.2.15.18. Deve possuir capacidade de colocar múltiplas palavras/frases em uma única regra de detecção;

2.2.15.19. Deve ter a capacidade nativa de detectar uma grande variedade de padrões de dados que representam dados confidenciais (por exemplo, CPFs, depósitos, dados da tarja magnética, IBAN)

2.2.15.20. Deve ter a capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, Canadá, Inglaterra, Alemanha, França, Itália, Espanha, Holanda, Suíça, Austrália, China, Coréia do Sul, Taiwan, Cingapura e Brasil;

2.2.15.21. Deve permitir detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido;

2.2.15.22. Deve ter a capacidade de excluir automaticamente faixas de números inválidos para tipos de dados específicos, como "ranges" de teste, para no mínimo, cartão de credito;

2.2.15.23. Deve possuir minimamente 60 modelos de políticas preexistentes que incluem palavras-chave e padrões de dados, para no mínimo, as principais normas internacionais HIPAA, PCI, SOX, Cobit, ISO 27002, FISMA e NSA;

2.2.15.24. A atividade de detecção deve ser realizada de forma distribuída, por cada um dos módulos da solução (servidores, agentes e monitores de rede), não podendo ser realizada pelo servidor de gerenciamento central;

2.2.15.25. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção;

2.2.15.26. Deve ter a capacidade de integrar diretamente com AD para criar regras de detecção de endpoint baseada em usuário e grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada;

2.2.15.27. Deve ter a capacidade de exportar e importar com facilidade as políticas existentes, pela interface gráfica do console;

2.2.15.28. Deve permitir ocultar certos dados, como informações de identidade do remetente, durante a visualização do Incidente na tela do Console, dependendo do nível de acesso dado ao operador da ferramenta, para no mínimo, os seguintes tópicos:

2.2.15.28.1. Endereço de e-mail;

2.2.15.28.2. Nome de usuário;

2.2.15.28.3. Proprietário do arquivo;

2.2.15.29. Deve permite criar funções de administração separadas, para dados armazenados e dados em uso, estejam na rede ou no endpoint, no mínimo para:

2.2.15.29.1. Administração dos servidores;
2.2.15.29.2. Administração de usuários;
2.2.15.29.3. Criação e edição de políticas;
2.2.15.29.4. Solução de incidentes;

2.2.15.30. Deve suportar a verificação de arquivos compactados recursivos (exemplo zip dentro de zip);

2.2.15.31. Deve suportar de forma comprovada em manual do produto a detecção de dados no idioma português brasileiro;

2.2.15.32. Deve suportar de forma comprovada em manual do produto a detecção de dados identificados para no mínimo 25 línguas européias ocidentais e asiáticas, dentre elas devem constar línguas de dois bytes como chinês, coreano e japonês;

2.2.15.33. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails;

2.2.15.34. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem;

2.2.15.35. Deve identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados;

2.2.15.36. Deve ser capaz de gerar incidentes para detecção apenas se após um determinado percentual de cópia do conteúdo for atingido;

2.2.15.37. Deve possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:

2.2.15.37.1. CPF;
2.2.15.37.2. CNPJ;
2.2.15.37.3. Cartões de Crédito;

2.2.15.38. Deve possibilitar a utilização de expressões regulares para identificação de conteúdo;

2.2.15.39. Deve ter a capacidade de detectar presença de conteúdo cifrado/criptografado;

2.2.16. Resposta a Incidentes

2.2.16.1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política;

2.2.16.2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações;

2.2.16.3. Deve ser possível a notificar automaticamente o remetente e o gerente ou superior hierárquico do usuário envolvido no incidente;

2.2.16.4. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

2.2.16.4.1. Bloqueio de mensagem;
2.2.16.4.2. Quarentena de arquivo;
2.2.16.4.3. Notificação ao usuário;

2.2.16.4.4. Bloqueio do acesso web, bloqueio de cópia e impressão;

2.2.16.5. Deve disponibilizar interface de resposta totalmente personalizável que permita combinações de várias ações de reparo e reação, através do acionamento de um único botão na interface gráfica do Incidente.

2.2.16.6. Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis;

2.2.16.7. Deve exibir todos os detalhes do incidente em uma única página;

2.2.16.8. Deve permitir destacar (highlight) na tela do incidente os dados confidenciais detectados;

2.2.16.9. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida ("preview") na tela do incidente, sem a necessidade de usar software externo;

2.2.16.10. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente;

2.2.16.11. Deve possibilitar a exibição na tela do Incidente no console um link que possibilite o download e a abertura destes itens usando um software externo;

2.2.16.12. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente;

2.2.16.13. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema (incluindo políticas, relatórios, funções e workflow) otimizadas para verticais das indústrias específicas;

2.2.16.14. A solução deve possuir integrada a console a funcionalidade de workflow para tratamento e escalação dos incidentes;

2.2.16.15. Deve ser possível utilizar no workflow características, para no mínimo: severidade, status, filas de tratamento e atributos dos incidentes;

2.2.16.16. As informações detectadas nos incidentes devem ser possíveis de ser visualizadas através da console de gerenciamento;

2.2.16.17. Deve ser possível ocultar a visualização de evidencias de acordo com o nível de permissão atribuído ao operador da ferramenta;

2.2.16.18. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente, para no mínimo:

2.2.16.18.1. Timestamp;
2.2.16.18.2. Método de detecção;
2.2.16.18.3. Remetente e destinatário;
2.2.16.18.4. Mensagens e anexos;
2.2.16.18.5. Protocolo e endereço IP;

2.2.16.19. Deve agregar diversos incidentes em um caso para investigação mais detalhada;

2.2.16.20. Deve possibilidade de exportar incidentes para formato HTML, de forma que não exista necessidade de credenciais de acesso a solução para visualização off-line das informações;

2.2.16.21. Deve segregar acesso aos incidentes de acordo com características, para no mínimo:

2.2.16.21.1. Unidade de negócio;

2.2.16.21.2. País;
2.2.16.21.3. Gerente do usuário envolvido;
2.2.16.21.4. Severidade;

2.2.17. Relatórios

2.2.17.1. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:

2.2.17.1.1. Timestamp;
2.2.17.1.2. Tamanho e data do arquivo;
2.2.17.1.3. Endereço IP de origem e destino;
2.2.17.1.4. Histórico de incidentes e detalhes;
2.2.17.1.5. Remetente e destinatário;

2.2.17.2. Deve fornecer relatórios de tendências com gráficos distribuídos em uma linha de tempo;

2.2.17.3. Deve exportar relatórios para formato HTML e CSV;

2.2.17.4. Deve agendar relatórios para envio automático através de e-mail (datas específicas e periodicamente);

2.2.17.5. Deve apresentar um painel ("dashboard") para visualização executiva dos relatórios;

2.2.17.6. Deve permitir gerar relatórios resumidos por níveis, agrupados, sumarizados e com capacidade de detalhamento (drill-down);

2.2.17.7. Deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP;

2.2.17.8. Deve ter a capacidade para configurar, salvar relatórios e painéis de visualização ("dashboards") personalizados por usuário;

2.2.17.9. Deve possibilitar a execução de relatórios em todo o histórico de incidentes armazenados na base de dados, via console web e via API;

2.2.18. Monitoramento de Rede

2.2.18.1. Deve fornecer opção para monitorar o tráfego de rede de forma passiva, em modo promíscuo, sem appliances in-line;

2.2.18.2. Deve classificar protocolos independente da porta TCP/IP utilizada;

2.2.18.3. Deve alertar em caso de sobrecarga e perda de pacotes para análise, inclusive mostrando a quantidade de pacotes perdidos;

2.2.18.4. Deve possuir escalabilidade para monitorar links com velocidade acima de Gigabit Ethernet;

2.2.18.5. Deve analisar protocolos de rede comuns utilizados em serviços, para no mínimo:
2.2.18.5.1. Web (HTTP / HTTPS);
2.2.18.5.2. Correio Eletrônico (SMTP / POP);
2.2.18.5.3. Transferência de arquivos (FTP / SFTP);
2.2.18.5.4. Instant Messaging;

2.2.18.6. Deve possibilitar a análise de outros protocolos através da especificação de portas utilizadas;

2.2.18.7. Deve determinar a quantidade de tráfego analisado;

2.2.18.8. Deve bloquear e-mails que violem políticas;

2.2.18.9. Deve alertar ao remetente e administrador em caso de bloqueio de e-mail;

2.2.18.10. Deve ter a capacidade de combinar o tráfego de IM (nativo) em sessões de longa duração;

2.2.18.11. Deve ter a capacidade de filtrar o tráfego da rede para inspeção, para no mínimo os seguintes pontos:

2.2.18.11.1. Segundo o protocolo;
2.2.18.11.2. Faixa de IP;
2.2.18.11.3. Remetente de e-mail
2.2.18.11.4. Destinatário de e-mail;

2.2.18.12. Deve fornecer estatísticas de tráfego detalhadas e resultados gerais de dados, para no mínimo:

2.2.18.12.1. Nº de mensagens;
2.2.18.12.2. Nº de incidentes;
2.2.18.12.3. Protocolo;
2.2.18.12.4. Resumo por hora;

2.2.18.13. Deve permitir bloquear, redirecionar e colocar em quarentena condicionalmente as mensagens SMTP, com base no conteúdo da mensagem;

2.2.18.14. Deve permitir bloquear condicionalmente as mensagens HTTP, com base no conteúdo da mensagem;

2.2.18.15. Deve remove condicionalmente o corpo da mensagem e anexos específicos em um e-mail da Internet e também ações HTTP POST;

2.2.18.16. O produto não deve requer o uso de MTA ou proxy web incorporados, permitindo usar os produtos já existentes no ambiente;

2.2.18.17. Deve permitir integração com gateway de criptografia de e-mail para uma criptografia de e-mail condicional de acordo com o conteúdo, compatível no mínimo com:

2.2.18.17.1. PGP;
2.2.18.17.2. PostX;
2.2.18.17.3. Zix;
2.2.18.17.4. Voltage;
2.2.18.17.5. Tumbleweed;

2.2.18.18. Deve permitir bloqueio de e-mail implementado em uma arquitetura reflexiva (MTA único) e de encaminhamento (MTA múltiplo);

2.2.18.19. Deve permitir inspecionar mensagens criptografadas por TLS;

2.2.18.20. Deve permitir usar registros DNS MX para balancear carga e tolerância a falhas;

2.2.18.21. Deve gerenciar conflitos de políticas, fornecendo diferentes regras de gerenciamento para várias políticas;

2.2.18.22. Deve suporta instalar o módulo de prevenção de rede em uma máquina virtual VMware;

2.2.18.23. Deve ter a capacidade de integrar-se a no mínimo os seguintes MTAs abaixo, para análise e controle de e-mail:

2.2.18.23.1. CipherTrust;
2.2.18.23.2. IronPort;
2.2.18.23.3. Postfix;
2.2.18.23.4. Symantec BrightMail;
2.2.18.23.5. Proofpoint;
2.2.18.23.6. Sendmail;
2.2.18.23.7. SonicWall;
2.2.18.23.8. Tumbleweed;

2.2.18.24. Deve bloquear e remover conteúdo em transmissões de protocolos HTTP e FTP através da integração de no mínimo os seguintes proxies:

2.2.18.24.1. Blue Coat ProxySG;
2.2.18.24.2. Cisco CE 5.2.3;
2.2.18.24.3. NetCache 6.0;
2.2.18.24.4. MS ISA Server;

2.2.18.25. Deve bloquear transmissões de conteúdo confidencial cifrado por HTTPS e SSL da integração com Blue Coat ProxySG;

2.2.19. Monitoramento de Storage

2.2.19.1. Deve verificar existência de conteúdo confidencial em file systems para no mínimo CIFS, NFS, DFS, SMB, Novell, NTFS, ext2 e HFS;

2.2.19.2. Deve permitir a análise dos file systems sem a necessidade de agentes nos servidores de origem;

2.2.19.3. Deve permitir a análise dos file systems através de agentes em sistemas operacionais, para no mínimo:

2.2.19.3.1. AIX;
2.2.19.3.2. Linux;
2.2.19.3.3. Solaris;
2.2.19.3.4. Windows 2003;

2.2.19.4. Deve analisar conteúdo armazenado em ambientes complexos, para no mínimo:

2.2.19.4.1. Microsoft Sharepoint;
2.2.19.4.2. Lotus Notes;
2.2.19.4.3. Microsoft SQL Server;
2.2.19.4.4. Oracle;
2.2.19.4.5. Webservers;
2.2.19.4.6. Microsoft Exchange;
2.2.19.4.7. Documentum;
2.2.19.4.8. Live Link;

2.2.19.5. Deve possuir API para permitir a verificação de repositório de dados;

2.2.19.6. Deve permitir coleta automática de arquivos que violem políticas para análise legal (legal holding);

2.2.19.7. Deve ter a capacidade de criar respostas personalizadas para os incidentes gerados pela detecção em dados armazenados;

2.2.19.8. Deve copiar os arquivos encontrados que violem políticas;

2.2.19.9. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário;

2.2.19.10. Deve notificar através de e-mail e alerta Syslog em caso de violação de política;

2.2.19.11. Deve exibir nos incidentes e relatórios informações, no mínimo de:

2.2.19.11.1. Nome e tamanho do arquivo;

2.2.19.11.2. Dono do arquivo;

2.2.19.11.3. Localização e permissões;

2.2.19.12. Deve ser capaz de determinar os proprietários ("owners") de arquivos com dados confidencias dentro de repositórios NAS (Network-Attached Storage);

2.2.19.12.1. Devido à quantidade de usuários e processos que acessam arquivos e dispositivos, o produto deve ser capaz de identificar os usuários reais, que de fato utilizam o arquivo e dispositivo;

2.2.19.12.2. Deve ser capaz de identificar os "N" últimos usuários a acessar um determinado arquivo, "X" configurável;

2.2.19.12.3. Deve integrar-se ao dispositivo NAS (Network-Attached Storage) via API nativa;

2.2.19.12.3.1. Netapp;

2.2.19.12.3.2. EMC Celerra;

2.2.19.12.4. Deve ser compatível com dispositivos:

2.2.19.12.4.1. Netapp;

2.2.19.12.4.2. EMC Celerra;

2.2.19.13. Deve-se poder filtrar os usuários "não humanos" (usuários de serviços) na determinação dos donos reais dos arquivos;

2.2.19.14. Deve permitir agendamento constante das verificações de violação de política nos file systems;

2.2.19.15. Deve possibilitar configuração de janelas de tempo para pausar verificações;

2.2.19.16. Deve utilizar técnicas de paralelismo e controle de banda;

2.2.19.17. Deve configurar e controlar todas as varreduras a partir de um único console centralizado;

2.2.19.18. Deve permitir aplicar filtros para verificar na varredura arquivos de um determinado tipo ou em certo diretório;

2.2.19.19. Deve permitir aplicar filtros para ignorar na varredura arquivos de um determinado tipo ou em certo diretório;

2.2.19.20. Deve permitir realizar verificações incrementais em apenas arquivos novos e em arquivos alterados;

2.2.19.21. Deve permitir aplicar filtros para verificar arquivos adicionados, acessados e modificados entre determinadas datas;

2.2.19.22. Deve preservar os atributos do arquivo, inclusive o atributo "acessado em" após realizar a varredura;

2.2.19.23. Deve permitir agendamento de varreduras automáticas;

2.2.19.24. Deve ter a capacidade de interromper e pausar manualmente a verificação;

2.2.19.25. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado;

2.2.19.26. Deve permite limitar o uso da largura de banda da rede;

2.2.19.27. Deve ter a capacidade de definir número limite de incidentes para interromper varreduras;

2.2.19.28. Deve ter a capacidade de executar múltiplas verificações contra múltiplos alvos físicos ao mesmo tempo;

2.2.19.29. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados;

2.2.19.30. Deve ter a capacidade de executar varredura de sistemas em locais remotos, com largura de banda limitada;

2.2.19.31. Deve permitir varreduras com e sem o uso de agentes;

2.2.19.32. Deve suportar rodar o produto de varredura em máquina virtual VMware ESX e servidor real;

2.2.19.33. Deve permitir limitar portas de comunicação entre sistema-alvo e servidor de varredura;

2.2.19.34. Não deve impor requisitos de DLL e SO para o sistema verificado;

2.2.20. Monitoramento em Estações de Trabalho

2.2.20.1. O cliente para instalação em estações de trabalho deverá possuir compatibilidade, no mínimo, com os sistemas operacionais:

2.2.20.1.1. Windows XP;
2.2.20.1.2. Windows 2003;
2.2.20.1.3. Windows Vista;
2.2.20.1.4. Windows 7, em versões 32 e 64 bits;
2.2.20.1.5. Citrix **XenApp;**
2.2.20.1.6. **Citrix XenServer**;

2.2.20.2. Deve permitir a distribuição do agente através de ferramentas de terceiros, no mínimo:

2.2.20.2.1. Microsoft System Center;
2.2.20.2.2. IBM Tivoli;
2.2.20.2.3. Symantec Altiris;

2.2.20.3. O agente deve possuir mecanismos para evitar que o usuário interrompa os serviços do agente;

2.2.20.4. Deve ter a capacidade de monitorar e bloquear tentativas de cópia de conteúdo confidencial para no mínimo os dispositivos:

2.2.20.4.1. Drives USB;
2.2.20.4.2. CD/DVD;
2.2.20.4.3. Impressoras e fax;

2.2.20.5. Deve monitorar tentativas de cópia de conteúdo confidencial para o disco rígido;

2.2.20.6. Deve identificar a movimentação de fragmentos de informações confidenciais mesmo através de operações do tipo "copiar e colar" em tipos de documentos diferentes, para no mínimo:

2.2.20.6.1. Arquivos de editores de texto *.doc e *.docx para e-mail;

2.2.20.6.2. Arquivos de planilhas eletrônicas *.xls e *.xlsx para arquivos de apresentações *.ppt e *.pptx;

2.2.20.7. Atualizações dos agentes devem ser enviadas diretamente pela console de gerenciamento;

2.2.20.8. Deve exibir alerta "pop-up" na tela do usuário em caso de violação de política;

2.2.20.8.1. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em "pop-up", escolhendo opções de justificativa configuráveis pelo administrador da ferramenta, reportando para a console de gerenciamento, categorizadas no console para posterior geração de relatórios por categoria de justificativa;

2.2.20.8.2. Deve para um grupo pré-determinado de usuários ("VIPs") permitir o envio de informação confidencial, apresentando um "pop-up" de alerta quanto da criticidade da informação e solicitando confirma da ação, a qual deve ser logada na console central;

2.2.20.9. Todas as políticas devem estar ativas mesmo se a estação estiver fora da rede;

2.2.20.10. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial;

2.2.20.11. Deve permitir monitorar e bloquear transmissão HTTP;

2.2.20.12. Deve permitir monitorar e bloquear transmissão HTTPS, integrando-se a, no mínimo com os browsers;

2.2.20.12.1. Internet Explorer;

2.2.20.12.2. Mozilla Firefox;

2.2.20.13. Deve permitir monitorar e bloquear e-mails, integrando-se via plug-in ao cliente, no mínimo:

2.2.20.13.1. Microsoft Outlook;

2.2.20.13.2. Lotus Notes;

2.2.20.14. Deve permitir monitorar e bloquear transmissão FTP;

2.2.20.15. Deve permitir monitorar e bloquear dados enviados a um fax local e de rede;

2.2.21. Solução para Criptografia dos Dados

2.2.21.1. Configuração simples e intuitiva de opções de instalação e políticas do cliente

2.2.21.1.1. Configurações e políticas padrão do software cliente e instalação inclusas em um único pacote de instalação. Usa formato de instalação padrão (.MSI)

2.2.21.1.2. Capacidade de personalizar políticas de tempo de instalação para diferentes grupos de usuários

2.2.21.1.3. O software cliente pode ser distribuído e instalado usando

infraestrutura e processos existentes de distribuição de software

2.2.21.1.4. Metodologia de implementação de cliente escalável para atender aos planos projetados de implementação

2.2.21.1.5. Suporte à instalação silenciosa de software cliente

2.2.21.1.6. A instalação e configuração do software não deve requerer a criação de compartilhamentos de rede, nem outras mudanças na infraestrutura da rede local

2.2.21.1.7. A implementação do cliente deve requerer apenas 1 reinicialização no terminal, após a instalação

2.2.22. Opções de Políticas e Experiência do Usuário Final

2.2.22.1. Opção para tornar dispositivos removíveis de armazenamento somente para leitura até estarem criptografados

2.2.22.2. Opção para forçar a criptografia de dispositivos removíveis de armazenamento

2.2.22.3. Permitir que usuários apaguem, com segurança, o volume criptografado

2.2.22.4. Permitir que usuários preservem os dados existentes no volume criptografado

2.2.22.5. Os usuários criptografarão o volume com uma senha cuja força é determinada por uma política administrativa

2.2.22.6. O volume criptografado deve ser acessado em qualquer terminal válido da plataforma com a senha de criptografia definida pelo usuário

2.2.22.7. O recipiente da solução também deve poder ser descriptografado com uma chave de recuperação comandada por política

2.2.22.8. Permitir que o usuário crie discos virtuais da solução a partir de pastas em um disco rígido local

2.2.22.9. Os recipientes da solução podem ser gravados em CD/DVD

2.2.22.10. Os CDs/DVDs criptografados com a solução deve poder ser acessados em qualquer terminal válido da plataforma, com a senha de criptografia

2.2.22.11. Opção para permitir que os usuários alterem a senha da solução no primeiro uso. Isso permitirá que os administradores criem vários volumes criptografados e os dispersem para os usuários, conforme necessário, garantindo que serão criptografados com uma senha de usuário exclusiva

2.2.22.12. Permitir que usuários alterem a senha da solução para um determinado dispositivo por meio de um utilitário na bandeja do sistema

2.2.23. Confidencialidade e Sigilo da Informação na Rede

2.2.23.1. Permitir e Negar que usuários do terminal criem pastas da solução;

2.2.23.2. Permitir e Negar que usuários do terminal criptografem arquivos individuais com a solução;

2.2.23.3. Opção para forçar a criptografia de arquivos em pastas especificadas pelo administrador. Os arquivos nas pastas especificadas serão criptografados com a chave do usuário em cada terminal;

2.2.23.4. Opção para impedir a criptografia de arquivos em pastas especificadas

pelo administrador;

2.2.23.5. Opção para criptografar arquivos criados com aplicativos de usuário definidos pelo administrador. Todos os arquivos definidos serão criptografados com a chave do usuário;

2.2.23.6. Opção para impedir a criptografia de arquivos criados por aplicativos específicos, como soluções de backup e FTP;

2.2.23.7. A solução deve ser inicializada pelo menu iniciar e pelo ícone na bandeja do sistema

2.2.23.8. A funcionalidade da solução deve poder ser acessada pelo menu de contexto do Windows, clicando com o botão direito

2.2.23.9. O usuário deve poder criar uma pasta protegida da solução

2.2.23.10. O usuário deve poder adicionar usuários a uma pasta protegida da solução

2.2.23.11. Os usuários adicionados a uma pasta protegida devem poder receber vários níveis de controle de acesso

2.2.23.12. Usuários adicionais da pasta protegida devem poder adicionar outros usuários

2.2.23.13. O usuário deve poder remover a criptografia da solução de um arquivo específico se for o administrador da pasta

2.2.23.14. Os usuários da pasta da solução com permissão de administrador de grupo, ou administrador, podem remover o acesso de outros usuários à pasta criptografada da solução

2.2.23.15. Quando usuários forem removidos da lista de acesso de uma pasta, os arquivos ali contidos serão atualizados para refletir a mudança

2.2.23.16. Opção para importar lista de acesso de usuários de outra pasta protegida pela solução

2.2.23.17. Arquivos protegidos em uma pasta da solução mostrarão uma dica visual ao usuário final, na forma de um ícone de cadeado azul e branco, sobre o ícone normal do arquivo

2.2.23.18. Um usuário com a solução instalada, mas sem acesso a uma pasta específica, não poderá navegar pelo conteúdo de uma pasta protegida

2.2.23.19. Um usuário sem a solução instalada poderá navegar pelo conteúdo de uma pasta criptografada pela solução, mas não poderá ler os arquivos criptografados

2.2.23.20. As pastas da solução podem existir em um disco rígido local

2.2.23.21. As pastas da solução podem existir em um dispositivo removível de armazenamento

2.2.23.22. As pastas da solução podem existir em um servidor de arquivos na rede

2.2.24. Confidencialidade e Sigilo no E-Mail

2.2.24.1. O servidor de gerenciamento deve suportar o modelo "Soft Appliance" sendo instalado em uma seleção de hardware certificada e independente

2.2.24.2. O servidor de gerenciamento deve suportar as plataformas de virtualização VMWare ESX 3.5.0, 4.0, ESXi 3.5.0

2.2.24.3. Suportar criptografia forte e confiável baseada em padrões abertos e

protegidos de mensagens, OpenPGP e S/MIME

2.2.24.4. Suportar criptografia do corpo da mensagem e todos os anexos, além de suportar e também para várias codificações de conjuntos de caracteres

2.2.24.5. Suportar criptografia no gateway e ponto a ponto com política central para controlar o comportamento e a interoperação entre ambos

2.2.24.6. Suportar gerenciamento e publicação de chave central/certificados

2.2.24.7. Suportar criptografia ponto a ponto pela integração com o Outlook, Lotus Notes, baseados em IMAP/POP/SMTP

2.2.24.8. Suportar e integrar com o fluxo de mensagens do protocolo SMTP com filtragem de conteúdo e produtos DLP

2.2.24.9. Suportar a recuperação de chave baseada em política ou pela organização, que pode ser dividida para armazenamento e uso seguro

2.2.25. Servidor de Gerenciamento de Chave e Política

2.2.25.1. Suportar gerenciamento de chave e controle de políticas tanto para o e-mail do gateway (proxy SMTP) como para um cliente ponto a ponto opcional;

2.2.25.2. Suporte para estender a mesma plataforma/servidor de gerenciamento para controlar diversas necessidades adicionais de criptografia de clientes;

2.2.25.3. Suportar opções de políticas granulares de e-mail para ativar a segurança de mensagens e diferentes ações com base nos destinatários;

2.2.25.4. Suportar autenticação administrativa opcional de dois fatores;

2.2.25.5. Suportar funções administrativas;

2.2.25.6. Suportar múltiplos servidores de gerenciamento sincronizados para redundância, redirecionamento e escalabilidade;

2.2.25.7. Suportar agendamento automatizado e seguro do backup e opções integradas de recuperação;

2.2.25.8. Suportar registros detalhados, incluindo suporte para syslog remoto e relatórios integrados;

2.2.25.9. Suportar SNMP para monitoramento do sistema e alertas;

2.2.25.10. Suportar para hospedagem de um serviço de diretório de chave verificada para troca de chaves com parceiros e terceiros;

2.2.25.11. Suportar um repositório de chaves públicas hospedado por fornecedor para a troca e verificação de chaves com terceiros;

2.2.25.12. Suportar o uso do diretório existente LDAP para identidades de e-mail, autenticação e grupos de políticas;

2.2.25.13. Suportar gerenciamento automatizado de chave, como renovação, expiração e revogação, com suporte CRL integrado;

2.2.25.14. Suportar roteamento granular baseado em políticas para servidores de arquivo SMTP;

2.2.25.15. Suportar múltiplas opções flexíveis de distribuição de e-mail e os formatos de mensagem padronizados;

2.2.25.16. Suportar personalização/branding do portal baseado na web e para

todos os modelos de mensagens ;

2.2.25.17. Suportar geração automática de chaves e certificados e gerenciamento de ciclo de vida controlado por política administrativa;

2.2.25.18. Suportar integração com dispositivos Windows Mobile ;

2.2.25.19. Suportar integração com dispositivos BlackBerry por meio de pacotes de suporte para S/MIME;

2.2.25.20. Suportar política administrativa para permitir a redefinição de senhas de usuários externos do portal da web, de modo manual ou automático, via e-mail;

2.2.25.21. Suportar verificação automatizada de chaves e interoperação com outros parceiros que também usam a mesma solução do servidor central;

2.2.26. Instalação e Configuração do Cliente

2.2.26.1. Um único pacote MSI instala vários aplicativos de criptografia gerenciados por uma chave central e um servidor de políticas;

2.2.26.2. Criptografa, descriptografa, assina digitalmente e verifica mensagens de e-mail de modo automático e transparente, de acordo com políticas individuais ou de gerenciamento centralizado;

2.2.26.3. Quando implementado com uma solução de criptografia no gateway, o cliente pode distribuir mensagens de modo seguro para usuários externos que não possuem uma solução de criptografia de e-mail, independente do servidor de criptografia no gateway estar, ou não, no fluxo de e-mail;

2.2.26.4. Capacidade de impor políticas para usuários off-line controlando o que acontece com o e-mail quando o servidor de gerenciamento não pode ser alcançado pelo cliente de criptografia;

2.2.26.5. Capacidade de bloquear quais recursos estão habilitados, visíveis para o usuários e são obrigatórios - incluindo a criptografia manual opcional e botões que se integram com o Microsoft Outlook;

2.2.26.6. Opção administrativa para controlar a frequência com que um cliente recupera políticas atualizadas;

2.2.26.7. Capacidade de fornecer autenticação opcional de dois fatores usando smartcards, criando uma nova chave ou usando uma já existente;

2.2.26.8. As soluções de DLP e Criptografia devem ser exclusivamente do mesmo fabricante;

2.2.26.9. Permitir a integração das soluções de DLP com a solução de Criptografia de dados de forma nativa, sem necessidade de desenvolver qualquer tipo de programa, script, ou semelhante;

2.2.26.10. Garantir que quando um usuário executar uma cópia de arquivo para dispositivos removíveis, e este contenha informações confidenciais detectadas pelo DLP, o mesmo seja criptografado automaticamente através da solução de Criptografia para dispositivos móveis;

2.2.26.11. Garantir que quando um usuário executar uma cópia de arquivo para compartilhamento de rede, e este contenha informações confidenciais detectadas pelo DLP, o mesmo seja criptografado automaticamente

através da solução de Criptografia de compartilhamentos de rede;

2.2.26.12. Permitir que quando um usuário enviar um e-mail e este contenha informações confidenciais detectadas pelo DLP, o mesmo seja encaminhado automaticamente para o servidor de criptografia de mensagens. Este servidor irá efetuar a criptografia da mensagem confidencial e somente assim esta será encaminhada para os destinatários.

2.2.26.13. Garantir que os logs de segurança das soluções de DLP e Criptografia de dados sejam correlacionados através da solução de Gerenciamento de Trilhas de Auditoria e Eventos de Informações de Segurança.

2.2.27. Solução de Conformidade e Gerenciamento de Legados

2.2.27.1. Deve executar todas as funções através de um único agente, inclusive a verificação do endpoint e a monitoração e bloqueio de dados que saem do endpoint;

2.2.27.2. Deve permitir definir limites em % da CPU, disco, e a largura de banda utilizada pelo agente;

2.2.27.3. Deve gerenciar atualizações de software, políticas, logins, alertas e configurações por meio de um console centralizado;

2.2.27.4. Deve integrar-se com os drivers do Windows e em várias aplicações para garantir a estabilidade, atividade conjunta e segurança, não permitindo a utilização da abordagem de rootkit;

2.2.27.5. Deve possibilitar a verificação com base em agente permitindo execução simultânea em um número ilimitado de endpoints;

2.2.27.6. Deve permitir implementar as mesmas políticas para verificações com e sem agente;

2.2.27.7. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados;

2.2.27.8. Deve permitir gerar relatórios de progresso da verificação em tempo real;

2.2.27.9. Deve ter a capacidade de verificar e executar somente quando a máquina está inativa;

2.2.27.10. Ser capaz de descobrir qualquer dispositivo que possua um endereço IP atribuído (computador, servidor, impressora, roteador, *switch*, *hub* e outros) independente de fabricante ou fornecedor;

2.2.27.11. Ser capaz de descobrir dispositivos por meio do protocolo SNMP (Simple Network Management Protocol);

2.2.27.12. Permitir o descobrimento pelos métodos:

2.2.27.12.1. Range de IP através de subnets e VLANs;

2.2.27.12.2. Domínio;

2.2.27.13. Descobrimento de portas habilitadas (port scan);

2.2.27.14. Descobrimento de portas críticas, definidas pelo administrador, que estiverem habilitadas nos computadores;

2.2.27.15. Permitir a realização de inventário e descobrimento esporadicamente pelo administrador e automaticamente por meio de agenda flexível,

permitindo definir frequência e horário, sendo possíveis pelo menos os seguintes filtros:

2.2.27.15.1. IP e range de IP;

2.2.27.15.2. Comunidade SNMP;

2.2.27.16. Captura de inventário básico independente de uso de solução de inventário provisionando as seguintes informações gerais dos clientes:

2.2.27.16.1. *Hostname* e domínio;

2.2.27.16.2. Sistema operacional, idioma, diretório de instalação e sistema de arquivos;

2.2.27.16.3. Versão do sistema operacional e Service Pack;

2.2.27.16.4. Tipo do dispositivo (computador, móvel, dispositivo de rede);

2.2.27.16.5. Endereço Mac;

2.2.27.16.6. Configurações TCP/IP de todas as placas de rede incluindo virtuais;

2.2.27.16.7. Indicação de endereço: IP fixo ou dinâmico;

2.2.27.17. Captura de eventos de *logon* e *logoff* identificando usuário, domínio, data de *logon* e *logoff* e tempo total logado, independentemente se o computador estiver em domínio e se o *logon* for em domínio ou local, permitindo ao administrador identificar os usuários que estavam conectados no computador em determinado horário;

2.2.27.18. Execução do inventário através de políticas definidas na console central para dispositivos com agente;

2.2.27.19. Executar o inventário mesmo em computadores desligados, desde que estejam com alimentação de energia na fonte (cabo ligado na tomada) e conectados à rede, no mínimo das seguintes formas:

2.2.27.19.1. Ligar o computador, inicializar o sistema operacional e executar o inventário em computadores cuja placa de rede e BIOS suportem a tecnologia *wake-on-lan*;

2.2.27.19.2. Ligar o computador, inicializar o sistema operacional e executar o inventário em computadores que suportem a tecnologia vPro, desde que o seu processador seja compatível com a tecnologia vPro;

2.2.27.19.3. Dar suporte à definição de limite de tempo máximo para execução do inventário, provocando a interrupção do processo caso leve mais tempo que o limite definido;

2.2.27.20. Execução do inventário de forma silenciosa sem exibição de janela e sem requerer nenhuma ação para o usuário;

2.2.27.21. Inventário de pelo menos os seguintes tipos de informação de computadores Windows:

2.2.27.21.1. Processador, quantidade, velocidade e tipo/marca;

2.2.27.21.2. Tipo de computador: *desktop*, *laptop*, servidor ou outra classificação do fabricante;

2.2.27.21.3. Fabricante do *hardware*, modelo, número de série;