GOVERNO DO ESTADO DO PIAUÍ

AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

Processo nº 00117.001755/2019-32

1. OBJETO

Registro de Preço para contratação, SOB DEMANDA, de solução unificada de segurança para proteção de e-mail, proteção de Endpoint e proteção contra-ataques avançados, com garantia de 36 meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades dos órgãos e entes da Administração Pública, de acordo com as especificações técnicas contidas no Termo de Referência.

2. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

A ação de modernização do datacenter da ATI planejada e executada pela administração estadual preparou, com a aquisição de software, equipamentos e capacitação de pessoal, de forma a se tornar aderente a nova Lei de Proteção de Dados Pessoais (LGPD - Lei N° 13.709 de 14 de Agosto de 2018), e com ela os órgãos da administração direta estadual podem adotar, a fim de atender os requisitos de segurança para garantir a preservação de Dados Pessoais manipulados pelos órgãos estaduais.

O projeto de adequação a LGPD é um processo contínuo e de diversas frentes, além da mudança de cultura, do mapeamento de processos que manipulam os dados pessoais do cidadão e/ou servidores, ferramentas de monitoramento e de mitigação de invasões e de usos indevidos de dados.

3. ENQUADRAMENTO DA CONTRATAÇÃO

3.1 REGISTRO DE PREÇO NA MODALIDADE DE PREGÃO ELETRÔNICO - MENOR PREÇO POR LOTE - ADJUDICAÇÃO POR LOTE.

Será adotado o **Sistema de Registro de Preço modalidade Pregão Eletrônico** para o processo em questão, devido ao objeto deste Termo de Referência se enquadrar nos Incisos I e II do Art. 10º do Decreto Estadual nº 11.319/2004. Por se tratar de bem comum, com características e especificações usuais de mercado. O referido Pregão Eletrônico será realizado pela SEADPREV-I e a ATI-PI, como coparticipe.

A modalidade se faz necessária em virtude das mudanças de quantidade de pontos a serem instalados pelo novo modelo de gestão, o qual deverá ser prestado com base no mapeamento das subsecretarias, fato esse que poderá afetar diretamente na quantidade listada neste Termo de Referência, podendo ainda sofrer alterações quanto a localidade, sendo impossível prever com exatidão, justificando assim, a contratação dos serviços com criação de Registro de Preço.

3.2 DA CLASSIFICAÇÃO COMO SERVIÇO COMUM

O Objeto desta contratação de serviço se enquadra nos termos do parágrafo único, do art. 1º, da Lei nº 10.520, de 2002, com características e especificações usuais de mercado, podendo, portanto, ser solicitado por meio da modalidade de Pregão Eletrônico.

Embora a Lei do Pregão nos forneça um conceito do tipo aberto sobre o que sejam comuns, após analisar 03 (três) aspectos, quais sejam: a possibilidade de padronizar o objeto por meio de critérios objetivos de desempenho e qualidade comuns no mercado correspondente; se havia disponibilidade no mercado deste material, e, verificado se as especificações adotadas eram usuais neste mesmo mercado, a presente aquisição foi considerada comum e verificou-se que as especificações são usuais pelo mercado.

Os objetos deste termo de referência tratam-se de serviços comuns, cujos padrões de desempenho e qualidade podem ser objetivamente definidos no Termo de Referência, por meio de especificações usuais de mercado, nos termos do art. 1º, §1º da Lei nº 10.520/2002, c/c o art. 10º, I, II do Decreto Estadual nº 11.319/2004.

Entende que devido à padronização existente no mercado, os bens e serviços de Tecnologia da Informação geralmente atendem a protocolos, métodos e técnicas preestabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado.

A presente solicitação de contratação se classifica como execução de serviço de informática e automação, nos termos da Lei nº 8.248/91 e decreto estadual PI 14.631/11.

4. DESCRIÇÃO DETALHADA DO OBJETO

LOTE ÚNICO	DESCRIÇÃO	QTDE	MÉTRICA
1	Solução de segurança para Desktops (Endpoint)	8.100	Unidades

LOTE ÚNICO	DESCRIÇÃO	QTDE	MÉTRICA
2	Solução de segurança completa para Desktops (Completa)	8.100	Unidades
3	Solução de Segurança para ambiente virtualizado, datacenter e nuvem	825	Unidades
4	Solução de proteção contra ameaças avançadas – 4 Gbps	3	Unidades
5	Solução de anti-spam (gateway de e-mail)	5.100	Unidades
6	Proteção de Filtro WEB	5.100	Unidades
7	Pacote de Instalação (40 horas)	19	Pacotes
8	Treinamento (Hands-on) (40 horas)	17	Unidades
9	Operação assistida/HORAS (pacote de 40 horas)	20	Pacotes

4.1. **Item 1 - Solução de segurança para Desktops (Endpoint)**

4.1.1. **Módulo de proteção anti-malware**

4.1.1.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.1.1.1.1. Windows 7 (x86/x64);

4.1.1.1.2. Windows 8.1 (x86/x64);

4.1.1.1.3. Windows 10 (x86/x64).

4.1.1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

4.1.1.3. Deve ser integrada ao Windows Security Center, quando utilizado em plataforma Microsoft ft;

4.1.1.4. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

4.1.1.5. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

4.1.1.5.1. Processos em execução em memória principal (RAM);

4.1.1.5.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

4.1.1.5.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, Microsoft ft CAB;

4.1.1.5.4. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

4.1.1.6. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;

4.1.1.7. Deve possuir detecção heurística de vírus desconhecidos;

4.1.1.8. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

4.1.1.9. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

4.1.1.9.1. Em tempo real de arquivos acessados pelo usuário;

4.1.1.9.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

4.1.1.9.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

4.1.1.9.4. Por linha de comando, parametrizável, com opção de limpeza;

4.1.1.9.5. Automáticos do sistema com as seguintes opções:

4.1.1.9.5.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

4.1.1.9.5.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

4.1.1.9.5.3. Frequência: horária, diária, semanal e mensal;

4.1.1.9.5.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

4.1.1.10. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

4.1.1.11. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

4.1.1.12. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

4.1.1.13. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

4.1.1.14. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

4.1.1.15. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

4.1.1.16. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

4.1.1.17. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

4.1.1.18. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

4.1.1.19. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

4.1.1.20. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obscuração que o módulo de Machine Learning em pré-execução não consiga detectar;

4.1.1.21. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

4.1.1.22. Deve bloquear processos comuns associados a ransomware.

4.1.2. **Funcionalidade de atualização**

4.1.2.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

4.1.2.2. Deve permitir atualização incremental da lista de definições de vírus;

4.1.2.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

4.1.2.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

4.1.2.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

4.1.2.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

4.1.2.7. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

4.1.2.8. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

4.1.3. **Funcionalidade de administração**

4.1.3.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

4.1.3.2. Deve possibilitar instalação "silenciosa";

4.1.3.3. Deve permitir o bloqueio por nome de arquivo;

4.1.3.4. Deve permitir o travamento de pastas e diretórios;

4.1.3.5. Deve permitir o travamento de compartilhamentos;

4.1.3.6. Deve permitir o rastreamento e bloqueio de infecções;

4.1.3.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

4.1.3.8. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

4.1.3.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

4.1.3.10. Deve permitir a desinstalação através da console de gerenciamento da solução;

4.1.3.11. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

4.1.3.12. Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

4.1.3.13. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

4.1.3.14. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

4.1.3.15. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

4.1.3.16. Deve permitir a deleção dos arquivos quarentenados;

4.1.3.17. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

4.1.3.18. Deve permitir integração com Active Directory para acesso a console de administração;

4.1.3.19. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

4.1.3.20. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

4.1.3.21. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.1.3.22. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

4.1.3.23. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

4.1.3.24. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

4.1.3.25. Deve possuir solução de reputação de sites locais para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.1.3.26. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional

4.1.3.27. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

4.1.3.28. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

4.1.3.29. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

4.1.3.30. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

4.1.3.31. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

4.1.3.32. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

4.1.3.33. Deve permitir a criação de usuários locais de administração da console de anti-malware;

4.1.3.34. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

4.1.3.35. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

4.1.3.36. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

4.1.3.37. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

4.1.3.38. Deve permitir a gerência de domínios separados para usuários previamente definidos;

4.1.3.39. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

4.1.3.40. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

4.1.4. **Funcionalidade de controle de dispositivos**

4.1.4.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.1.4.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como: CD-ROM, DVD, com as opções de acesso total leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.1.4.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

4.1.4.4. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.1.4.5. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

4.1.5. **Módulo de proteção anti-malware para estações Linux**

4.1.5.1. Distribuições homologadas pelo fabricante:

4.1.5.1.1. SUSE Linux Enterprise 10 e 11;

4.1.5.1.2. Red Hat enterprise Linux 4.0, 5.0 e 6.0;

4.1.5.1.3. Centos 4.0, 5.0 e 6.0.

4.1.5.2. O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição Linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante;

4.1.5.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

4.1.5.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática nos sistemas operacionais;

4.1.5.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits e outros;

4.1.5.6. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

4.1.5.7. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

4.1.5.8. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

4.1.5.9. As mensagens exibidas aos usuários devem ser traduzidas para o Português do Brasil.

4.1.6. **Módulo de proteção anti-malware para estações macOS**

4.1.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

4.1.6.1.1. macOS 10.14 (Mojave) em processadores 32 e 64 bits;

4.1.6.1.2. macOS 10.13 (High Sierra) em processadores 32 e 64 bits;

4.1.6.1.3. macOS 10.12 (Sierra) em processadores 32 e 64 bits;

4.1.6.1.4. OS X 10.11 (El Capitan) em processadores 32 e 64 bits;

4.1.6.1.5. OS X 10.10 (Yosemite) em processadores 32 e 64 bits.

4.1.6.2. Suporte ao Apple Remote Desktop para instalação remota da solução;

4.1.6.3. Gerenciamento integrado à console de gerência central da solução

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

4.1.6.5. Permitir a verificação das ameaças da maneira manual e agendada;

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

4.1.6.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos;

4.1.6.8. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

4.1.6.9. Deve possuir no mecanismo de autoproteção as seguintes proteções:

4.1.6.9.1. Autenticação de comandos IPC;

4.1.6.9.2. Proteção e verificação dos arquivos de assinatura;

4.1.6.9.3. Proteção dos processos do agente de segurança;

4.1.6.9.4. Proteção das chaves de registro do agente de segurança;

4.1.6.9.5. Proteção do diretório de instalação do agente de segurança.

4.1.7. **Funcionalidade de HIPS – Host IPS e Host Firewall**

4.1.7.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

4.1.7.1.1. Windows 7 (x86/x64);

4.1.7.1.2. Windows 8.1 (x86/x64);

4.1.7.1.3. Windows 10 (x86/x64).

4.1.7.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

4.1.7.3. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

4.1.7.4. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

4.1.7.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

4.1.7.6. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

4.1.7.7. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

4.1.7.8. O modulo de IDS deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack;

4.1.7.9. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

4.1.7.10. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

4.1.7.11. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas.

4.1.8. **Módulo para controle de aplicações**

4.1.8.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.1.8.1.1. Windows 7 (x86/x64);

4.1.8.1.2. Windows 8.1 (x86/x64);

4.1.8.1.3. Windows 10 (x64).

4.1.8.2. As regras de controle de aplicação devem permitir as seguintes ações:

4.1.8.2.1. Permissão de execução;

4.1.8.2.2. Bloqueio de execução;

4.1.8.2.3. Bloqueio de novas instalações.

4.1.8.3. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,

4.1.8.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

4.1.8.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

4.1.8.5.1. Assinatura SHA-1 e SHA-256 do executável;

4.1.8.5.2. Atributos do certificado utilizado para assinatura digital do executável;

4.1.8.5.3. Caminho lógico do executável;

4.1.8.5.4. Base de assinaturas de certificados digitais válidos e seguros.

4.1.8.6. As regras de controle de aplicação devem possuir categorias pré-determininadas de aplicações;

4.1.8.7. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

4.1.8.8. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento.

4.1.9. **Módulo de proteção contra vazamento de informações – DLP**

4.1.9.1. Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais:

4.1.9.1.1. Windows 7 (x86/x64);

4.1.9.1.2. Windows 8.1 (x86/x64);

4.1.9.1.3. Windows 10 (x64).

4.1.9.2. Deve possuir nativamente templates para atender as seguintes regulamentações:

4.1.9.2.1. PCI/DSS;

4.1.9.2.2. HIPAA;

4.1.9.2.3. GLBA;

4.1.9.2.4. SB-1386;

4.1.9.2.5. US PII.

4.1.9.3. Deve ser capaz de detectar informações, em arquivos nos formatos:

4.1.9.3.1. Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtt, wordpad, text; xml, html;

4.1.9.3.2. Gráficos: visio, postscript, pdf, ff;

4.1.9.3.3. Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

4.1.9.3.4. Códigos: c/c++, java, verilog, autocad.

4.1.9.4. Deve ser capaz de detectar informações, com base em:

4.1.9.4.1. Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;

4.1.9.4.2. Palavras ou frases configuráveis;

4.1.9.4.3. Expressões regulares;

4.1.9.4.4. Extensão dos arquivos.

4.1.9.5. Deve ser capaz de detectar em arquivos compactados;

4.1.9.6. Deve permitir a configuração de quantas camadas de compressão serão verificadas;

4.1.9.7. Deve permitir a criação de modelos personalizados para identificação de informações;

4.1.9.8. Deve permitir a criação de modelos com base em regras e operadores lógicos;

4.1.9.9. Deve possuir modelos padrões;

4.1.9.10. Deve permitir a importação e exportação de modelos;

4.1.9.11. Deve permitir a criação de políticas personalizadas

4.1.9.12. Deve permitir a criação de políticas baseadas em múltiplos modelos;

4.1.9.13. Deve permitir mais de uma ação para cada política, como:

4.1.9.13.1. Apenas registrar o evento da violação;

4.1.9.13.2. Bloquear a transmissão;

4.1.9.13.3. Gerar alertar para o usuário;

4.1.9.13.4. Gerar alertar na central de gerenciamento;

4.1.9.13.5. Capturar informação para uma possível investigação da violação.

4.1.9.14. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;

4.1.9.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

4.1.9.15.1. Cliente de e-mail;

4.1.9.15.2. Protocolos http, https;

4.1.9.15.3. Mídias removíveis;

4.1.9.15.4. Discos óticos cd/dvd;

4.1.9.15.5. Gravação cd/dvd;

4.1.9.15.6. Aplicações de mensagens instantâneas;

4.1.9.15.7. Tecla de print screen;

4.1.9.15.8. Aplicações p2p;

4.1.9.15.9. Área de transferência do Windows;

4.1.9.15.10. Webmail;

4.1.9.15.11. Armazenamento na nuvem (cloud);

4.1.9.15.12. Impressoras;

4.1.9.15.13. Scanners;

4.1.9.15.14. Compartilhamentos de arquivos;

4.1.9.15.15. Activesync;

4.1.9.15.16. Criptografia PGP;

4.1.9.15.17. Disquete;

4.1.9.15.18. Portas com, lpt, firewire (ieee 1394);

4.1.9.15.19. Modems;

4.1.9.15.20. Infravermelho;

4.1.9.15.21. Bluetooth;

4.1.9.16. Deve permitir a criação de exceções nas restrições dos meios de transmissão.

4.1.10. **Módulo de criptografia**

4.1.10.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.1.10.1.1. Windows 7 (x86/x64);

4.1.10.1.2. Windows 8.1 (x86/x64);

4.1.10.1.3. Windows 10 (x64).

4.1.10.2. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

4.1.10.2.1. Disco completo (Full Disk);

4.1.10.2.2. Pastas e arquivos;

4.1.10.2.3. Mídias removíveis;

4.1.10.2.4. Anexos de e-mails;

4.1.10.2.5. Automática de disco.

4.1.10.3. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

4.1.10.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

4.1.10.5. Deve possuir suporte ao algoritmo de criptografia AES-256;

4.1.10.6. Deve possuir a capacidade de exceções para criptografia automática;

4.1.10.7. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

4.1.10.8. Deve possuir certificação FIPS 140-2;

4.1.10.9. Deve possuir funcionalidade de criptografia por software ou hardware;

4.1.10.10. Deve ser compatível com os padrões SED ('self-encrypting drive), OPAL e OPAL2;

4.1.10.11. Deve possuir compatibilidade de autenticação por múltiplos fatores;

4.1.10.12. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

4.1.10.13. Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

4.1.10.14. Deve possuir políticas por usuários, grupos e dispositivos;

4.1.10.15. Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

4.1.10.15.1. Sequência de cores;

4.1.10.15.2. Autenticação com AD;

4.1.10.15.3. Single sign-on com AD;

4.1.10.15.4. Senha pré-definida;

4.1.10.15.5. Número PIN;

4.1.10.15.6. Smart card.

4.1.10.16. Deve possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

4.1.10.17. Deve possuir mecanismos de criptografia transparentes para o usuário;

4.1.10.18. Deve possuir mecanismos para wipe (limpeza) remoto;

4.1.10.19. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

4.1.10.20. Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

4.1.10.21. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

4.1.10.22. Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

4.1.10.23. O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

4.1.10.24. O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

4.1.10.25. O ambiente de autenticação pré-inicialização deve permitir a mudança do *layout* do teclado;

4.1.10.26. O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

4.1.10.27. O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

4.1.10.28. Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (MBR – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades da solução de criptografia e visualizar, testar e modificar as configurações de rede;

4.1.10.29. O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

4.1.10.30. Deve prover ferramenta presente na estação de trabalho que possibilite migra-la para um servidor de gerenciamento diferente;

4.1.10.31. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

4.1.10.31.1. Microsoft Bitlocker;

4.1.10.31.2. Apple Filevault.

4.1.10.32. As capacidades de gerência das soluções terceiras de criptografia devem incluir:

4.1.10.32.1. Habilitar a criptografia;

4.1.10.32.2. Exibir o estado da criptografia (ativado, desativado);

4.1.10.32.3. Habilitar o aviso legal;

4.1.10.32.4. Editar o intervalo de sincronia.

4.1.10.33. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

4.1.10.34. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

4.1.10.35. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

4.1.10.36. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

4.1.10.37. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

4.1.10.38. Deve permitir a exibição de aviso legal quando a estação é inicializada;

4.1.10.39. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

4.1.10.40. Deve possibilitar que cada política tenha uma chave de criptografia única;

4.1.10.41. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

4.1.10.41.1. Chave do usuário: somente o usuário tem acesso aos arquivos;

4.1.10.41.2. Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

4.1.10.41.3. Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos.

4.1.10.42. Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

4.1.10.43. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

4.1.10.44. Deve possibilitar a desativação de dispositivos de armazenamento USB;

4.1.10.45. Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

4.1.10.46. Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

4.1.10.47. Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

4.1.10.48. Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

4.1.10.49. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

4.1.10.50. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

4.1.10.51. Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

4.1.10.52. Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

4.1.10.53. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

4.1.10.54. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

4.1.10.55. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.1.10.56. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

4.1.10.57. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação.

4.1.11. **Módulo de proteção para smartphones e tablets**

4.1.11.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

4.1.11.1.1. iOS;

4.1.11.1.2. Android.

4.1.11.2. As funcionalidades estarão disponíveis de acordo com cada plataforma;

4.1.11.3. Deve permitir o provisionamento de configurações de:

4.1.11.3.1. Wi-fi, Exchange Activesync, VPN, proxy HTTP global e certificados.

4.1.11.4. Deve possuir proteção de anti-malware;

4.1.11.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão SD e após atualização de vacinas;

4.1.11.6. Deve possuir capacidade de detecção de spam proveniente de SMS;

4.1.11.7. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

4.1.11.8. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

4.1.11.9. Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

4.1.11.10. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

4.1.11.11. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

4.1.11.12. Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

4.1.11.13. Controle da política de segurança de senhas, com critérios mínimos de:

4.1.11.13.1. Padrão de senha;

4.1.11.13.2. Uso obrigatório de senha;

4.1.11.13.3. Tamanho mínimo;

4.1.11.13.4. Tempo de expiração;

4.1.11.13.5. Bloqueio automático da tela;

4.1.11.13.6. Bloqueio por tentativas inválidas.

4.1.11.14. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

4.1.11.14.1. Bluetooth;

4.1.11.14.2. Descoberta de dispositivos bluetooth;

4.1.11.14.3. Câmera;

4.1.11.14.4. Cartões de memória;

4.1.11.14.5. Wlan/Wifi;

4.1.11.14.6. Aceitar TLS não confiável;

4.1.11.14.7. Instalação de aplicativos;

4.1.11.14.8. Sincronia automática enquanto em modo roaming;

4.1.11.14.9. Dados de diagnóstico;

4.1.11.14.10. Forçar backups criptografados;

4.1.11.14.11. Itunes;

4.1.11.14.12. Imessage;

4.1.11.14.13. Compra dentro de aplicativos;

4.1.11.14.14. Remoção de aplicativos;

4.1.11.14.15. Safari;

4.1.11.14.16. Auto preenchimento;

4.1.11.14.17. Javascript;

4.1.11.14.18. Popups;

4.1.11.14.19. Forçar aviso de fraude;

4.1.11.14.20. Aceitar cookies;

4.1.11.14.21. Captura de tela;

4.1.11.14.22. Siri;

4.1.11.14.23. Siri com tela bloqueada;

4.1.11.14.24. Filtro de profanidade;

4.1.11.14.25. Jogos multijogador;

4.1.11.14.26. Discagem por voz;

4.1.11.14.27. Youtube;

4.1.11.14.28. Abertura de documentos de aplicativos gerenciados em aplicativos terceiros;

4.1.11.14.29. Abertura de documentos de aplicativos terceiros em aplicativos gerenciados;

4.1.11.14.30. GPS;

4.1.11.14.31. Microsoft Activesync;

4.1.11.14.32. MMS/SMS;

4.1.11.14.33. Porta infravermelha;

4.1.11.14.34. Porta serial;

4.1.11.14.35. Alto-falante;

4.1.11.14.36. Armazenamento USB;

4.1.11.14.37. 3G;

4.1.11.14.38. Modo de desenvolvedor;

4.1.11.14.39. Ancoragem (tethering).

4.1.12. **Gerenciamento centralizado para todos os itens**

4.1.12.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos;

4.1.12.2. Instalação do servidor na plataforma Windows 2012 Server ou superior, seja o servidor físico ou virtual;

4.1.12.3. Suportar base de dados Microsoft SQL;

4.1.12.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

4.1.12.5. Deve possuir integração com Microsoft Active Directory;

4.1.12.6. Deve permitir níveis de administração por usuários ou grupos de usuários;

4.1.12.7. Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

4.1.12.8. Deve disponibilizar sua interface através dos protocolos HTTP e HTTPS;

4.1.12.9. Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

4.1.12.10. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

4.1.12.11. Geração de relatórios e gráficos e parametrizáveis nos formatos HTML, PDF, XML e CSV;

4.1.12.12. Deve gerar relatórios e gráficos pré-definidos nos formatos PDF, ActiveX e Crystal Report (*.rpt);

4.1.12.13. Deve permitir criação de modelos de relatórios customizados;

4.1.12.14. Deve permitir logon via single-sign-on com os demais produtos da solução;

4.1.12.15. Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

4.1.12.16. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

4.1.12.17. Deve permitir o controle individual de cada componente a ser atualizado;

4.1.12.18. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

4.1.12.19. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

4.1.12.20. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

4.1.12.21. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

4.1.12.22. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

4.1.12.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

4.1.12.24. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

4.1.12.25. Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

4.1.12.26. Deve permitir o controle do intervalo de expiração de comandos administrativos;

4.1.12.27. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

4.1.12.28. Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

4.1.12.29. Deve permitir a configuração da duração do bloqueio;

4.1.12.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias

4.1.12.31. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

4.1.12.32. Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

4.1.12.33. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser man dos e no número máximo de registros, por tipo de evento;

4.1.12.34. Deve de permitir a criação de políticas de segurança personalizadas;

4.1.12.35. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

4.1.12.35.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

4.1.12.35.2. Range de endereços IPS;

4.1.12.35.3. Sistema operacional;

4.1.12.35.4. Agrupamento lógicos dos módulos.

4.1.12.36. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

4.1.12.37. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

4.1.12.38. Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;

4.1.12.39. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.1.12.40. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

4.1.12.41. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

4.1.12.42. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

4.1.12.43. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

4.2. **Item 2 - Solução de segurança completa para Desktops (Completa)**

4.2.1. **Módulo de proteção anti-malware**

4.2.1.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.2.1.1.1. Windows 7 (x86/x64);

4.2.1.1.2. Windows 8.1 (x86/x64);

4.2.1.1.3. Windows 10 (x86/x64).

4.2.1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

4.2.1.3. Deve ser integrada ao Windows Security Center, quando utilizado em plataforma Microsoft;

4.2.1.4. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

4.2.1.5. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

4.2.1.5.1. Processos em execução em memória principal (RAM);

4.2.1.5.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

4.2.1.5.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, Microsoft ft CAB;

4.2.1.5.4. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

4.2.1.6. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;

4.2.1.7. Deve possuir detecção heurística de vírus desconhecidos;

4.2.1.8. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

4.2.1.9. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

4.2.1.9.1. Em tempo real de arquivos acessados pelo usuário;

4.2.1.9.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

4.2.1.9.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

4.2.1.9.4. Por linha de comando, parametrizável, com opção de limpeza;

4.2.1.9.5. Automáticos do sistema com as seguintes opções:

4.2.1.9.5.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

4.2.1.9.5.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

4.2.1.9.5.3. Frequência: horária, diária, semanal e mensal;

4.2.1.9.5.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

4.2.1.10. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

4.2.1.11. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

4.2.1.12. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

4.2.1.13. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

4.2.1.14. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

4.2.1.15. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

4.2.1.16. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

4.2.1.17. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

4.2.1.18. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

4.2.1.19. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

4.2.1.20. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

4.2.1.21. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

4.2.1.22. Deve bloquear processos comuns associados a ransomware.

4.2.2. **Funcionalidade de atualização**

4.2.2.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

4.2.2.2. Deve permitir atualização incremental da lista de definições de vírus;

4.2.2.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

4.2.2.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

4.2.2.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

4.2.2.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

4.2.2.7. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

4.2.2.8. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

4.2.3. **Funcionalidade de administração**

4.2.3.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

4.2.3.2. Deve possibilitar instalação "silenciosa";

4.2.3.3. Deve permitir o bloqueio por nome de arquivo;

4.2.3.4. Deve permitir o travamento de pastas e diretórios;

4.2.3.5. Deve permitir o travamento de compartilhamentos;

4.2.3.6. Deve permitir o rastreamento e bloqueio de infecções;

4.2.3.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

4.2.3.8. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

4.2.3.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

4.2.3.10. Deve permitir a desinstalação através da console de gerenciamento da solução;

4.2.3.11. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

4.2.3.12. Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

4.2.3.13. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

4.2.3.14. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

4.2.3.15. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

4.2.3.16. Deve permitir a deleção dos arquivos quarentenados;

4.2.3.17. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

4.2.3.18. Deve permitir integração com Active Directory para acesso a console de administração;

4.2.3.19. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

4.2.3.20. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

4.2.3.21. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.2.3.22. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

4.2.3.23. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

4.2.3.24. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

4.2.3.25. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.2.3.26. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional

4.2.3.27. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

4.2.3.28. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

4.2.3.29. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

4.2.3.30. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

4.2.3.31. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

4.2.3.32. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

4.2.3.33. Deve permitir a criação de usuários locais de administração da console de anti-malware;

4.2.3.34. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

4.2.3.35. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

4.2.3.36. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

4.2.3.37. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

4.2.3.38. Deve permitir a gerência de domínios separados para usuários previamente definidos;

4.2.3.39. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

4.2.3.40. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

4.2.4. **Funcionalidade de controle de dispositivos**

4.2.4.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

4.2.4.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.2.4.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

4.2.4.4. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.2.4.5. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

4.2.5. **Módulo de proteção anti-malware para estações Linux**

4.2.5.1. Distribuições homologadas pelo fabricante:

4.2.5.1.1. SUSE Linux Enterprise 10 e 11;

4.2.5.1.2. Red Hat enterprise Linux 4.0, 5.0 e 6.0;

4.2.5.1.3. Centos 4.0, 5.0 e 6.0.

4.2.5.2. O agente deve possuir código aberto possibilitando assim adequação a qualquer kernel e distribuição Linux, incluindo desenvolvidas ou alteradas internamente e para versões não homologadas pelo fabricante;

4.2.5.3. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

4.2.5.4. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática nos sistemas operacionais;

4.2.5.5. Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits e outros;

4.2.5.6. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;

4.2.5.7. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço IP do cliente e ação realizada;

4.2.5.8. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

4.2.5.9. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

4.2.5.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

4.2.5.11. As mensagens exibidas aos usuários devem ser traduzidas para o Português do Brasil.

4.2.6. **Módulo de proteção anti-malware para estações macOS**

4.2.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

4.2.6.1.1. macOS 10.14 (Mojave) em processadores 32 e 64 bits;

4.2.6.1.2. macOS 10.13 (High Sierra) em processadores 32 e 64 bits;

4.2.6.1.3. macOS 10.12 (Sierra) em processadores 32 e 64 bits;

4.2.6.1.4. OS X 10.11 (El Capitan) em processadores 32 e 64 bits;

4.2.6.1.5. OS X 10.10 (Yosemite) em processadores 32 e 64 bits.

4.2.6.2. Suporte ao Apple Remote Desktop para instalação remota da solução;

4.2.6.3. Gerenciamento integrado à console de gerência central da solução

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

4.2.6.5. Permitir a verificação das ameaças da maneira manual e agendada;

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

4.2.6.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos;

4.2.6.8. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

4.2.6.9. Deve possuir no mecanismo de autoproteção as seguintes proteções:

4.2.6.9.1. Autenticação de comandos IPC;

4.2.6.9.2. Proteção e verificação dos arquivos de assinatura;

4.2.6.9.3. Proteção dos processos do agente de segurança;

4.2.6.9.4. Proteção das chaves de registro do agente de segurança;

4.2.6.9.5. Proteção do diretório de instalação do agente de segurança.

4.2.7. **Funcionalidade de HIPS – Host IPS e Host Firewall**

4.2.7.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

4.2.7.1.1. Windows 7 (x86/x64);

4.2.7.1.2. Windows 8.1 (x86/x64);

4.2.7.1.3. Windows 10 (x86/x64).

4.2.7.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

4.2.7.3. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

4.2.7.4. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

4.2.7.5. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

4.2.7.6. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

4.2.7.7. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

4.2.7.8. O modulo de IDS deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack;

4.2.7.9. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

4.2.7.10. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

4.2.7.11. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas.

4.2.8. **Módulo para controle de aplicações**

4.2.8.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.2.8.1.1. Windows 7 (x86/x64);

4.2.8.1.2. Windows 8.1 (x86/x64);

4.2.8.1.3. Windows 10 (x64).

4.2.8.2. As regras de controle de aplicação devem permitir as seguintes ações:

4.2.8.2.1. Permissão de execução;

4.2.8.2.2. Bloqueio de execução;

4.2.8.2.3. Bloqueio de novas instalações.

4.2.8.3. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,

4.2.8.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

4.2.8.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

4.2.8.5.1. Assinatura SHA-1 e SHA-256 do executável;

4.2.8.5.2. Atributos do certificado utilizado para assinatura digital do executável;

4.2.8.5.3. Caminho lógico do executável;

4.2.8.5.4. Base de assinaturas de certificados digitais válidos e seguros.

4.2.8.6. As regras de controle de aplicação devem possuir categorias pré-determininadas de aplicações;

4.2.8.7. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

4.2.8.8. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento.

4.2.9. **Módulo de proteção contra vazamento de informações – DLP**

4.2.9.1. Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais:

4.2.9.1.1. Windows 7 (x86/x64);

4.2.9.1.2. Windows 8.1 (x86/x64);

4.2.9.1.3. Windows 10 (x64).

4.2.9.2. Deve possuir nativamente templates para atender as seguintes regulamentações:

4.2.9.2.1. PCI/DSS;

4.2.9.2.2. HIPAA;

4.2.9.2.3. GLBA;

4.2.9.2.4. SB-1386;

4.2.9.2.5. US PII.

4.2.9.3. Deve ser capaz de detectar informações, em arquivos nos formatos:

4.2.9.3.1. Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtt, wordpad, text; xml, html;

4.2.9.3.2. Gráficos: visio, postscript, pdf, ff;

4.2.9.3.3. Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh;

4.2.9.3.4. Códigos: c/c++, java, verilog, autocad.

4.2.9.4. Deve ser capaz de detectar informações, com base em:

4.2.9.4.1. Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros;

4.2.9.4.2. Palavras ou frases configuráveis;

4.2.9.4.3. Expressões regulares;

4.2.9.4.4. Extensão dos arquivos.

4.2.9.5. Deve ser capaz de detectar em arquivos compactados;

4.2.9.6. Deve permitir a configuração de quantas camadas de compressão serão verificadas;

4.2.9.7. Deve permitir a criação de modelos personalizados para identificação de informações;

4.2.9.8. Deve permitir a criação de modelos com base em regras e operadores lógicos;

4.2.9.9. Deve possuir modelos padrões;

4.2.9.10. Deve permitir a importação e exportação de modelos;

4.2.9.11. Deve permitir a criação de políticas personalizadas

4.2.9.12. Deve permitir a criação de políticas baseadas em múltiplos modelos;

4.2.9.13. Deve permitir mais de uma ação para cada política, como:

4.2.9.13.1. Apenas registrar o evento da violação;

4.2.9.13.2. Bloquear a transmissão;

4.2.9.13.3. Gerar alertar para o usuário;

4.2.9.13.4. Gerar alertar na central de gerenciamento;

4.2.9.13.5. Capturar informação para uma possível investigação da violação.

4.2.9.14. Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede;

4.2.9.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

4.2.9.15.1. Cliente de e-mail;

4.2.9.15.2. Protocolos http, https;

4.2.9.15.3. Mídias removíveis;

4.2.9.15.4. Discos óticos cd/dvd;

4.2.9.15.5. Gravação cd/dvd;

4.2.9.15.6. Aplicações de mensagens instantâneas;

4.2.9.15.7. Tecla de print screen;

4.2.9.15.8. Aplicações p2p;

4.2.9.15.9. Área de transferência do Windows;

4.2.9.15.10. Webmail;

4.2.9.15.11. Armazenamento na nuvem (cloud);

4.2.9.15.12. Impressoras;

4.2.9.15.13. Scanners;

4.2.9.15.14. Compartilhamentos de arquivos;

4.2.9.15.15. Activesync;

4.2.9.15.16. Criptografia PGP;

4.2.9.15.17. Disquete;

4.2.9.15.18. Portas com, lpt, firewire (ieee 1394);

4.2.9.15.19. Modems;

4.2.9.15.20. Infravermelho;

4.2.9.15.21. Bluetooth;

4.2.9.16. Deve permitir a criação de exceções nas restrições dos meios de transmissão.

4.2.10. **Módulo de criptografia**

4.2.10.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.2.10.1.1. Windows 7 (x86/x64);

4.2.10.1.2. Windows 8.1 (x86/x64);

4.2.10.1.3. Windows 10 (x64).

4.2.10.2. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

4.2.10.2.1. Disco completo (Full Disk);

4.2.10.2.2. Pastas e arquivos;

4.2.10.2.3. Mídias removíveis;

4.2.10.2.4. Anexos de e-mails;

4.2.10.2.5. Automática de disco.

4.2.10.3. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

4.2.10.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

4.2.10.5. Deve possuir suporte ao algoritmo de criptografia AES-256;

4.2.10.6. Deve possuir a capacidade de exceções para criptografia automática;

4.2.10.7. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

4.2.10.8. Deve possuir certificação FIPS 140-2;

4.2.10.9. Deve possuir funcionalidade de criptografia por software ou hardware;

4.2.10.10. Deve ser compatível com os padrões SED ('self-encrypting drive), OPAL e OPAL2;

4.2.10.11. Deve possuir compatibilidade de autenticação por múltiplos fatores;

4.2.10.12. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

4.2.10.13. Deve possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

4.2.10.14. Deve possuir políticas por usuários, grupos e dispositivos;

4.2.10.15. Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

4.2.10.15.1. Sequência de cores;

4.2.10.15.2. Autenticação com AD;

4.2.10.15.3. Single sign-on com AD;

4.2.10.15.4. Senha pré-definida;

4.2.10.15.5. Número PIN;

4.2.10.15.6. Smart card.

4.2.10.16. Deve possuir auto ajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

4.2.10.17. Deve possuir mecanismos de criptografia transparentes para o usuário;

4.2.10.18. Deve possuir mecanismos para wipe (limpeza) remoto;

4.2.10.19. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

4.2.10.20. Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

4.2.10.21. O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

4.2.10.22. Deve ser possível especificar o tipo de autenticação das redes wireless disponíveis;

4.2.10.23. O ambiente de autenticação pré-inicialização deve conter indicação visual do estado de conectividade de rede da estação/notebook;

4.2.10.24. O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

4.2.10.25. O ambiente de autenticação pré-inicialização deve permitir a mudança do *layout* do teclado;

4.2.10.26. O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

4.2.10.27. O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

4.2.10.28. Ambiente de autenticação pré-inicialização deve prover uma ferramenta que permita a execução de procedimentos de identificação de problema, assim como a realização das seguintes tarefas administrativas: desfazer a criptografia do disco, restaurar o registro mestre de inicialização (MBR – master boot record) ao estado anterior ao estado alterado pelo ambiente de autenticação pré-inicialização, montar partições criptografadas, modificar a política de criptografia aplicada à estação de trabalho, adicionar, remover e editar atributos dos usuários existentes na lista de usuários permitidos a se autenticar na estação de trabalho, visualizar os registros (logs) das atividades da solução de criptografia e visualizar, testar e modificar as configurações de rede;

4.2.10.29. O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

4.2.10.30. Deve prover ferramenta presente na estação de trabalho que possibilite migra-la para um servidor de gerenciamento diferente;

4.2.10.31. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

4.2.10.31.1. Microsoft Bitlocker;

4.2.10.31.2. Apple Filevault.

4.2.10.32. As capacidades de gerência das soluções terceiras de criptografia devem incluir:

4.2.10.32.1. Habilitar a criptografia;

4.2.10.32.2. Exibir o estado da criptografia (ativado, desativado);

4.2.10.32.3. Habilitar o aviso legal;

4.2.10.32.4. Editar o intervalo de sincronia.

4.2.10.33. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

4.2.10.34. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

4.2.10.35. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

4.2.10.36. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

4.2.10.37. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

4.2.10.38. Deve permitir a exibição de aviso legal quando a estação é inicializada;

4.2.10.39. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

4.2.10.40. Deve possibilitar que cada política tenha uma chave de criptografia única;

4.2.10.41. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

4.2.10.41.1. Chave do usuário: somente o usuário tem acesso aos arquivos;

4.2.10.41.2. Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

4.2.10.41.3. Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos.

4.2.10.42. Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

4.2.10.43. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

4.2.10.44. Deve possibilitar a desativação de dispositivos de armazenamento USB;

4.2.10.45. Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

4.2.10.46. Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

4.2.10.47. Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

4.2.10.48. Deve possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação;

4.2.10.49. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

4.2.10.50. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

4.2.10.51. Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

4.2.10.52. Definição do número de caracteres iguais consecutivos que não poderão ser utilizados na nova senha;

4.2.10.53. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

4.2.10.54. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

4.2.10.55. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.2.10.56. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

4.2.10.57. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação.

4.2.11. **Módulo de proteção para smartphones e tablets**

4.2.11.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

4.2.11.1.1. iOS;

4.2.11.1.2. Android.

4.2.11.2. As funcionalidades estarão disponíveis de acordo com cada plataforma;

4.2.11.3. Deve permitir o provisionamento de configurações de:

4.2.11.3.1. Wi-fi, Exchange Activesync, VPN, proxy HTTP global e certificados.

4.2.11.4. Deve possuir proteção de anti-malware;

4.2.11.5. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão SD e após atualização de vacinas;

4.2.11.6. Deve possuir capacidade de detecção de spam proveniente de SMS;

4.2.11.7. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

4.2.11.8. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

4.2.11.9. Deve possuir funcionalidade de firewall para bloqueio de tráfego de entrada e saída, com possibilidades de enumeração de regras de exceção;

4.2.11.10. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

4.2.11.11. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

4.2.11.12. Deve permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

4.2.11.13. Controle da política de segurança de senhas, com critérios mínimos de:

4.2.11.13.1. Padrão de senha;

4.2.11.13.2. Uso obrigatório de senha;

4.2.11.13.3. Tamanho mínimo;

4.2.11.13.4. Tempo de expiração;

4.2.11.13.5. Bloqueio automático da tela;

4.2.11.13.6. Bloqueio por tentativas inválidas.

4.2.11.14. Controle de acesso à seguinte lista funções e status desativação de funções dos dispositivos móveis:

4.2.11.14.1. Bluetooth;

4.2.11.14.2. Descoberta de dispositivos bluetooth;

4.2.11.14.3. Câmera;

4.2.11.14.4. Cartões de memória;

4.2.11.14.5. Wlan/Wifi;

4.2.11.14.6. Aceitar TLS não confiável;

4.2.11.14.7. Instalação de aplicativos;

4.2.11.14.8. Sincronia automática enquanto em modo roaming;

4.2.11.14.9. Dados de diagnóstico;

4.2.11.14.10. Forçar backups criptografados;

4.2.11.14.11. Itunes;

4.2.11.14.12. Imessage;

4.2.11.14.13. Compra dentro de aplicativos;

4.2.11.14.14. Remoção de aplicativos;

4.2.11.14.15. Safari;

4.2.11.14.16. Auto preenchimento;

4.2.11.14.17. Javascript;

4.2.11.14.18. Popups;

4.2.11.14.19. Forçar aviso de fraude;

4.2.11.14.20. Aceitar cookies;

4.2.11.14.21. Captura de tela;

4.2.11.14.22. Siri;

4.2.11.14.23. Siri com tela bloqueada;

4.2.11.14.24. Filtro de profanidade;

4.2.11.14.25. Jogos multijogador;

4.2.11.14.26. Discagem por voz;

4.2.11.14.27. Youtube;

4.2.11.14.28. Abertura de documentos de aplicativos gerenciados em aplicativos terceiros;

4.2.11.14.29. Abertura de documentos de aplicativos terceiros em aplicativos gerenciados;

4.2.11.14.30. GPS;

4.2.11.14.31. Microsoft Activesync;

4.2.11.14.32. MMS/SMS;

4.2.11.14.33. Porta infravermelha;

4.2.11.14.34. Porta serial;

4.2.11.14.35. Alto-falante;

4.2.11.14.36. Armazenamento USB;

4.2.11.14.37. 3G;

4.2.11.14.38. Modo de desenvolvedor;

4.2.11.14.39. Ancoragem (tethering).

4.2.12. **Gerenciamento centralizado para todos os itens**

4.2.12.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos;

4.2.12.2. Instalação do servidor na plataforma Windows 2012 Server ou superior, seja o servidor físico ou virtual;

4.2.12.3. Suportar base de dados Microsoft SQL;

4.2.12.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

4.2.12.5. Deve possuir integração com Microsoft Active Directory;

4.2.12.6. Deve permitir níveis de administração por usuários ou grupos de usuários;

4.2.12.7. Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

4.2.12.8. Deve disponibilizar sua interface através dos protocolos HTTP e HTTPS;

4.2.12.9. Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

4.2.12.10. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

4.2.12.11. Geração de relatórios e gráficos e parametrizáveis nos formatos HTML, PDF, XML e CSV;

4.2.12.12. Deve gerar relatórios e gráficos pré-definidos nos formatos PDF, ActiveX e Crystal Report (*.rpt);

4.2.12.13. Deve permitir criação de modelos de relatórios customizados;

4.2.12.14. Deve permitir logon via single-sign-on com os demais produtos da solução;

4.2.12.15. Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

4.2.12.16. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

4.2.12.17. Deve permitir o controle individual de cada componente a ser atualizado;

4.2.12.18. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

4.2.12.19. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

4.2.12.20. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

4.2.12.21. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

4.2.12.22. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

4.2.12.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

4.2.12.24. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

4.2.12.25. Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

4.2.12.26. Deve permitir o controle do intervalo de expiração de comandos administrativos;

4.2.12.27. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

4.2.12.28. Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

4.2.12.29. Deve permitir a configuração da duração do bloqueio;

4.2.12.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias

4.2.12.31. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

4.2.12.32. Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

4.2.12.33. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser man dos e no número máximo de registros, por tipo de evento;

4.2.12.34. Deve de permitir a criação de políticas de segurança personalizadas;

4.2.12.35. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

4.2.12.35.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

4.2.12.35.2. Range de endereços IPS;

4.2.12.35.3. Sistema operacional;

4.2.12.35.4. Agrupamento lógicos dos módulos.

4.2.12.36. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

4.2.12.37. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

4.2.12.38. Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;

4.2.12.39. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.2.12.40. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

4.2.12.41. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

4.2.12.42. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

4.2.12.43. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

4.2.13. **Modulo de anti-spam (gateway de e-mail)**

4.2.13.1. Pré-Filtro

4.2.13.1.1. Permitir configurar filtro de vírus (em nuvem) antes da chegada ao ambiente interno;

4.2.13.1.2. Permitir configurar filtro de SPAMs por reputação antes da chegada ao ambiente (na nuvem);

4.2.13.1.3. Permitir configurar filtro de SPAMs por característica (heurística) antes da chegada ao ambiente (na nuvem);

4.2.13.1.4. Permitir balanceamento de carga (Load Balance) para o mesmo domínio;

4.2.13.1.5. Possui gerenciamento de configurações em nuvem de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente.

4.2.13.2. SPAM / Phishing

4.2.13.2.1. Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys identified Mail (DKIM);

4.2.13.2.2. Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

4.2.13.2.3. Possuir a detecção de SPAMs utilizando tecnologia heurística;

4.2.13.2.4. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;

4.2.13.2.5. Permitir a criação de White e Black Lists para detecção de SPAMs;

4.2.13.2.6. Possuir proteção contra Phishings;

4.2.13.2.7. Possuir proteção inteligente contra ataques de Engenharia Social;

4.2.13.2.8. Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

4.2.13.2.9. Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados (Exploits) e Ataque de dia-zero (Zero-Day);

4.2.13.2.10. Possuir reputação de links que estejam dentro do corpo das mensagens;

4.2.13.2.11. Possuir níveis de sensibilidade no bloqueio de mensagens com links de má reputação;

4.2.13.2.12. Possuir White List para a checagem de reputação em URL's dentro de mensagens.

4.2.13.3. Vírus

4.2.13.3.1. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

4.2.13.3.2. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

4.2.13.3.3. Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

4.2.13.3.4. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

4.2.13.3.5. Proteção contra Spywares, sem a necessidade de um software ou agente adicional;

4.2.13.3.6. Proteção contra Dialers, sem a necessidade de um software ou agente adicional;

4.2.13.3.7. Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

4.2.13.3.8. Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

4.2.13.3.9. Proteção contra Adwares, sem a necessidade de um software ou agente adicional;

4.2.13.3.10. Proteção contra Ferramentas, sem a necessidade de um software ou agente adicional;

4.2.13.3.11. Bloqueio de malware empacotado (packed malware) de forma heurística;

4.2.13.3.12. A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentando como resultado a análise informações:

4.2.13.3.12.1. Processos de AutoStart;

4.2.13.3.12.2. Modificações de Arquivos de Sistema;

4.2.13.3.12.3. Serviços criados e modificados;

4.2.13.3.12.4. Atividade de Rede Suspeita;

4.2.13.3.12.5. Modificações de Registros.

4.2.13.3.13. O Fabricante ofertado deve possuir conhecimento em mais de 190 milhões de ameaças conhecidas.

4.2.13.4. Filtros

4.2.13.4.1. Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;

4.2.13.4.2. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

4.2.13.4.3. Permitir criar filtros definidos pelo tamanho de mensagem;

4.2.13.4.4. Possuir proteção contra Graymail;

4.2.13.4.5. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

4.2.13.4.6. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

4.2.13.4.7. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;

4.2.13.4.8. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

4.2.13.4.9. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

4.2.13.4.10. Permitir criar regras distintas para mensagens que entram e saem do ambiente;

4.2.13.4.11. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

4.2.13.4.12. Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;

4.2.13.4.13. Permitir limitar o número de destinatários por mensagem;

4.2.13.4.14. Possuir regra específica para anexos protegidos por senha;

4.2.13.4.15. Possuir módulo de Data Loss Prevention (DLP), prevenindo ações de vazamento de informações, com regras baseadas em:

4.2.13.4.15.1. Palavras chaves;

4.2.13.4.15.2. Expressões regulares;

4.2.13.4.15.3. Extensões de arquivos.

4.2.13.4.16. Possuir verificação de mensagens criptográficas de cliente que suporte os seguintes cipher suítes:

4.2.13.4.16.1. AES128-SHA;

4.2.13.4.16.2. DHE-RSA-AES128-SHA;

4.2.13.4.16.3. AES256-SHA;

4.2.13.4.16.4. ADH-RC4-MD5;

4.2.13.4.16.5. RC4-SHA;

4.2.13.4.16.6. RC4-MD5;

4.2.13.4.16.7. DHE-DSS-AES128-SHA;

4.2.13.4.16.8. IDEA-CBC-SHA.

4.2.13.5. Filtros por IP

4.2.13.5.1. Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

4.2.13.5.2. Permitir a configuração individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);

4.2.13.5.3. Possibilidade de exceções ao bloqueio por reputação com base em pais range de IP ou endereço IP;

4.2.13.5.4. Configurar nível de sensibilidade da reputação de IPs em até quatro níveis;

4.2.13.5.5. Permitir configurar o código de erro para mensagens rejeitadas;

4.2.13.5.6. Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:

4.2.13.5.6.1. Realizar a busca em, no mínimo, cinco bases de dados localizados no site do fabricante;

4.2.13.5.6.2. Não necessitar instalação adicional;

4.2.13.5.6.3. As bases devem ser do mesmo fabricante do software para gateway SMTP.

4.2.13.5.7. Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails));

4.2.13.5.8. Permitir personalizar os filtros baseado em:

4.2.13.5.8.1. Tempo;

4.2.13.5.8.2. Total de mensagens;

4.2.13.5.8.3. Porcentagem de mensagens;

4.2.13.5.8.4. Ação a ser tomada.

4.2.13.5.9. Prevenir contra-ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

4.2.13.5.10. Prevenir contra-ataques de Vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

4.2.13.5.11. Prevenir contra ataques DHA (Directory Harvest A ack);

4.2.13.5.12. Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas.

4.2.13.6. Ações

4.2.13.6.1. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

4.2.13.6.2. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

4.2.13.6.3. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

4.2.13.6.4. Permitir inserção de carimbo no assunto da mensagem;

4.2.13.6.5. Permitir a inserção de um header customizado (X-header);

4.2.13.6.6. Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;

4.2.13.6.7. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

4.2.13.6.8. Permitir a inserção de texto no corpo da mensagem;

4.2.13.6.9. Permitir customizar a mensagem que será inserida no corpo das mensagens;

4.2.13.6.10. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

4.2.13.6.11. Permitir inserir variáveis nas notificações, onde informem:

4.2.13.6.11.1. Remetente;

4.2.13.6.11.2. Destinatário;

4.2.13.6.11.3. Assunto;

4.2.13.6.11.4. Data;

4.2.13.6.11.5. Nome do arquivo detectado;

4.2.13.6.11.6. Nome do vírus detectado;

4.2.13.6.11.7. Protocolo de escaneamento;

4.2.13.6.11.8. Tamanho total da mensagem e seus anexos;

4.2.13.6.11.9. Tamanho total do anexo;

4.2.13.6.11.10 Número de anexos detectados pela regra;

4.2.13.6.11.11 Ação tomada pela ferramenta;

4.2.13.6.11.12 Nome da quarentena para onde a mensagem foi enviada.

4.2.13.6.12. Permitir configurar ações para mensagens fora do padrão (mensagens mal formadas);

4.2.13.6.13. Permitir ação personalizada para mensagens com anexos protegidos por senha;

4.2.13.6.14. Permitir quarentenar mensagens de SPAM;

4.2.13.6.15. Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

4.2.13.6.16. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria.

4.2.13.7. Quarentena

4.2.13.7.1. Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

4.2.13.7.2. Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

4.2.13.7.3. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

4.2.13.7.4. Permitir exclusão automática das mensagens em quarentena;

4.2.13.7.5. Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo:

4.2.13.7.5.1. Microsoft Active Directory;

4.2.13.7.5.2. OpenLDAP;

4.2.13.7.5.3. Sun iPlanet Directory.

4.2.13.8. Administração

4.2.13.8.1. Gerenciamento via console web HTTPS (Internet Explorer / Firefox);

4.2.13.8.2. A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento;

4.2.13.8.3. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

4.2.13.8.4. Realizar atualização de vacinas de forma incremental;

4.2.13.8.5. Realizar atualização da versão do software. A atualização deve permitir conexão através de serviço Proxy;

4.2.13.8.6. Possibilidade de configurar o “greeting” SMTP;

4.2.13.8.7. Permitir o controle de relay baseado no domínio e/ou endereço IP;

4.2.13.8.8. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

4.2.13.8.9. Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;

4.2.13.8.10. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio;

4.2.13.8.11. Definição de timeout de conexão SMTP;

4.2.13.8.12. Suporte a ilimitadas conexões SMTP;

4.2.13.8.13. Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único;

4.2.13.8.14. Ter a capacidade de proteger o tráfego POP3;

4.2.13.8.15. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

4.2.13.8.16. A solução deve ofertar possibilidade de ter domínio mascarado;

4.2.13.8.17. Possuir autenticação via TLS (Transport Layer Security);

4.2.13.8.18. Possuir mecanismo de alerta especifico para ataques do tipo Command & Control (C&C).

4.2.13.9. Relatórios

4.2.13.9.1. A solução deve apresentar relatórios criados através de console web;

4.2.13.9.2. A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

4.2.13.9.3. A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

4.2.13.9.4. A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

4.2.13.9.5. Possuir integração com LDAP (Microsoft Active Directory, Lotus Domino, Sun iPlanet Directory);

4.2.13.9.6. A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

4.2.13.9.7. A solução deve possibilitar trafego via Secure SMTP;

4.2.13.9.8. A solução deve permitir reindexação da base de dados de forma agendada;

4.2.13.9.9. É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;

4.2.13.9.10. A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;

4.2.13.9.11. A solução deve integrar o login da console de gerenciamento com o serviço de LDAP pré-configurado.

4.2.13.10. Características Gerais da Solução de anti-spam

4.2.13.10.1. A solução deve ser oferecida em formato de software appliance;

4.2.13.10.2. Não serão aceitas soluções Open Source;

4.2.13.10.3. A solução deve ser gerenciada totalmente por sua console Web, além de possui interface CLI intuitiva com gerenciamento dedicado à solução;

4.2.13.10.4. A solução precisa ser compatível com as seguintes plataformas de virtualização:

4.2.13.10.5. Vmware ESXi 5.0 ou superior;

4.2.13.10.6. Hyper-V;

4.2.13.10.7. Microsoft Hyper-V Server 2008 R2 SP1;

4.2.13.10.8. Microsoft Hyper-V Server 2012 R2.

4.2.13.11. ANTI-SPAM para Exchange

4.2.13.11.1. Suporte a Cluster Microsoft bem como as versões do MS-Exchange 2003, 2007 e 2010. No caso do MS-Exchange 2007, suportar a instalação na plataforma Windows 2008;

4.2.13.11.2. Deve ter o serviço clusterizado e trabalho em cluster ativo-ativo e ativo-passivo;

4.2.13.11.3. Permitir a instalação remota a múltiplos servidores Exchange, monitorando o status de cada instalação;

4.2.13.11.4. Permitir possibilidade de instalação silenciosa sem intervenção do administrador;

4.2.13.11.5. Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;

4.2.13.11.6. Permitir configurar as portas de comunicação para o gerenciamento;

4.2.13.11.7. Realizar a verificação em background, para não impactar na performance;

4.2.13.11.8. Possuir verificação em memória e multi-thread;

4.2.13.11.9. Possuir ação de limpeza para os arquivos anexados;

4.2.13.11.10. Permitir a verificação em tempo real, manual ou agendada de grupos e bases de dados no Exchange;

4.2.13.11.11. A verificação no Information Store deve ser realizada nas Public e Private Stores;

4.2.13.11.12. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;

4.2.13.11.13. Bloqueio dos arquivos em anexos deve ser com base em política por usuário e integrado com o active directory para a criação dessas políticas

4.2.13.11.14. Permitir a verificação no Internet Mail Connector (IMC);

4.2.13.11.15. Prover proteção para mensagens enviadas via Outlook Web Access (OWA);

4.2.13.11.16. Permitir a filtragem baseado no tamanho da mensagem;

4.2.13.11.17. Realizar a verificação contra códigos maliciosos no corpo da mensagem;

4.2.13.11.18. Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;

4.2.13.11.19. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

4.2.13.11.20. Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

4.2.13.11.21. Deve ter approved list para recebimento de mensagens de determinados senders;

4.2.13.11.22. Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;

4.2.13.11.23. Os usuários devem ter a capacidade de, se permitido, criarem suas exceções de recebimento através de white list gerenciada no próprio Outlook;

4.2.13.11.24. Avaliar reputação de links HTTP que estejam dentro do email quanto a sua reputação e caso reputação negativa deve ser tomada uma ação na mensagem;

4.2.13.11.25. Permitir criar regras de controle de conteúdo definidos por rotas, usuários e grupos;

4.2.13.11.26. Regra de controle de conteúdo deve procurar por conteúdo no subject, corpo e cabeçalho da mensagem;

4.2.13.11.27. Deve ter a possibilidade de em caso de um conteúdo malicioso, executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem, passar parte da mensagem;

4.2.13.11.28. Possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os emails detectados como SPAM, para que o usuário possa refinar a ferramenta;

4.2.13.11.29. Deve possuir área de quarentena no servidor com gerencia pelo administrador através da liberação de mensagens ou deleção;

4.2.13.11.30. Deve possuir exceções nas políticas de bloqueio de anexo e de bloqueio de conteúdo;

4.2.13.11.31. No caso de violação de anexo não desejado deve possuir capacidade de executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem;

4.2.13.11.32. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

4.2.13.11.33. Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;

4.2.13.11.34. Permitir o gerenciamento de vários servidores Exchange simultaneamente;

4.2.13.11.35. Gerenciamento via console web (Internet Explorer);

4.2.13.11.36. Possuir controle de timeout para a console de gerenciamento;

4.2.13.11.37. Permitir configurar as notificações a serem enviadas para o administrador, via email e SNMP;

4.2.13.11.38. Realizar ações específicas para cada tipo de código malicioso;

4.2.13.11.39. Capacidade para, em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;

4.2.13.11.40. Permitir um gerenciamento da quarentena, podendo enviar, encaminhar e apagar mensagens que estiverem nela;

4.2.13.11.41. Proteção contra spywares, sem a necessidade de um software ou agente adicional;

4.2.13.11.42. Deve detectar e bloquear malwares empacotados (packed malwares);

4.2.13.11.43. Para mensagens infectadas, deve poder tomar as seguintes ações: limpar, substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar, quarentenar parte da mensagem;

4.2.13.11.44. Produto deve ter capacidade de fazer reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;

4.2.13.11.45. Produto deve executar rastreamento agendado ou manual nas mailboxes dos usuários;

4.2.13.11.46. Deve possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;

4.2.13.11.47. Deve possuir capacidade de single-sing-on para acesso da console web de gerenciamento;

4.2.13.11.48. Deve reconhecer e ser compatível com IPV6;

4.2.13.11.49. Deve integrar-se com MOM/SCOM da Microsoft para envio de notificações;

4.2.13.11.50. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;

4.2.13.11.51. Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;

4.2.13.11.52. Deve gerar relatórios de:

4.2.13.11.52.1. Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;

4.2.13.11.52.2. Principais vírus/malwares, spywares e graywares;

4.2.13.11.52.3. Principais senders de vírus/malwares, spywares e graywares;

4.2.13.11.52.4. Resumo das ações tomadas contra vírus/malwares, spywares e graywares;

4.2.13.11.52.5. Resumo do bloqueio de anexos;

4.2.13.11.52.6. Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;

4.2.13.11.52.7. Principais tipos de anexos bloqueados;

4.2.13.11.52.8. Principais nomes de anexos bloqueados;

4.2.13.11.52.9. Principais extensões de anexos bloqueados;

1. Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;
2. Principais remetentes e destinatários filtrados.
3. Resumo de spam
4. Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;
5. Principais fontes e destinatários de spam;
6. Tráfego por hora, dia e mês.

4.2.13.12. Módulo de inspeção de e-mails entre caixas de correio e serviços online Microsoft

4.2.13.12.1. Aplicar proteções anti-malware, verificação de URL's maliciosas para a proteção dos serviços Exchange Online, SharePoint Online e OneDrive for Business da Microsoft;

4.2.13.12.2. A verificação Anti-malware deverá permitir a customização das ações a serem tomadas por exemplo: quarentena, deletar e passar;

4.2.13.12.3. Aplicar proteções contra Comprometimento de E-mail utilizando análise de escrita;

4.2.13.12.4. Realizar integração nuvem-a-nuvem, através de API da Microsoft, realizando a análise de malware em sandbox;

4.2.13.12.5. Monitorar em tempo real para bloquear, colocar em quarentena, ou fazer relatórios de políticas de conformidade;

4.2.13.12.6. Empregar detecção de malware por meio de sandbox sem assinaturas, para diminuir seu risco de violação;

4.2.13.12.7. Monitorar o comportamento real de arquivos suspeitos em ambientes sandbox virtuais usando múltiplas versões de sistemas operacionais e aplicações;

4.2.13.12.8. As políticas deverão possuir a capacidade de serem realizadas por usuário ou grupo;

4.2.13.12.9. Possuir um dashboard com as principais ameaças detectadas do tipo Ransomware, Phishing, Comprometimento de E-mail.

4.2.13.12.10. A solução deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens.

4.2.13.12.11. A solução deverá compartilhar objetos suspeitos previamente analisados em Sandbox com gerencia centralizada.

4.2.13.12.12. A Sandbox deverá ter a opção para funcionar em modo monitor não tomando nenhuma ação nos arquivos detectados.

4.2.13.12.13. Os alertas enviados deverão permitir a customização tanto para o usuário quanto para o *administrator*.

4.2.13.12.14. Deverá possui a funcionalidade de verificação de SPAM com níveis de detecções diferentes.

4.2.13.12.15. As ações realizadas pelo Anti-Spam deverão possuir as seguintes opções: quarentena, adicionar uma tag no assunto, deletar ou mover para a pasta de lixo.

4.2.13.12.16. Deverá permitir o administrador adicionar ou bloquear um endereço na lista de remetentes.

4.2.13.13. Modulo de inspeção de entrada e saída de e-mails

4.2.13.13.1. A proteção de e-mails para Office 365 deverá possuir os seguintes níveis de serviço:

4.2.13.13.1.1. Disponibilidade do serviço 99,93% de uptime;

4.2.13.13.1.2. Efetividade no bloqueio de SPAM 99% ou maior;

4.2.13.13.1.3. Ocorrência de Falsos-positivos não mais que 0,0003%;

4.2.13.13.1.4. Latência máxima na entrega de mensagens não mais que um minuto.

4.2.13.14. Proteção Anti-Spam

4.2.13.14.1. A solução deverá ser capaz de:

4.2.13.14.1.1. Permitir a Filtragem baseada em reputação IP para no mínimo:

1. Remetentes permitidos com base no endereço IP;
2. Remetentes bloqueados com base no endereço IP;
3. Bloqueio de e-mails baseados em países / regiões.

4.2.13.14.1.2. Permitir a Filtragem de Remetente e Destinatários para, no mínimo:

1. Remetentes aprovados por endereço de e-mail ou domínio;
2. Remetentes bloqueados por endereço de e-mail ou domínio.
3. Validar destinatário de entrada de e-mail.

4.2.13.14.1.3. Detectar spam baseado em assinatura e padrões;

4.2.13.14.1.4. Proteção anti-phishing;

4.2.13.14.1.5. Proteção anti-ransomware;

4.2.13.14.1.6. Proteção contra-ataques de Engenharia Social;

4.2.13.14.1.7. Identificar mensagens de email marketing;

4.2.13.14.1.8. Análise de spam com base no contexto da mensagem;

4.2.13.14.1.9. Realizar ajustes do nível de Sensibilidade de Spam para, no mínimo: O mais baixo (mais conservador), Baixo, moderadamente baixo, moderadamente alto, alto e Máximo (mais agressivo);

4.2.13.14.1.10As opções de configuração devem ser, no mínimo, as seguintes:

1. Filtrar por nome do anexo;
2. Filtrar por extensão de anexo;
3. Filtrar por tipo de arquivo anexado (true file type);
4. Filtrar por tamanho de anexo;
5. Filtrar por número de anexos;
6. Filtrar por tamanho total da mensagem;
7. Filtrar por palavras-chave no assunto;
8. Filtrar por palavras-chave no corpo;
9. Filtrar por palavras-chave no cabeçalho;
10. Filtrar por tipo de arquivo dentro de arquivos zip;
11. Filtro de arquivos protegidos por senha.

4.2.13.14.1.11A solução deverá ser capaz de realizar a quarentena de mensagens através de políticas implementadas para este fim, com as seguintes opções:

1. Quantidade de e-mails a serem exibidos no Portal de Administração de Quarentena;
2. Período de Retenção de Quarentena (antes de ser descartada);
3. Campo de Pesquisa de Quarentena;
4. Consulta de mensagens de quarentena usando curinga ou domínio, remetente e destinatário;
5. Pesquisar mensagens de quarentena por assunto;
6. Identificar o motivo pelo qual a mensagem foi quarentenada;
7. Excluir e-mail quarentenado;
8. Reprocessar mensagem na quarentena.

4.2.13.15. Quarentena Digest

4.2.13.15.1. Modelos pré-definidos personalizáveis com texto simples e versões HTML;

4.2.13.15.2. Redefinir para padrão modelos de texto sem formatação e HTML;

4.2.13.15.3. Suporta a adição de tokens / variáveis para acesso à quarentena;

4.2.13.15.4. Frequência diária com opção de enviar mais de uma vez durante o dia;

4.2.13.15.5. Frequência semanal.

4.2.13.16. Rastreamento de e-mail

4.2.13.16.1. A solução deverá possuir:

4.2.13.16.1.1. Campo de pesquisa de mensagem;

4.2.13.16.1.2. Controle de conteúdo de mensagens End-to-end;

4.2.13.16.1.3. Pesquisa de Mensagens usando coringa ou domínio;

4.2.13.16.1.4. Mostrar eventos de rastreamento completos das mensagens;

4.2.13.16.1.5. Mostrar desencadeamento de política;

4.2.13.16.1.6. Mostrar endereço IP do MTA do remetente e do destinatário;

4.2.13.16.1.7. Rastrear a mensagem por assunto, remetente e destinatário.

4.2.13.17. Plataforma SMTP

4.2.13.17.1. A solução deverá ser capaz de tratar:

4.2.13.17.1.1. Tamanho máximo de mensagem permitida;

4.2.13.17.1.2. Número máximo de destinatários em um e-mail;

4.2.13.17.1.3. O número máximo de camadas em um arquivo compactado;

4.2.13.17.1.4. Tamanho máximo de arquivos permitido após a descompressão;

4.2.13.17.1.5. Número máximo de arquivos permitidos em ZIP, Office;

4.2.13.17.1.6. Taxa de compressão máxima (%) de um arquivo compactado;

4.2.13.17.1.7. Restrição de conexões simultâneas;

4.2.13.17.1.8. ESMTP, 8bitmime, DSN;

4.2.13.17.1.9. Suprimir informações de MTA no cabeçalho recebido;

4.2.13.17.1.10 Autenticação Básica (SASL);

4.2.13.17.1.11 SSL / TLS para SMTP.

4.2.13.18. Proteção Antivírus e SMTP

4.2.13.18.1. A solução deverá ser capaz de:

4.2.13.18.1.1. Realizar a Detecção Anti-malware;

4.2.13.18.1.2. Realizar a Detecção de vírus através de Assinatura;

4.2.13.18.1.3. Realizar a Detecção de vírus via Heurística;

4.2.13.18.1.4. Realizar a Inspeção de malware no corpo da mensagem;

4.2.13.18.1.5. Realizar a Inspeção de malware em anexos;

4.2.13.18.1.6. Realizar a Proteção anti-spyware

4.2.13.18.1.7. Detectar URLs maliciosas no corpo da mensagem;

4.2.13.18.1.8. Detectar malwares em arquivos compactados;

4.2.13.18.1.9. Utilizar tecnologia de detecção própria para a 'Scan Engine' (o motor de escaneamento e a solução Anti-spam devem ser do mesmo fabricante);

4.2.13.18.1.10 Ter a opção para desativar a filtragem de malware;

4.2.13.18.1.11 Permitir realizar a detecção anti-malware em e-mails de saída;

4.2.13.18.1.12 Verificar a reputação de Endereço IP do remetente;

4.2.13.18.1.13 Analisa de URLs no momento do clique e bloquear caso a URL seja maliciosa;

4.2.13.18.1.14 Possuir Analise Preditiva para ameaças desconhecidas com alto risco;

4.2.13.18.1.15 Deve suportar o padrão SPF – Sender Policy Framework -para a verificação das mensagens;

4.2.13.18.1.16 Deve suportar o padrão DKIM - Domain Keys Indentified Mail -para a verificação das mensagens;

4.2.13.18.1.17 Deve suportar o padrão DMARC - Domain Message Authentication Reporting & Conformance - para a verificação das mensagens.

4.2.14. **Módulo de Filtro WEB**

4.2.14.1. O software deve ser atualizado gratuitamente, incluindo melhorias e novas versões durante o período de vigência do contrato;

4.2.14.2. Gerenciamento via console web;

4.2.14.3. Deve possuir a certtícação da VmWare para Software Appliance ou a possibilidade de instalação no formato de Bare Metal, formato no qual depende da homologação do hardware por parte do fabricante;

4.2.14.4. **Virtual Appliance:**

4.2.14.4.1. Suportar Vmware ESXi 5.5 ou superior;

4.2.14.4.2. Microsoft Hyper-v 2.0 Windows Server 2012 R2 ou superior.

4.2.14.5. A solução Virtual appliance deve fornecer junto da sua ISO de instalação um banco de dados;

4.2.14.6. Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e ActiveX maliciosos, sem a necessidade de um agente ou software adicional;

4.2.14.7. Toda a solução deverá ser do mesmo fabricante;

4.2.14.8. Permitir criar políticas de verificação baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;

4.2.14.9. Permitir um controle de quota em Megabytes ou por tempo para o acesso à internet, por usuário ou grupo de usuário, por dia, semana e mês;

4.2.14.10. Permitir a utilização da ferramenta em modo Transparent Bridge, Forward Proxy, Proxy Reverso;

4.2.14.11. Possuir suporte ao protocolo ICAP e WCCP,

4.2.14.12. Utilizar os seguintes serviços de diretório:

4.2.14.12.1. Microsoft Active Directory;

4.2.14.12.2. Linux OpenLDAP Directory ou;

4.2.14.12.3. Sun Java System Directory Server 5.2.

4.2.14.13. Permitir configurar os usuários que terão acesso à internet, baseado em seus logins, endereço IP e range IP;

4.2.14.14. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

4.2.14.15. Permitir a geração de relatórios, de forma manual ou agendada, com todos os eventos da ferramenta: códigos maliciosos, páginas acessadas, URL's bloqueadas, atividade por período e spywares detectados;

4.2.14.16. Atualização automática das vacinas de forma incremental e da versão do software;

4.2.14.17. Gerenciamento centralizado com a mesma console que administra o resto da solução;

4.2.14.18. Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;

4.2.14.19. Possuir um tratamento especial para Java Applets, onde esse é verificado quanto à sua assinatura e certificado, podendo tomar ações distintas para cada combinação entre elas, podendo ainda configurar que operações um Applet pode executar na máquina do usuário e como seus certificados serão validados;

4.2.14.20. A análise anti-malware da tecnologia deve ser realizada em Real Time, possibilitando uma ação imediata quando identificada uma ameaça;

4.2.14.21. O tratamento da análise de tráfego da tecnologia quando detectado um vírus deve ser de limpar, deletar ou quarentenar;

4.2.14.22. Possuir um tratamento especial para Activex, onde esse é verificado quanto à sua assinatura, e podendo tomar ações distintas para elas e como seus certificados serão validados;

4.2.14.23. Permitir configurar os certificados digitais que são seguros, colocando também os não seguros em uma lista negra;

4.2.14.24. A tecnologia deve ser capaz de identificar e bloquear conexões com redes zumbis (Botnets);

4.2.14.25. Possuir banco de dados de URL categorizados em, no mínimo, 80 categorias e tomar as seguintes ações para o acesso a estas categorias: PERMITIR, BLOQUEAR, MONITORAR, ALERTAR, TEMPO de ACESSO e ACESSO com SENHA. Este banco de dados deve estar hospedado na Internet para que se tenha uma atualização mais rápida das categorias.

4.2.14.26. A tecnologia deve possuir integrado a mesma solução um Cache de páginas HTTP que visa a melhorar o desempenho da navegação.

4.2.14.27. A configuração do tamanho dos objetos que serão armazenados no cache devem passíveis de modificação pelo Administrador da tecnologia;

4.2.14.28. Possibilidade de permissão de acesso websites definidos nas categorias em períodos pré-determinados;

4.2.14.29. Possuir integração com Safe Search do Google e do Yahoo;

4.2.14.30. Possuir análise de malware sobre o tráfego HTTPS;

4.2.14.31. Possibilidade de permitir customizar notificações para o usuário de acordo com a política de acesso definida:

4.2.14.31.1. HTTPS Access Denied;

4.2.14.31.2. HTTPS Cer ficate Failure;

4.2.14.31.3. HTTP/HTTPS Scanning;

4.2.14.31.4. HTTP/HTTPS Blocked File Type;

4.2.14.31.5. URL Blocking;

4.2.14.31.6. FTP Scanning;

4.2.14.31.7. FTP Blocked File Type;

4.2.14.31.8. IntelliTunnel (bloqueio de Instant Messaging);

4.2.14.31.9. Applets and ActiveX Instrumenta on;

4.2.14.31.10. Pattern File Updates;

4.2.14.31.11. URL Filtering and Scan Engines Update.

4.2.14.32. Possuir recurso para permitir / bloquear no mínimo 420 aplicações diferentes e este recurso deve funcionar no mínimo em dois modos de instalação (Forward Proxy e Bridge);

4.2.14.33. Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey, ...);

4.2.14.34. Possuir recurso de Web Reputation (reputação de HTTP), integrada com a solução de antivírus, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.2.14.35. Deve possuir a funcionalidade de replicar as configurações entre outros servidores de proteção do gateway HTTP através de uma tecnologia auxiliar de centralização de logs, reports e configurações;

4.2.14.36. Deve possuir capacidade de criar os seguintes perfis de acesso a console de gerencia: Administrador, Auditor e Reports;

4.2.14.37. Possuir ferramenta integrada para Back-up e restore das configurações da solução;

4.2.14.38. Possuir funcionalidade de geração de relatórios com as seguintes características:

4.2.14.38.1. A tecnologia deve contemplar a funcionalidade de Data Loss Prevention, afim, de evitar o vazamento de informações;

4.2.14.38.2. A solução deve contemplar templates contra vazamento de informações que atendam regulamentações de compliance.

4.2.14.38.3. A tecnologia deve possibilitar a criação de novos templates que visam a customização da tecnologia, afim, de proteger dados específicos;

4.2.14.38.4. A tecnologia deve permitir o acesso a redes sociais restringindo jogos e a possibilidade de submeter posts;

4.2.14.38.5. Os relatórios devem permitir que a partir da sua console seja possível submeter configurações das políticas de acesso à internet entre diversas instâncias da tecnologia de WEB Gateway;

4.2.14.38.6. Os relatórios devem possuir no mínimo 50 tipos de relatórios pré-definidos, que tragam visibilidade de acesso: URLS mais acessadas, usuários que mais acessam a internet, acesso por categoria do web site, consumo de banda e violações de regra;

4.2.14.38.7. Os relatórios devem disponibilizar um Dashboard de visualização dos acessos dos usuários ao WEB Gateway em tempo real;

4.2.14.38.8. A tecnologia standalone de relatórios deve permitir que geração seja agendada e enviada por e-mail;

4.2.14.38.9. A solução de filtro web deverá submeter arquivos suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise as seguintes informações:

4.2.14.38.9.1. Processos de AutoStart;

4.2.14.38.9.2. Modificações de Arquivos de Sistema;

4.2.14.38.9.3. Serviços criados e modificados;

4.2.14.38.9.4. Atividade de Rede Suspeita;

4.2.14.38.9.5. Modificações de Registros.

4.2.14.38.10. A análise de ameaças avançadas deverá realizar automaticamente o bloqueio em ações suspeitas nos filtro web contra a ameaça analisada em sandbox.

4.3. **Item 3 - Solução de Segurança para ambiente virtualizado, datacenter e nuvem**

4.3.1. **Características Gerais da Solução**

4.3.1.1. A solução deverá ser compatível com, pelo menos, os seguintes sistemas operacionais:

4.3.1.1.1. Windows XP SP3 (x86/x64);

4.3.1.1.2. Windows Server 2003 (32-bit/64-bit);

4.3.1.1.3. Windows Server 2008 (32-bit/64-bit), 2008 R2, 2012, 2012 R2, 2012 Server Core, 2016 (64-bit);

4.3.1.1.4. Windows 7 (x86/x64);

4.3.1.1.5. Windows 8 e 8.1 (x86/x64);

4.3.1.1.6. Windows 10 (x86/x64);

4.3.1.1.7. Red Hat Enterprise 5, 6, 7 (32-bit/64-bit);

4.3.1.1.8. SUSE Enterprise 10, 11, 12 (32-bit/64-bit);

4.3.1.1.9. CentOS (32-bit/64-bit);

4.3.1.1.10. Ubuntu (64-bit);

4.3.1.1.11. Debian (64-bit);

4.3.1.1.12. Oracle Linux;

4.3.1.1.13. Oracle Solaris 9, 10, 11 (64-bit SPARC), 10, 11 (64-bit x86);

4.3.1.1.14. AIX 5.3, 6.1, 7.1 e HP-UX 11i v3 (11.31).

4.3.1.2. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

4.3.1.3. A solução deverá permitir a integração com VMware vSphere 6 e com NSX estendendo os benefícios da micro-segmentação em um datacenter definido por softwares e fazendo com que as políticas de segurança estejam atreladas às VMs onde quer que elas estejam;

4.3.1.4. A solução deverá permitir a integração com Vmware Vrealize para o monitoramento do ambiente;

4.3.1.5. A solução deverá permitir a integração com pelo menos as seguintes plataforma de nuvem: Vmware vCloud, MS Azure e AWS;

4.3.1.6. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

4.3.1.7. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

4.3.1.8. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;

4.3.1.9. A console de administração deverá permitir o envio de notificações via SMTP;

4.3.1.10. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

4.3.1.11. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

4.3.1.12. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

4.3.1.13. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

4.3.1.14. A solução deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

4.3.1.15. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;

4.3.1.16. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF e RTF;

4.3.1.17. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

4.3.1.18. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS e Firewall;

4.3.1.19. A console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle e SQL;

4.3.1.20. A console de gerenciamento deve apresentar alta disponibilidade de modo que na ausência da principal os clientes automaticamente se comuniquem com a secundária e todas as configurações devem permanecer;

4.3.1.21. Quando operando em modo alta disponibilidade, ambos os consoles devem compartilhar a mesma database;

4.3.1.22. A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;

4.3.1.23. A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;

4.3.1.24. Para efeito de administração, deve ser possível de se replicar a estrutura do Active Directory na console de administração;

4.3.1.25. A solução de segurança para data center deverá suportar Docker para proteger os containers;

4.3.1.26. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

4.3.1.27. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

4.3.1.28. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

4.3.1.29. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

4.3.1.30. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

4.3.1.31. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;

4.3.1.32. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormenteativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

4.3.1.33. Os agentes para plataforma Linux deverão ser instalador por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

4.3.1.34. Para efeito de administração, a solução deverá avisar quando um agente encontrar-se não conectado a sua console de gerenciamento;

4.3.1.35. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

4.3.1.36. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

4.3.1.37. A solução deverá vir com perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;

4.3.1.38. Deverá possuir uma hierarquia de prevalecimento de configurações, seguindo no mínimo a ordem: Global -> Perfis -> hosts;

4.3.1.39. A solução deverá mostrar quais máquinas estão usando determinada política.

4.3.1.40. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

4.3.1.41. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

4.3.1.42. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

4.3.1.43. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

4.3.1.44. Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;

4.3.1.45. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

4.3.1.46. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

4.3.1.47. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

4.3.1.48. A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs, no mínimo com: IBM Qradar, HPArcSight, RSA Envision e NetIQ de modo a permitir enviar os seus logs para essas soluções;

4.3.1.49. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

4.3.1.50. A solução deverá ter a possibilidade de enviar eventos da console via SNMP;

4.3.1.51. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

4.3.1.52. A solução deverá permitir exportar relatórios para no mínimo os formatos PDF e RTF;

4.3.1.53. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

4.3.1.54. A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;

4.3.1.55. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

4.3.1.56. Após a atualização deve ser informado o que foi modificado ou adicionado;

4.3.1.57. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;

4.3.1.58. A console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras;

4.3.1.59. A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

4.3.1.60. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

4.3.1.61. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

4.3.1.62. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

4.3.1.63. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

4.3.1.64. Possibilidade de customizar a escolha do serviço de Whois para a identificação dos IPs que estejam realizando ataques;

4.3.1.65. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

4.3.1.66. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

4.3.1.67. A console de gerenciamento deve se integrar com o Vmware vCenter 4.0 ou Superior, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

4.3.1.68. A partir desta integração, deverá ser possível gerir a segurança dos guests VM, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado.

4.3.1.69. Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente Vmware e suas APIs, seja possível proteger as guests VMs sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests VMs.

4.3.1.70. A solução deverá ser capaz de implementar as funcionalidades de Anti-malware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Windows através de um único agente;

4.3.1.71. A solução deverá ser capaz de implementar as funcionalidades de Anti-malware, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Linux através de um único agente;

4.3.1.72. A solução deverá ser capaz de implementar as funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Solaris através de um único agente;

4.3.1.73. A solução deverá ser capaz de implementar as funcionalidades de Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais HP-UX e AIX através de um único agente;

4.3.1.74. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

4.3.1.75. Precisa ter a capacidade de desabilitar as regras não mais necessáriasdos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

4.3.1.76. A solução deverá ser possuir, no mínimo, as seguintes certticações de validação e/ou compatibilidade com padrões de mercado:

4.3.1.76.1. Certtied Red Hat Ready;

4.3.1.76.2. Cisco UCS validated;

4.3.1.76.3. Common Criteria EAL 4+;

4.3.1.76.4. EMC VSPE X validated;

4.3.1.76.5. NetApp FlexPod validated;

4.3.1.76.6. VCE Vblock validated.

4.3.2. **Módulo Anti-malware**

4.3.2.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

4.3.2.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

4.3.2.3. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

4.3.2.4. A mesma solução deverá ter a capacidade de realizar o rastreamento de códigos maliciosos em tempo real, por demanda e agendado em ambiente VMware sem a necessidade de agentes nas máquinas virtuais;

4.3.2.5. A solução deverá ter a capacidade de impedir a gravação de malwares realtime em ambiente VMware 4.1 ou superior com vShield Endpoint;

4.3.2.6. A solução deve permitir proteção de anti-malware em ambientes Linux (Ubuntu,CentOS, Red Hat e SuSe) utilizando agentes;

4.3.2.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

4.3.2.8. A solução deverá oferecer scanear processos em memória em busca de Malware;

4.3.2.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

4.3.2.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;

4.3.2.11. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta.

4.3.2.12. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

4.3.2.13. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware.

4.3.3. **Módulo Web Reputation**

4.3.3.1. Deve permitir a proteção contra acesso a websites ou URL consideradas maliciosas ou de baixa reputação;

4.3.3.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

4.3.3.3. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

4.3.3.4. A proteção deve suportar implementação sem a necessidade de instalação de agentes de segurança do fabricante da solução de segurança, através de integração com tecnologia VMware;

4.3.3.5. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança;

4.3.4. **Módulo de Host Firewall**

4.3.4.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

4.3.4.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

4.3.4.3. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

4.3.4.4. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

4.3.4.5. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

4.3.4.6. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

4.3.4.7. Precisa ter a capacidade de definição de regras para contextos específicos;

4.3.4.8. Precisa ter a capacidade de realização de varredura de portas nos servidores;

4.3.4.9. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de IPs, lista de MACs, lista de portas;

4.3.4.10. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

4.3.4.11. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

4.3.4.12. O firewall deverá ser stateful bidirecional;

4.3.4.13. O firewall deverá permitir liberar ou apenas logar eventos;

4.3.4.14. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

4.3.4.15. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass e deny;

4.3.4.16. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

4.3.4.17. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

4.3.4.18. Deverá realizar pseudo stateful em tráfego UDP;

4.3.4.19. Deverá logar a atividade stateful;

4.3.4.20. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

4.3.4.21. Deverá permitir limitar o número de meias conexões vindas de um computador;

4.3.4.22. Deverá prevenir ack storm;

4.3.4.23. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

4.3.4.24. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

4.3.5. **Módulo de Inspeção de Pacotes**

4.3.5.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

4.3.5.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

4.3.5.3. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

4.3.5.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. A opção de detecção e bloqueio deverá possibilitar ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;

4.3.5.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

4.3.5.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

4.3.5.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

4.3.5.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

4.3.5.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injec on e Cross Site Scrip ng. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

4.3.5.10. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

4.3.5.11. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

4.3.5.12. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

4.3.5.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

4.3.5.14. Deverá ser capaz de inspecionar tráfego incoming SSL;

4.3.5.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

4.3.5.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

4.3.5.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

4.3.5.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

4.3.5.19. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

4.3.5.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

4.3.5.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

4.3.5.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

4.3.5.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

4.3.5.24. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

4.3.5.25. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

4.3.5.26. As regras devem ser atualizadas automaticamente pelo fabricante;

4.3.5.27. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

4.3.6. **Módulo de Monitoramento de Integridade**

4.3.6.1. A solução deverá permitir a implantação nas plataformas Linux, Windows, Solaris, HP-UX, AIX, através da instalação de agentes;

4.3.6.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

4.3.6.3. A solução deverá fazer uso da tecnologia Intel TPM/TXT para monitorar a integridade contra mudanças não autorizadas a nível do Hypervisor;

4.3.6.4. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

4.3.6.5. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

4.3.6.6. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

4.3.6.7. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

4.3.6.8. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

4.3.6.9. O monitoramento poderá ser realizado em Realtime ou utilizando de scans periódicos para detectar mudanças de integridade;

4.3.6.10. Deverá alertar toda vez que uma modificação ocorrer em realtime para ambiente Windows e pseudo realtime para ambiente Linux, quando utilizamos agente;

4.3.6.11. Deverá logar e colocar em relatório todas as modificações que ocorram;

4.3.6.12. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

4.3.6.13. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

4.3.6.14. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

4.3.6.15. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

4.3.7. **Módulo de Inspeção de Logs**

4.3.7.1. A solução deverá permitir sua implantação nas plataformas Linux, Windows, Solaris, HP-UX, AIX;

4.3.7.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

4.3.7.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

4.3.7.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

4.3.7.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

4.3.7.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

4.3.7.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

4.3.7.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

4.3.7.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

4.3.7.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

4.3.7.11. As regras poderão ser modificadas por severidade de ocorrência de eventos;

4.3.7.12. As regras devem se atualizar automaticamente pelo fabricante;

4.3.7.13. Permitir modificação pelo administrador em regras para adequação ao ambiente.

4.3.8. **Módulo de Controle de Aplicações**

4.3.8.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

4.3.8.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

4.3.8.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

4.3.8.4. A console deverá exibir eventos de no mínimo 30 dias;

4.3.8.5. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período de tempo que deve ser no máximo 10 horas;

4.3.8.6. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

4.4. **Item 4 - Solução de proteção contra ameaças avançadas - 4 Gbps**

4.4.1. Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:

4.4.1.1. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

4.4.1.2. Detecção de ataques direcionados;

4.4.1.3. Analisador virtual de ameaças;

4.4.1.4. Correlação de regras para detecção de conteúdo malicioso;

4.4.1.5. Análise de todos os estágios de uma sequência de ataques.

4.4.2. **Características Gerais da Solução**

4.4.2.1. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo:

4.4.2.1.1. Serviço de Monitoração e Análise de Ameaças Digitais em rede;

4.4.2.1.2. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

4.4.2.1.3. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network exploit, web exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

4.4.2.1.4. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos.

4.4.2.1.5. Análise e correlação de atividades maliciosas tais como:

4.4.2.1.5.1. Detecção específica de malwares conhecidos e arquivos contaminados através deassinaturas de antivírus tradicional no tráfego da rede;

4.4.2.1.5.2. Detecção de vermes de rede e de e-mail no tráfego de rede;

4.4.2.1.5.3. Detecção de programas de exploração de vulnerabilidades (Exploits) na rede;

4.4.2.1.5.4. Detecção de empacotamentos maliciosos no tráfego da rede;

4.4.2.1.5.5. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

4.4.2.1.5.6. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

4.4.2.2. Permitir a rápida identificação da criticidade dos eventos de segurança;

4.4.2.3. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

4.4.2.4. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

4.4.2.5. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

4.4.2.6. Permitir a integração com sistemas de serviço de diretório;

4.4.2.7. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

4.4.2.8. A análise de SMTP será realizada em uma solução separada do sensor de HTTP e demais protocolos;

4.4.2.9. A análise em SMTP será realizando de modo MTA (Inline);

4.4.2.10. A análise de e-mail em sandbox deverá ocorrer em arquivos Microsoft Office, PDF, arquivos compactados e executáveis do tipo PE;

4.4.2.11. A análise em sandbox será realizada na própria solução, não sendo necessário integrações com demais soluções ofertadas;

4.4.2.12. A solução devera possuir mecanismo de derivar senhas de arquivos protegidos, para análise em sandbox;

4.4.2.13. A solução devera possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

4.4.2.14. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

4.4.2.15. Deve possuir pelo menos 1 sensor para "escutar" o tráfego de rede de throughput de 4Gbps de análise;

4.4.2.16. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

4.4.2.17. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

4.4.2.18. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

4.4.2.19. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

4.4.2.20. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bi orent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUni ve, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

4.4.2.21. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

4.4.2.22. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;

4.4.2.23. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

4.4.2.24. Capacidade de identificar artefatos maliciosos direcionados para dispositivos móveis rodando o sistema operacional Android, tais como smartphones e tablets;

4.4.2.25. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

4.4.2.26. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;

4.4.2.27. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes

simultâneos e integrados a solução para processamento de alto desempenho;

4.4.2.28. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

4.4.2.29. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

4.4.2.30. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

4.4.2.31. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

4.4.2.32. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

4.4.2.33. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

4.4.2.34. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;

4.4.2.35. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

4.4.2.36. Deverá permitir a análise especifica de eventos de segurança de computadores suspeitos de atividade maliciosa;

4.4.2.37. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

4.4.2.38. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

4.4.2.39. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

4.4.2.40. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

4.4.2.41. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

4.4.2.42. Deve possuir interface web para busca e investigação local de incidentes;

4.4.2.43. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows XP e Windows 7;

4.4.2.44. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

4.4.2.45. Deve possuir capacidade de análise virtual de artefatos internamente;

4.4.2.46. Deve possuir regras que identifiquem comunicações dos seguintes pos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;

4.4.2.47. Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

4.4.2.48. Deve possuir regras que identifiquem comunicações P2P, instant messengers e streaming;

4.4.2.49. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

- 4.4.2.49.1. Resumidos;
- 4.4.2.49.2. Visão Geral dos Incidentes de Segurança;
- 4.4.2.49.3. Discriminação dos Tipos de Incidentes;
- 4.4.2.49.4. Top Ameaças Analisadas;
- 4.4.2.49.5. Top Hosts Infectados;
- 4.4.2.49.6. Recomendações de Segurança;
- 4.4.2.49.7. Executivos.

4.4.2.50. Deve possuir detalhes técnicos dos incidentes detectados;

4.4.2.51. Deve possuir estatística do tráfego analisado;

4.4.2.52. Deve possuir indicadores de risco do ambiente;

4.4.2.53. Recomendações de Segurança;

4.4.2.54. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

4.4.2.55. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;

4.4.2.56. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

4.4.2.57. As atualizações do produto (pa erns e outros componentes) não devem causar down me ou impacto na operação;

4.4.2.58. Deve possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de analise virtual;

4.4.2.59. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

4.4.2.60. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

4.4.2.61. Deve ser capaz de detectar tentativas de scan de rede;

4.4.2.62. Deve ser capaz de detectar propagação de malwares na rede;

4.4.2.63. Deve ser capaz de detectar tentativas de brute-force;

4.4.2.64. Deve ser capaz de detectar tentativas de fuga e roubo de informação;

4.4.2.65. Deve ser capaz de detectar ameaças que se replicam na rede;

4.4.2.66. Deve ser capaz de detectar Exploits na rede;

4.4.2.67. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

4.4.2.68. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

4.4.2.69. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

4.4.2.70. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

4.4.2.71. Capacidade de salvar uma investigação antes de ser finalizada;

4.4.2.72. Capacidade de restaurar uma investigação para con nuá-la ou consultá-la;

4.4.2.73. Capacidade de emitir relatórios baseados nas investigações;

4.4.2.74. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

4.4.2.75. Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque;

4.4.2.76. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

4.4.2.77. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

4.4.2.78. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

4.4.2.79. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

4.4.2.80. Deve permitir recebimento de logs via syslog;

4.4.2.81. Deve permitir encaminhamento de logs via syslog;

4.4.2.82. Deve permitir receber logs de diferentes dispositivos;

4.4.2.83. Deve possuir engine de correlação de eventos;

4.4.2.84. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

4.4.2.85. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes;

4.4.2.86. Deve permitir a configuração de alarmes personalizados, com base em investigações;

4.4.2.87. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação.

4.4.3. **Características do Módulo de Análise Virtual**

4.4.3.1. Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX);

4.4.3.2. Deve suportar análise de documentos em PDF;

4.4.3.3. Deve submeter um documento PDF a pelo menos duas versões do Adobe Reader;

4.4.3.4. Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR);

4.4.3.5. Deve analisar dinamicamente binários PE de 32-bits;

4.4.3.6. Deve analisar dinamicamente binários PE de 64-bits;

4.4.3.7. Deve permitir criação de sandbox personalizada pelo usuário;

4.4.3.8. Deve permitir criação de sandbox local utilizando Windows XP 32-bits em inglês e português;

4.4.3.9. Deve permitir criação de sandbox local utilizando Windows 7 em inglês e português;

4.4.3.10. Deve permitir criação de sandbox local utilizando Windows 8 em inglês e português;

4.4.3.11. Deve permitir criação de sandbox local utilizando Windows 8.1 em inglês e português;

4.4.3.12. Deve permitir criação de sandbox local utilizando Windows 10 em inglês e português;

4.4.3.13. Deve permitir criação de sandbox local utilizando Windows 2003/2003 R2 em inglês e português;

4.4.3.14. Deve permitir criação de sandbox local utilizando Windows 2008/2008 R2 em inglês e português;

4.4.3.15. Deve permitir criação de sandbox local utilizando Windows 2012/2012 R2 em inglês e português;

4.4.3.16. Deve permitir criação de sandbox local utilizando Windows 2016 em inglês e português;

4.4.3.17. Deve analisar dinamicamente bibliotecas dinâmicas (DLL);

4.4.3.18. Deve analisar dinamicamente binários BHO;

4.4.3.19. Deve poder funcionar em ambiente totalmente virtualizado;

4.4.3.20. Deve possuir tecnologia própria de análise de artefatos em sandboxing;

4.4.3.21. Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência;

4.4.3.22. Deve prover possibilidade de uso da rede dedicada para a internet na análise de sandbox;

4.4.3.23. Deve analisar dinamicamente arquivos do Adobe Flash (SWF);

4.4.3.24. Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra;

4.4.3.25. Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo, ao nível de API, exibindo as funções com argumentos e retornos de execução;

4.4.3.26. Deve analisar dinamicamente rootkits;

4.4.3.27. Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado;

4.4.3.28. Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema;

4.4.3.29. Capacidade de integração via API com soluções terceiras;

4.4.3.30. O Fabricante deverá disponibilizar acesso a base de dados externa que possibilite a correlação entre informações geradas no ambiente com informações de outros clientes que foram afetados pelo mesmo padrão ou tipo de ameaça. Este acesso deverá ser web, e deverá possuir referências e atalhos nos próprios relatórios e logs locais da solução.

4.4.4. **Características da Console de Gerenciamento da Solução de Proteção Contra Ameaças Avançadas**

4.4.4.1. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneçaativa e funcionando;

4.4.4.2. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;

4.4.4.3. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

4.4.4.4. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

4.4.4.5. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

4.4.4.6. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

4.4.4.7. A console de gerenciamento deverá ser gerenciada por Internet Explorer e Firefox;

4.4.4.8. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

4.4.4.9. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

4.4.4.10. Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a análise de artefatos por meio de analisador virtual com a capacidade de gerar no mínimo 24 máquinas virtuais de análise;

4.4.4.11. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.

4.4.4.12. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações;

4.4.4.12.1. Uso de CPU

4.4.4.12.2. Uso de Disco;

4.4.4.12.3. Uso de Memória;

4.4.4.12.4. Tráfego malicioso analisado;

4.4.4.12.5. Todo o tráfego analisado.

4.4.5. **Logs e Relatórios da Solução de Proteção Contra Ameaças Avançadas**

4.4.5.1. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

4.4.5.1.1. Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

4.4.5.1.2. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações;.

4.4.5.2. A solução deverá ter integração com ferramentas de SIEM;

4.4.5.3. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da redecorporativa;

4.4.5.4. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;

4.4.5.5. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

4.4.5.5.1. Computadores infectados;

4.4.5.5.2. Origem de infecções;

4.4.5.5.3. Estatísticas de ameaças;

4.4.5.5.4. Riscos potenciais de segurança;

4.4.5.5.5. Riscos de perda de informações;

4.4.5.5.6. Risco de sistema comprometido;

4.4.5.5.7. Risco de disseminação de ameaças;

4.4.5.5.8. Eventos suspeitos;

4.4.5.5.9. Infecções de malware.

4.4.5.6. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

4.4.5.7. Critérios de pesquisa por dia, mês e ano;

4.4.5.8. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

4.4.5.9. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

4.4.5.10. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

4.4.6. **Gerenciamento centralizado para todos os itens**

4.4.6.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos, solução de anti-spam e solução contra ameaças avançadas;

4.4.6.2. Instalação do servidor na plataforma Windows 2012 Server ou superior, seja o servidor físico ou virtual;

4.4.6.3. Suportar base de dados Microsoft SQL;

4.4.6.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

4.4.6.5. Deve possuir integração com Microsoft Active Directory;

4.4.6.6. Deve permitir níveis de administração por usuários ou grupos de usuários;

4.4.6.7. Deve permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

4.4.6.8. Deve disponibilizar sua interface através dos protocolos HTTP e HTTPs;

4.4.6.9. Deve permitir a alteração das configurações das ferramentas ofertadas, de maneira remota;

4.4.6.10. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

4.4.6.11. Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

4.4.6.12. Deve gerar relatórios e gráficos pré-definidos nos formatos rtt, pdf, ActiveX e crystal report (*.rpt);

4.4.6.13. Deve permitir criação de modelos de relatórios customizados;

4.4.6.14. Deve permitir logon via single sign-on com os demais produtos da solução;

4.4.6.15. Deve permitir a atualização de todos os componentes de todos os módulos gerenciados;

4.4.6.16. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

4.4.6.17. Deve permitir o controle individual de cada componente a ser atualizado;

4.4.6.18. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

4.4.6.19. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

4.4.6.20. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

4.4.6.21. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

4.4.6.22. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

4.4.6.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

4.4.6.24. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

4.4.6.25. Deve permitir a escolha do intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

4.4.6.26. Deve permitir o controle do intervalo de expiração de comandos administrativos;

4.4.6.27. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

4.4.6.28. Deve permitir a configuração do número de tentativa inválidas de login para o bloqueio de usuários;

4.4.6.29. Deve permitir a configuração da duração do bloqueio;

4.4.6.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

4.4.6.31. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

4.4.6.32. Deve permitir a configuração das informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

4.4.6.33. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser man dos e no número máximo de registros, por tipo de evento;

4.4.6.34. Deve permitir a criação de políticas de segurança personalizadas;

4.4.6.35. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

4.4.6.35.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

4.4.6.35.2. Range de endereços IPS;

4.4.6.35.3. Sistema operacional;

4.4.6.35.4. Agrupamento lógicos dos módulos.

4.4.6.36. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

4.4.6.37. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

4.4.6.38. Deve permitir a gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;

4.4.6.39. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.4.6.40. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

4.4.6.41. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

4.4.6.42. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

4.4.6.43. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes.

4.5. **Item 5 - Solução de anti-spam (gateway de e-mail)**

4.5.1. **Pré-Filtro**

4.5.1.1. Permitir configurar filtro de vírus (em nuvem) antes da chegada ao ambiente interno;

4.5.1.2. Permitir configurar filtro de SPAMs por reputação antes da chegada ao ambiente (na nuvem);

4.5.1.3. Permitir configurar filtro de SPAMs por característica (heurística) antes da chegada ao ambiente (na nuvem);

4.5.1.4. Permitir balanceamento de carga (Load Balance) para o mesmo domínio;

4.5.1.5. Possui gerenciamento de configurações em nuvem de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente.

4.5.2. **SPAM / Phishing**

4.5.2.1. Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys identified Mail (DKIM);

4.5.2.2. Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

4.5.2.3. Possuir a detecção de SPAMs utilizando tecnologia heurística;

4.5.2.4. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 4 níveis;

4.5.2.5. Permitir a criação de White e Black Lists para detecção de SPAMs;

4.5.2.6. Possuir proteção contra Phishings;

4.5.2.7. Possuir proteção inteligente contra ataques de Engenharia Social;

4.5.2.8. Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

4.5.2.9. Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados (Exploits) e Ataque de dia-zero (Zero-Day);

4.5.2.10. Possuir reputação de links que estejam dentro do corpo das mensagens;

4.5.2.11. Possuir níveis de sensibilidade no bloqueio de mensagens com links de má reputação;

4.5.2.12. Possuir White List para a checagem de reputação em URL's dentro de mensagens.

4.5.3. **Vírus**

4.5.3.1. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

4.5.3.2. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

4.5.3.3. Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;

4.5.3.4. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

4.5.3.5. Proteção contra Spywares, sem a necessidade de um software ou agente adicional;

4.5.3.6. Proteção contra Dialers, sem a necessidade de um software ou agente adicional;

4.5.3.7. Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

4.5.3.8. Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

4.5.3.9. Proteção contra Adwares, sem a necessidade de um software ou agente adicional;

4.5.3.10. Proteção contra Ferramentas, sem a necessidade de um software ou agente adicional;

4.5.3.11. Bloqueio de malware empacotado (packed malware) de forma heurística;

4.5.3.12. A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentando como resultado a análise informações:

4.5.3.12.1. Processos de AutoStart;

4.5.3.12.2. Modificações de Arquivos de Sistema;

4.5.3.12.3. Serviços criados e modificados;

4.5.3.12.4. Atividade de Rede Suspeita;

4.5.3.12.5. Modificações de Registros.

4.5.3.13. O Fabricante ofertado deve possuir conhecimento em mais de 190 milhões de ameaças conhecidas.

4.5.4. **Filtros**

4.5.4.1. Possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;

4.5.4.2. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

4.5.4.3. Permitir criar filtros definidos pelo tamanho de mensagem;

4.5.4.4. Possuir proteção contra Graymail;

4.5.4.5. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

4.5.4.6. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

4.5.4.7. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro;

4.5.4.8. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

4.5.4.9. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

4.5.4.10. Permitir criar regras distintas para mensagens que entram e saem do ambiente;

4.5.4.11. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

4.5.4.12. Permitir a criação de grupos de usuários para configuração de regras por grupo ou usuário;

4.5.4.13. Permitir limitar o número de destinatários por mensagem;

4.5.4.14. Possuir regra específica para anexos protegidos por senha;

4.5.4.15. Possuir módulo de Data Loss Prevention (DLP), prevenindo ações de vazamento de informações, com regras baseadas em:

4.5.4.15.1. Palavras chaves;

4.5.4.15.2. Expressões regulares;

4.5.4.15.3. Extensões de arquivos.

4.5.4.16. Possuir verificação de mensagens criptográficas de cliente que suporte os seguintes cipher suítes:

4.5.4.16.1. AES128-SHA;

4.5.4.16.2. DHE-RSA-AES128-SHA;

4.5.4.16.3. AES256-SHA;

4.5.4.16.4. ADH-RC4-MD5;

4.5.4.16.5. RC4-SHA;

4.5.4.16.6. RC4-MD5;

4.5.4.16.7. DHE-DSS-AES128-SHA;

4.5.4.16.8. IDEA-CBC-SHA.

4.5.5. **Filtros por IP**

4.5.5.1. Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

4.5.5.2. Permitir a configuração individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);

4.5.5.3. Possibilidade de exceções ao bloqueio por reputação com base em pais range de IP ou endereço IP;

4.5.5.4. Configurar nível de sensibilidade da reputação de IPs em até quatro níveis;

4.5.5.5. Permitir configurar o código de erro para mensagens rejeitadas;

4.5.5.6. Permitir a verificação de endereços IPs para checar a sua legitimidade, sendo:

4.5.5.6.1. Realizar a busca em, no mínimo, cinco bases de dados localizados no site do fabricante;

4.5.5.6.2. Não necessitar instalação adicional;

4.5.5.6.3. As bases devem ser do mesmo fabricante do software para gateway SMTP.

4.5.5.7. Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails));

4.5.5.8. Permitir personalizar os filtros baseado em:

4.5.5.8.1. Tempo;

4.5.5.8.2. Total de mensagens;

4.5.5.8.3. Porcentagem de mensagens;

4.5.5.8.4. Ação a ser tomada.

4.5.5.9. Prevenir contra-ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

4.5.5.10. Prevenir contra-ataques de Vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

4.5.5.11. Prevenir contra ataques DHA (Directory Harvest A ack);

4.5.5.12. Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas.

4.5.6. **Ações**

4.5.6.1. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

4.5.6.2. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

4.5.6.3. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

4.5.6.4. Permitir inserção de carimbo no assunto da mensagem;

4.5.6.5. Permitir a inserção de um header customizado (X-header);

4.5.6.6. Permitir o direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;

4.5.6.7. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

4.5.6.8. Permitir a inserção de texto no corpo da mensagem;

4.5.6.9. Permitir customizar a mensagem que será inserida no corpo das mensagens;

4.5.6.10. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

4.5.6.11. Permitir inserir variáveis nas notificações, onde informem:

4.5.6.11.1. Remetente;

4.5.6.11.2. Destinatário;

4.5.6.11.3. Assunto;

4.5.6.11.4. Data;

4.5.6.11.5. Nome do arquivo detectado;

4.5.6.11.6. Nome do vírus detectado;

4.5.6.11.7. Protocolo de escaneamento;

4.5.6.11.8. Tamanho total da mensagem e seus anexos;

4.5.6.11.9. Tamanho total do anexo;

4.5.6.11.10. Número de anexos detectados pela regra;

4.5.6.11.11. Ação tomada pela ferramenta;

4.5.6.11.12. Nome da quarentena para onde a mensagem foi enviada.

4.5.6.12. Permitir configurar ações para mensagens fora do padrão (mensagens mal formadas);

4.5.6.13. Permitir ação personalizada para mensagens com anexos protegidos por senha;

4.5.6.14. Permitir quarentenar mensagens de SPAM;

4.5.6.15. Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

4.5.6.16. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria.

4.5.7. **Quarentena**

4.5.7.1. Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

4.5.7.2. Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

4.5.7.3. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

4.5.7.4. Permitir exclusão automática das mensagens em quarentena;

4.5.7.5. Deverá utilizar LDAP para autenticação ao portal de quarentena, suportando no mínimo:

4.5.7.5.1. Microsoft Active Directory;

4.5.7.5.2. OpenLDAP;

4.5.7.5.3. Sun iPlanet Directory.

4.5.8. **Administração**

4.5.8.1. Gerenciamento via console web HTTPS (Internet Explorer / Firefox);

4.5.8.2. A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento;

4.5.8.3. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

4.5.8.4. Realizar atualização de vacinas de forma incremental;

4.5.8.5. Realizar atualização da versão do software. A atualização deve permitir conexão através de serviço Proxy;

4.5.8.6. Possibilidade de configurar o “greeting” SMTP;

4.5.8.7. Permitir o controle de relay baseado no domínio e/ou endereço IP;

4.5.8.8. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

4.5.8.9. Permitir a verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;

4.5.8.10. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio;

4.5.8.11. Definição de timeout de conexão SMTP;

4.5.8.12. Suporte a ilimitadas conexões SMTP;

4.5.8.13. Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único;

4.5.8.14. Ter a capacidade de proteger o tráfego POP3;

4.5.8.15. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

4.5.8.16. A solução deve ofertar possibilidade de ter domínio mascarado;

4.5.8.17. Possuir autenticação via TLS (Transport Layer Security);

4.5.8.18. Possuir mecanismo de alerta especifico para ataques do tipo Command & Control (C&C).

4.5.9. **Relatórios**

4.5.9.1. A solução deve apresentar relatórios criados através de console web;

4.5.9.2. A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

4.5.9.3. A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

4.5.9.4. A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

4.5.9.5. Possuir integração com LDAP (Microsoft Active Directory, Lotus Domino, Sun iPlanet Directory);

4.5.9.6. A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

4.5.9.7. A solução deve possibilitar trafego via Secure SMTP;

4.5.9.8. A solução deve permitir reindexação da base de dados de forma agendada;

4.5.9.9. É preciso que a solução permita importação e exportação de suas políticas através da console de gerenciamento;

4.5.9.10. A solução deve permitir a criação de usuários com acessos diferentes de administrador à console de gerenciamento;

4.5.9.11. A solução deve integrar o login da console de gerenciamento com o serviço de LDAP pré-configurado.

4.5.10. **Características Gerais da Solução de anti-spam**

4.5.10.1. A solução deve ser oferecida em formato de software appliance;

4.5.10.2. Não serão aceitas soluções Open Source;

4.5.10.3. A solução deve ser gerenciada totalmente por sua console Web, além de possui interface CLI intuitiva com gerenciamento dedicado à solução;

4.5.10.4. A solução precisa ser compatível com as seguintes plataformas de virtualização:

4.5.10.5. Vmware ESXi 5.0 ou superior;

4.5.10.6. Hyper-V;

4.5.10.7. Microsoft Hyper-V Server 2008 R2 SP1;

4.5.10.8. Microsoft Hyper-V Server 2012 R2.

4.5.11. **ANTI-SPAM para Exchange**

4.5.11.1. Suporte a Cluster Microsoft bem como as versões do MS-Exchange 2003, 2007 e 2010. No caso do MS-Exchange 2007, suportar a instalação na plataforma Windows 2008;

4.5.11.2. Deve ter o serviço clusterizado e trabalho em cluster ativo-ativo e ativo-passivo;

4.5.11.3. Permitir a instalação remota a múltiplos servidores Exchange, monitorando o status de cada instalação;

4.5.11.4. Permitir possibilidade de instalação silenciosa sem intervenção do administrador;

4.5.11.5. Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;

4.5.11.6. Permitir configurar as portas de comunicação para o gerenciamento;

4.5.11.7. Realizar a verificação em background, para não impactar na performance;

4.5.11.8. Possuir verificação em memória e multi-thread;

4.5.11.9. Possuir ação de limpeza para os arquivos anexados;

4.5.11.10. Permitir a verificação em tempo real, manual ou agendada de grupos e bases de dados no Exchange;

4.5.11.11. A verificação no Information Store deve ser realizada nas Public e Private Stores;

4.5.11.12. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;

4.5.11.13. Bloqueio dos arquivos em anexos deve ser com base em política por usuário e integrado com o active directory para a criação dessas políticas;

4.5.11.14. Permitir a verificação no Internet Mail Connector (IMC);

4.5.11.15. Prover proteção para mensagens enviadas via Outlook Web Access (OWA);

4.5.11.16. Permitir a filtragem baseado no tamanho da mensagem;

4.5.11.17. Realizar a verificação contra códigos maliciosos no corpo da mensagem;

4.5.11.18. Realizar a verificação em arquivos baseado em seu tipo real, independente da extensão apresentada;

4.5.11.19. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

4.5.11.20. Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

4.5.11.21. Deve ter approved list para recebimento de mensagens de determinados senders;

4.5.11.22. Deve ter integração com a pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta;

4.5.11.23. Os usuários devem ter a capacidade de, se permitido, criarem suas exceções de recebimento através de white list gerenciada no próprio Outlook;

4.5.11.24. Avaliar reputação de links HTTP que estejam dentro do email quanto a sua reputação e caso reputação negativa deve ser tomada uma ação na mensagem;

4.5.11.25. Permitir criar regras de controle de conteúdo definidos por rotas, usuários e grupos;

4.5.11.26. Regra de controle de conteúdo deve procurar por conteúdo no subject, corpo e cabeçalho da mensagem;

4.5.11.27. Deve ter a possibilidade de em caso de um conteúdo malicioso, executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem, passar parte da mensagem;

4.5.11.28. Possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os emails detectados como SPAM, para que o usuário possa refinar a ferramenta;

4.5.11.29. Deve possuir área de quarentena no servidor com gerencia pelo administrador através da liberação de mensagens ou deleção;

4.5.11.30. Deve possuir exceções nas políticas de bloqueio de anexo e de bloqueio de conteúdo;

4.5.11.31. No caso de violação de anexo não desejado deve possuir capacidade de executar as seguintes ações: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o backup/cópia da mensagem;

4.5.11.32. Permitir a verificação contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;

4.5.11.33. Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;

4.5.11.34. Permitir o gerenciamento de vários servidores Exchange simultaneamente;

4.5.11.35. Gerenciamento via console web (Internet Explorer);

4.5.11.36. Possuir controle de timeout para a console de gerenciamento;

4.5.11.37. Permitir configurar as notificações a serem enviadas para o administrador, via email e SNMP;

4.5.11.38. Realizar ações específicas para cada tipo de código malicioso;

4.5.11.39. Capacidade para, em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;

4.5.11.40. Permitir um gerenciamento da quarentena, podendo enviar, encaminhar e apagar mensagens que estiverem nela;

4.5.11.41. Proteção contra spywares, sem a necessidade de um software ou agente adicional;

4.5.11.42. Deve detectar e bloquear malwares empacotados (packed malwares);

4.5.11.43. Para mensagens infectadas, deve poder tomar as seguintes ações: limpar, substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar, quarentenar parte da mensagem;

4.5.11.44. Produto deve ter capacidade de fazer reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;

4.5.11.45. Produto deve executar rastreamento agendado ou manual nas mailboxes dos usuários;

4.5.11.46. Deve possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;

4.5.11.47. Deve possuir capacidade de single sing on para acesso da console web de gerenciamento;

4.5.11.48. Deve reconhecer e ser compatível com IPV6;

4.5.11.49. Deve integrar-se com MOM/SCOM da Microsoft para envio de notificações;

4.5.11.50. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual;

4.5.11.51. Deve fazer filtro de conteúdo realizando o rastreamento dentro do anexo da mensagem;

4.5.11.52. Deve gerar relatórios de:

4.5.11.52.1. Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;

4.5.11.52.2. Principais vírus/malwares, spywares e graywares;

4.5.11.52.3. Principais senders de vírus/malwares, spywares e graywares;

4.5.11.52.4. Resumo das ações tomadas contra vírus/malwares, spywares e graywares;

4.5.11.52.5. Resumo do bloqueio de anexos;

4.5.11.52.6. Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;

4.5.11.52.7. Principais tipos de anexos bloqueados;

4.5.11.52.8. Principais nomes de anexos bloqueados;

4.5.11.52.9. Principais extenções de anexos bloqueados;

4.5.11.52.10. Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;

4.5.11.52.11. Principais remetentes e destinatários filtrados.

4.5.11.52.12. Resumo de spam

4.5.11.52.13. Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;

4.5.11.52.14. Principais fontes e destinatários de spam;

4.5.11.52.15. Tráfego por hora, dia e mês.

4.6. **Item 6 - Proteção de Filtro Web**

4.6.1. O software deve ser atualizado gratuitamente, incluindo melhorias e novas versões durante o período de vigência do contrato;

4.6.2. Gerenciamento via console web;

4.6.3. Deve possuir a certficação da VmWare para Software Appliance ou a possibilidade de instalação no formato de Bare Metal, formato no qual depende da homologação do hardware por parte do fabricante;

4.6.4. Virtual Appliance:

4.6.4.1. Suportar Vmware ESXi 5.5 ou superior;

4.6.4.2. Microsoft Hyper-v 2.0 Windows Server 2012 R2 ou superior.

4.6.5. A solução Virtual appliance deve fornecer junto da sua ISO de instalação um banco de dados;

4.6.6. Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e ActiveX maliciosos, sem a necessidade de um agente ou software adicional;

4.6.7. Toda a solução deverá ser do mesmo fabricante;

4.6.8. Permitir criar políticas de verificação baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;

4.6.9. Permitir um controle de quota em Megabytes ou por tempo para o acesso à internet, por usuário ou grupo de usuário, por dia, semana e mês;

4.6.10. Permitir a utilização da ferramenta em modo Transparent Bridge, Forward Proxy, Proxy Reverso;

4.6.11. Possuir suporte ao protocolo ICAP e WCCP,

4.6.12. Utilizar os seguintes serviços de diretório:

4.6.12.1. Microsoft Active Directory;

4.6.12.2. Linux OpenLDAP Directory ou;

4.6.12.3. Sun Java System Directory Server 5.2.

4.6.13. Permitir configurar os usuários que terão acesso à internet, baseado em seus logins, endereço IP e range IP;

4.6.14. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho da solução;

4.6.15. Permitir a geração de relatórios, de forma manual ou agendada, com todos os eventos da ferramenta: códigos maliciosos, páginas acessadas, URL's bloqueadas, atividade por período e spywares detectados;

4.6.16. Atualização automática das vacinas de forma incremental e da versão do software;

4.6.17. Gerenciamento centralizado com a mesma console que administra o resto da solução;

4.6.18. Possibilidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado;

4.6.19. Possuir um tratamento especial para Java Applets, onde esse é verificado quanto à sua assinatura e certificado, podendo tomar ações distintas para cada combinação entre elas, podendo ainda configurar que operações um Applet pode executar na máquina do usuário e como seus certificados serão validados;

4.6.20. A análise anti-malware da tecnologia deve ser realizada em Real Time, possibilitando uma ação imediata quando identificada uma ameaça;

4.6.21. O tratamento da análise de tráfego da tecnologia quando detectado um vírus deve ser de limpar, deletar ou quarentenar;

4.6.22. Possuir um tratamento especial para Activex, onde esse é verificado quanto à sua assinatura, e podendo tomar ações distintas para elas e como seus certificados serão validados;

4.6.23. Permitir configurar os certificados digitais que são seguros, colocando também os não seguros em uma lista negra;

4.6.24. A tecnologia deve ser capaz de identificar e bloquear conexões com redes zumbis (Botnets);

4.6.25. Possuir banco de dados de URL categorizados em, no mínimo, 80 categorias e tomar as seguintes ações para o acesso a estas categorias: PERMITIR, BLOQUEAR, MONITORAR, ALERTAR, TEMPO de ACESSO e ACESSO com SENHA. Este banco de dados deve estar hospedado na Internet para que se tenha uma atualização mais rápida das categorias.

4.6.26. A tecnologia deve possuir integrado a mesma solução um Cache de páginas HTTP que visa a melhorar o desempenho da navegação.

4.6.27. A configuração do tamanho dos objetos que serão armazenados no cache devem passíveis de modificação pelo Administrador da tecnologia;

4.6.28. Possibilidade de permissão de acesso websites definidos nas categorias em períodos pré-determinados;

4.6.29. Possuir integração com Safe Search do Google e do Yahoo;

4.6.30. Possuir análise de malware sobre o tráfego HTTPS;

4.6.31. Possibilidade de permitir customizar notificações para o usuário de acordo com a política de acesso definida:

4.6.31.1. HTTPS Access Denied;

4.6.31.2. HTTPS Cer ficate Failure;

4.6.31.3. HTTP/HTTPS Scanning;

4.6.31.4. HTTP/HTTPS Blocked File Type;

4.6.31.5. URL Blocking;

4.6.31.6. FTP Scanning;

4.6.31.7. FTP Blocked File Type;

4.6.31.8. IntelliTunnel (bloqueio de Instant Messaging);

4.6.31.9. Applets and ActiveX Instrumenta on;

4.6.31.10. Pattern File Updates;

4.6.31.11. URL Filtering and Scan Engines Update.

4.6.32. Possuir recurso para permitir / bloquear no mínimo 420 aplicações diferentes e este recurso deve funcionar no mínimo em dois modos de instalação (Forward Proxy e Bridge);

4.6.33. Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey, ...);

4.6.34. Possuir recurso de Web Reputation (reputação de HTTP), integrada com a solução de antivírus, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.6.35. Deve possuir a funcionalidade de replicar as configurações entre outros servidores de proteção do gateway HTTP através de uma tecnologia auxiliar de centralização de logs, reports e configurações;

4.6.36. Deve possuir capacidade de criar os seguintes perfis de acesso a console de gerencia: Administrador, Auditor e Reports;

4.6.37. Possuir ferramenta integrada para Back-up e restore das configurações da solução;

4.6.38. Possuir funcionalidade de geração de relatórios com as seguintes características:

4.6.39. A tecnologia deve contemplar a funcionalidade de Data Loss Prevention, afim, de evitar o vazamento de informações;

4.6.40. A solução deve contemplar templates contra vazamento de informações que atendam regulamentações de compliance.

4.6.41. A tecnologia deve possibilitar a criação de novos templates que visam a customização da tecnologia, afim, de proteger dados específicos;

4.6.42. A tecnologia deve permitir o acesso a redes sociais restringindo jogos e a possibilidade de submeter posts;

4.6.43. Os relatórios devem permitir que a partir da sua console seja possível submeter configurações das políticas de acesso à internet entre diversas instâncias da tecnologia de WEB Gateway;

4.6.44. Os relatórios devem possuir no mínimo 50 tipos de relatórios pré-definidos, que tragam visibilidade de acesso: URLS mais acessadas, usuários que mais acessam a internet, acesso por categoria do web site, consumo de banda e violações de regra;

4.6.45. Os relatórios devem disponibilizar um Dashboard de visualização dos acessos dos usuários ao WEB Gateway em tempo real;

4.6.46. A tecnologia standalone de relatórios deve permitir que geração seja agendada e enviada por e-mail.

4.7. **Item 7 - Pacote de Horas de Instalação (40 horas)**

4.7.1. Os softwares de solução de segurança a serem instalados no Estado do Piauí deverão ser configurados em equipamentos (estações de trabalho e servidores) fornecidos pela CONTRATANTE;

4.7.2. Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE;

4.7.3. No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:

4.7.3.1. Planejamento da instalação incluindo identificação de pré-requisitos;

4.7.3.2. Instalação e configuração do módulo de gerenciamento central;

4.7.3.3. Criar a senha de acesso com privilégio Administrativo para a Agência de Tecnologia da Informação do Estado do Piauí.

4.7.3.4. Instalação e configuração do software de endpoint protection em pelo menos 10 (dez) equipamentos;

4.7.3.5. Realizar customizações caso sejam solicitadas ou necessárias;

4.7.3.6. Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;

4.7.3.7. Realizar backup das configurações;

4.7.3.8. Documentar todas as configurações realizadas no ambiente.

4.7.4. Após a conclusão da instalação e implantação, a solução deverá ser formalmente homologada pela Gerência de Tecnologia da Informação do Estado do Piauí, o qual possuirá o prazo de 5(cinco) dias consecutivos contados a partir da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite).

4.8. **Item 8 - Treinamento (Hands-on) (40 horas)**

4.8.1. A CONTRATADA deverá ministrar treinamento on-site do tipo prático cobrindo todos os softwares inclusos na suíte de solução de segurança;

4.8.2. O conteúdo do treinamento deve abordar os assuntos de natureza teórica e prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

4.8.3. O treinamento pode ser separado conforme o produto a ser instalado no ambiente da Agência de Tecnologia da Informação, contendo ao menos os seguintes módulos:

4.8.3.1. Instalação do módulo de gerenciamento central;

4.8.3.2. Instalação do software de endpoint protection em estações de trabalho e servidores;

4.8.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução;

4.8.3.4. Resolução de problemas – troubleshooting;

4.8.3.5. Melhores práticas utilizadas no mercado para aproveitamento dos softwares e suas funcionalidades.

4.8.4. A carga horária mínima será de 16 horas divididas em expedientes de 4h/dia, das 9h às 13h;

4.8.4.1. O treinamento terá um total de cinco (5) participantes definidos pela Agência de Tecnologia da Informação do Estado do Piauí;

4.8.4.2. O material didático fornecido deve abordar todos os tópicos do curso;

4.8.4.3. A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;

4.8.4.4. É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;

4.8.4.5. Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pela Agência de Tecnologia da Informação do Estado do Piauí, o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

4.9. **Item 9 - Operação Assistida**

4.9.1. Por operação assistida entende-se a transferência de conhecimento, o esclarecimento de dúvidas para a equipe técnica da CONTRATANTE, o acompanhamento presencial do funcionamento dos equipamentos instalados e a pronta intervenção em caso de qualquer problema detectado no ambiente.

4.9.2. A CONTRATADA deverá prover o serviço de operação assistida pela quantidade de pacotes de horas contratadas após a conclusão da implantação do serviços. Durante este período a CONTRATADA deverá manter o ambiente da CONTRATANTE monitorado e acompanhado remotamente e eventualmente através de presença in loco de profissional competente.

4.9.3. As horas de Operação assistida serão utilizadas sob demanda por meio de Ordem de Serviço/OS, a critério do CONTRATANTE, e serão consumidas para realização de atividades críticas .

4.9.4. O serviço de operação assistida poderá ser prestado de forma presencial no endereço local do CONTRATANTE ou outro indicado por ele; bem como com todos os recursos ferramentais necessários para tanto, sem custos adicionais para o CONTRATANTE, durante todo o período de suporte técnico e garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual.

4.9.5. A Ordem de Serviço deverá conter no mínimo: descrição, prazo, período, local da execução e especificações técnicas do serviço, horas de apoio técnico especializado a serem utilizadas e produtos esperados;

4.9.6. Os serviços prestados deverão estar de acordo com as especificações constantes na Ordem de Serviço;

4.9.7. O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução. – quando a “Ordem de Serviço – OS” é emitida pelo CONTRATANTE, durante a execução – com o acompanhamento e supervisão de responsáveis do CONTRATANTE, e ao término da execução – com o fornecimento de “Relatórios de Atividade da Operação assistida” pela CONTRATADA e atesto dos mesmos por responsáveis do CONTRATANTE;

4.9.8. A partir da emissão da “Ordem de Serviço – OS”, a CONTRATADA terá até 05 (cinco) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento para início dos trabalhos; O CONTRATANTE comunicará à CONTRATADA quando uma “Ordem de Serviço – OS” estiver sendo elaborada para que a CONTRATADA possa se manifestar no interesse de agendamento de reunião para definição de procedimentos necessários para execução dos serviços;

4.9.9. As horas e procedimentos previstos inicialmente quando da abertura da “Ordem de Serviço – OS” serão validados no final das atividades e poderão sofrer adequações para estarem de acordo com o que foi efetivamente executado;

4.9.10. As horas efetivamente utilizadas nos procedimentos executados serão computadas de acordo com os dias e horários de entrada e saída do responsável da CONTRATADA às dependências do CONTRATANTE;

4.9.11. Para efeito de pagamento, somente após o término do computo dessas horas, a contratada emitirá fatura correspondente aos serviços concluídos na referida ordem de serviço;

4.9.12. Somente as ordens de serviço efetivamente concluídas, com o devido levantamento das horas computadas poderão ser faturadas;

4.9.13. Este serviço, de operação assistida, deverá estar disponível para acionamento no sistema 24 horas por dia vezes 7 dias por semana.

5. **DA JUSTIFICATIVA DO AGRUPAMENTO DOS ITENS EM LOTE ÚNICO**

5.1. Os itens que compõem o objeto da licitação serão licitados em **lote único**, por se tratar de serviços pertencentes ao mesmo segmento de mercado, o que poderá possibilitar o melhor aproveitamento dos recursos disponíveis no mercado e a economia em escala. A medida visa economia processual relativa ao procedimento licitatório e o gerenciamento/fiscalização contratual, além de assegurar a obtenção de propostas para todos os serviços de interesse da Administração.

5.2. O critério adotado justifica-se pela natureza do objeto, tendo em vista que, sua fragmentação em itens acarretará a perda do conjunto e perda de economia de escala, pois os itens guardam homogeneidade entre si, podendo ser fornecidos por um mesmo fornecedor.

5.3. Entretanto, por se tratar de uma solução para Proteção de Estações de trabalho e Servidores (ANTIVIRUS), baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte a implantação da solução, configuração, garantia, suporte e transferência de conhecimento; Como por exemplo: Um fornecedor de um produto de marca X não terá obrigações e competências de instalação e treinamento de um produto de marca Y, pois a contratação trata-se de uma solução única não podendo separa-la para vários fornecedores.

5.4. A separação de itens para vários fornecedores poderá também trazer prejuízos quanto responsabilidades contratual e na gestão do contrato desta Agência que diretamente impactará na qualidade da prestação de serviços ao aceitar uma tecnologia de antivírus e instalação e treinamento de empresas que não fornecem o mesmo produto.

6. CRITÉRIOS DE HABILITAÇÃO

6.1. HABILITAÇÃO JURÍDICA

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório da indicação de seus administradores;

c) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

d) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;e) No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte– segundo determinado pelo Departamento de Registro Empresarial e Integração - DREI;

f) Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva; indicar o responsável pela administração com poderes para assumir obrigações e assinar documentos em nome do licitante; apontar a sua sede; além de explicitar o objeto social, que deverá ser compatível com o objeto desta licitação, conforme a tabela da Classificação Nacional de Atividades Econômicas – CNAE, do IBGE.

6.2. QUALIFICAÇÃO TÉCNICA

a) A licitante será habilitada a participar do certame com a apresentação de, pelo menos, 01 (um) Atestado(s) de Capacidade Técnica, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove(m) a aptidão da licitante para desempenho de atividade pertinente e compatível em características e volume com o objeto da licitação, por meio da prestação satisfatória de serviços técnicos em território nacional.
b) O atestado deverá possuir informações suficientes para qualificar o seu objeto, bem como possibilitar ao CONTRATANTE confirmar sua veracidade junto à instituição emissora do atestado;
c) No caso deste processo licitatório, o fornecimento do(s) atestado(s) de capacidade técnica, deve referenciar um quantitativo mínimo de 30% (trinta por cento) para o fornecimento dos volumes prospectados para cada licença.
d) Para verificar a autenticidade dos atestados apresentados, o CONTRATANTE poderá realizar diligências ou requerer acompanhados dos comprovantes fiscais da execução do objeto.

6.2.1 **Da Declaração de que possui profissional qualificado**

6.2.1.1 A licitante deverá apresentar declaração, datada e assinada por seu representante legal, de que, caso se sagre vencedora do certame, no momento da assinatura do contrato, disporá de profissionais com nível superior e com as seguintes certificações ou equivalentes: profissionais capacitados e certificados nos produtos objeto desta licitação visando à execução de serviços de instalação e/ou de manutenção dos produtos componentes da solução ofertada.

6.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência ou de recuperação judicial, expedida pelo distribuidor da sede da pessoa jurídica. Para efeito de constatação da validade de tal certidão, será observado o prazo de validade constante na própria certidão. Caso a licitante esteja em recuperação judicial, será válida, para fins de qualificação econômico-financeira, a emissão de certidão, pela instância judicial competente, afirmando que a interessada está apta econômica e financeiramente a participar de procedimento licitatório, conforme Acórdão TCU nº 1201/2020 – Plenário.

b) O licitante deverá apresentar os seguintes índices contábeis, extraídos do último balanço patrimonial ou do balanço patrimonial referente ao período de existência da sociedade, atestando a boa situação financeira, conforme art. 7.2 da IN/MARE 05/95, Portaria GAB. SEAD. Nº 88/15:

LG= Liquidez Geral – superior a 1

SG= Solvência Geral – superior a 1

LC= Liquidez Corrente – superior a 1

Sendo,

LG= (AC+RLP) / (PC+PNC)

SG= AT / (PC+PNC)

LC= AC / PC

Onde:

AC= Ativo Circulante

RLP= Realizável a Longo Prazo

PC= Passivo Circulante

PNC= Passivo Não Circulante

AT= Ativo Total

c) As demonstrações contábeis apresentadas poderão ser submetidas à apreciação do Conselho Regional de Contabilidade.

d) O balanço patrimonial e as demonstrações contábeis, bem como os índices contábeis exigidos, deverão estar assinados por contador ou outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

e) A licitante que apresentar índice econômico igual ou inferior a 01 (um) em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente, deverá comprovar que possui **patrimônio líquido mínimo** não inferior a **10% (dez por cento)** do valor estimado da contratação ou item pertinente, por meio de Balanço Patrimonial e demonstrações contábeis do último exercício, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios.

6.4. REGULARIDADE FISCAL e TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto deste certame.

c) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço – FGTS (CRF, fornecido pela Caixa Econômica Federal). Será aceito certificado da matriz em substituição ao da filial ou vice-versa quando, comprovadamente, houver arrecadação centralizada;

d) Prova de regularidade para com a Justiça do Trabalho emitida pelo TST (Certidão Negativa de débitos Trabalhistas);

e) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

f) Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

6.4.1 Se, pelas documentações fornecidas diretamente pelo representante legal, não se puder inferir que o subscritor de tais declarações tem poderes para representar a empresa, esta será inabilitada.

6.4.2 Todos os documentos apresentados para habilitação deverão estar:

a) Em nome da licitante, com número do CNPJ e com o respectivo endereço da mesma;

b) Se a licitante for a matriz de uma empresa, todos os documentos deverão estar em nome da matriz;

c) Se a licitante for a filial de uma empresa, todos os documentos deverão estar em nome desta filial;

d) Se a licitante for a matriz da empresa e a fornecedora do objeto for uma de suas filiais, este fato deve ser expressamente registrado em declaração apresentada na qual a licitante indicará qual filial executará o objeto da licitação. Neste caso, os documentos relativos à regularidade fiscal, exigidos para a habilitação, deverão ser apresentados em nome da matriz e da filial, simultaneamente;

e) Serão dispensados da filial aqueles documentos que, pela sua própria natureza, comprovadamente, forem emitidos somente em nome da matriz;

f) Serão aceitos registros de CNPJ de licitantes matriz e filiais com diferenças de números nos documentos pertinentes ao CND e ao FGTS quando for comprovada a centralização do recolhimento dessas contribuições pela licitante.

6.4.3 A licitante ainda deverá apresentar declaração de que inexiste, no quadro funcional da empresa, menor de dezoito anos desempenhando trabalho noturno, perigoso ou insalubre ou menor de dezesseis anos executando qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos, conforme modelo constante nos anexos do Edital.

6.4.3 Caso permitida a participação de sociedades cooperativas, será exigida, ainda, a seguinte documentação complementar:

6.4.3.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764 de 1971;

6.4.3.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

6.4.3.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

6.4.3.4. O registro previsto na Lei n. 5.764/71, art. 107;

6.4.3.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

6.4.3.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

a) ata de fundação;

b) estatuto social com a ata da assembleia que o aprovou;

c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

d) editais de convocação das três últimas assembleias gerais extraordinárias;

e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e

f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

6.4.3.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/71 ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

7. CRITÉRIO DE ACEITAÇÃO DA PROPOSTA

7.1. Após o final da etapa de lances, o licitante classificado em primeiro lugar deverá encaminhar proposta de preços, em arquivo único, no prazo máximo de 24 (vinte e quatro) horas pelo próprio sistema eletrônico ou para o e-mail do Pregoeiro da sessão, contendo as especificações detalhadas do serviço, obedecendo ao **formulário de apresentação de proposta de preços** anexo ao edital.

7.1.1. Os documentos enviados por meio eletrônico poderão ser solicitados em original ou por cópia autenticada a qualquer momento pelo Pregoeiro, sob pena de desclassificação e da convocação dos licitantes remanescentes da ordem de classificação. Neste caso, todas as folhas que integrarem a proposta deverão estar assinadas e rubricadas pelo representante legal da proponente.

7.2 O licitante deverá consignar na proposta comercial o valor unitário e o valor total do(s) item(s), sendo considerada para efeito de julgamento e classificação das propostas o critério de **MENOR PREÇO POR LOTE**.

7.3 A proposta comercial terá **validade mínima de 90 (noventa) dias,** a contar da data da abertura da sessão pública.

7.4 Na elaboração de sua proposta, o licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

7.5 A apresentação da proposta implica a aceitação plena e total das condições deste TERMO DE REFERÊNCIA.

8. REDUÇÃO MINIMA ADMISSÍVEL PARA OS LANCES SUCESSIVOS

8.1 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado e as regras de aceitação dos mesmos. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, deverá ser de **R$ 10,00 (dez reais)**.

9. SANÇÕES ADMINISTRATIVAS (PENALIDADES)

9.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante ou adjudicatário que:

9.1.1. Não assinar a ata de registro de preços quando convocado dentro do prazo de validade da proposta, não aceitar/retirar a nota de empenho ou não assinar o termo de contrato decorrente da ata de registro de preços;

9.1.2. Apresentar documentação falsa;

9.1.3. Deixar de entregar os documentos exigidos no certame;

9.1.4. Ensejar o retardamento da execução do objeto;

9.1.5. Não mantiver a proposta;

9.1.6. Cometer fraude fiscal;

9.1.7. Comportar-se de modo inidôneo;

9.1.7.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

9.2. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

9.2.1. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

9.2.2. Impedimento de licitar e de contratar com o Estado do Piauí e descredenciamento no CADUF/PI, pelo prazo de até cinco anos.

9.3. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

9.4. As sanções serão aplicadas de acordo com a Lei Estadual nº 6.782/2016 e Decreto Estadual nº. 11.319/2004, facultada a defesa prévia da interessada, no prazo de 05 (cinco) dias úteis.

9.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade,

9.6. As penalidades administrativas aplicáveis à Contratada, por inadimplência, estão previstas nos artigos 81, 87, 88 e seus parágrafos, todos da Lei nº. 8.666/93, e art. 7º da Lei 10.520/2002, sem prejuízo das sanções previstas no contrato.

10. DAS CONDIÇÕES GERAIS DE CONTRATO

10.1 De acordo com o art. 12 do Decreto estadual nº 11.319/2004, o fato de existirem preços registrados, em nenhum caso, obriga a Administração a firmar qualquer tipo de contratação que deles poderão advir, sendo-lhe facultada a utilização e procura de outros meios, desde que respeitada a legislação respectiva, **assegurando-se a todos os possíveis beneficiários do registro preferência e igualdade de condições entre os registrados.**

10.2 Conforme disposto no art. 15 do Decreto estadual nº 11.319/2004, todos os fornecedores que tenham seus preços registrados, quando necessário, poderão ser convidados para firmar CONTRATAÇÕES decorrentes do registro de preços, desde que no período de sua vigência e observadas todas as exigências do instrumento convocatório e demais normas pertinentes.

10.3 O(s) contratado(s), após a assinatura do contrato, ficam obrigados ao cumprimento dos prazos e todas as condições estabelecidas previstas neste instrumento, no Edital e no contrato.

10.4 A recusa da execução do objeto ou o não cumprimento de qualquer obrigação prevista ensejará a aplicação das penalidades previstas neste instrumento, no Edital e no contrato.

10.5 É vedada a subcontratação, no todo ou em parte, do objeto a ser contratado.

10.6 Dentro da validade da Ata de Registro de Preços, o fornecedor registrado poderá ser convocado para assinar o contrato, ocasião em que terá o prazo de **05 (cinco) dias úteis para a realização do ato**, prorrogável por igual período, mediante a apresentação de motivo justo e aceito pela parte Contratante, sob pena de decair o direito à contratação, sem prejuízo da aplicação das penalidades cabíveis.

10.7 Da Vigência Contratual

10.7.1 O prazo de vigência do contrato a ser firmado será de **12 (Doze) meses,** a contar da data de sua assinatura, prorrogável na forma do art 57, IV, da Lei Nº 8.666/93, até o limite de 48 (Quarenta e Oito) meses.

10.8 **Da Execução dos Serviços**

10.8.1 **Prazo de Execução**:

a) Os prazos de início dos serviços são contados a partir da assinatura, do CONTRATANTE e da CONTRATADA, na Ordem de Serviço (OS) de cada serviço solicitado;

b) Os prazos de execução (descritos no macro cronograma) poderão ser prorrogados, desde que devidamente justificada a necessidade e anuído pelas partes.

10.8.2. **Horário e local da execução dos serviços:**

a) Os serviços serão executados e os produtos entregues preferencialmente na sede da CONTRATANTE, na cidade de Teresina-PI;

b) Eventualmente, alguns serviços poderão ser executados nas dependências da empresa CONTRATADA, quando de interesse da CONTRATANTE e da empresa CONTRATADA, sendo previamente autorizado pela CONTRATANTE;

c) Os serviços serão realizados durante à jornada de trabalho habitual de 06 (seis) horas diárias, de segunda a sexta-feira, no horário de expediente da CONTRATANTE.

10.8.3. **Condições para a execução dos serviços:**

a) A CONTRATANTE disponibilizará as condições físicas e logísticas adequadas, mobiliário, pontos lógicos, telefones, ferramentas e licenças (softwares) utilizados na CONTRATANTE, bem como o acesso às informações para gestão de estratégia e projetos necessárias para a perfeita execução dos serviços nas instalações da CONTRATANTE.

10.9 Do Recebimento dos Serviços

10.9.1 As contratações decorrentes deste Registro de Preços devem observar os seguintes prazos para recebimento dos serviços, conforme preceitua o art. 7º, inciso I, do Decreto nº 15.093, de 21 de fevereiro de 2013:

I - **provisoriamente**, no prazo de 15 (quinze) dias pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes;

II **- definitivamente**, por servidor ou comissão designada pela autoridade competente e presidida pelo fiscal do contrato, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, que se dará a cada 30 (trinta) dias, sem prejuízo da obrigação de o contratado reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, na forma prevista no art. 73, I, “b”, c/c art. 69 da Lei n. 8.666/1993, no prazo de até 03 (três) dias uteis;

10.9.1.1 O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

10.9.1.2 Na hipótese de o termo circunstanciado ou a verificação a que se refere **item 10.9.1** não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados à Administração

nos 15 (quinze) dias anteriores à exaustão dos mesmos, situação na qual será responsabilizado o fiscal ou comissão responsável pela fiscalização.

10.10 Da gestão e da fiscalização do contrato e da Garantia:

10.10.1 Nos termos dos Art. 67, § 1º, Lei nº. 8.666, de 1993, a CONTRATANTE designará um representante para representá-lo, acompanhar e fiscalizar a execução do Contrato, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização das falhas ou defeitos observados.

10.10.2 A(s) fiscalização (ões) da(s) contratação (ões) decorrente(s) deste Registro de Preços devem observar o disposto no Decreto nº 15.093, de 21 de fevereiro de 2013, que estabelece procedimentos para o acompanhamento dos contratos firmados por órgãos e entidades estaduais.

10.10.3 Haverá depósito em garantia da execução do contrato no valor de 2%, com validade de 90 dias após o termino da vigência contratual devendo ser renovada a cada prorrogação efetivada no contrato nos moldes do art.18 inciso XVII do decreto estadual 14.483/2011, e somente será liberada ante a comprovação de que empresa contratada quitou todas as suas obrigações para a satisfatória entrega do objeto deste TERMO DE REFERÊNCIA.

11. OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

11.1. DAS OBRIGAÇÕES DA CONTRATANTE

11.1.1. Cumprir fielmente o Contrato de modo que a CONTRATADA possa realizar os serviços com esmero e perfeição;

11.1.2. Receber os empregados e prepostos da CONTRATADA, devidamente credenciados, para manutenção e conservação dos equipamentos, tomando as providências administrativas que garantam o livre desempenho de tais atividades;

11.1.3. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos, após assinatura do Contrato, conforme disposto artigo 30 da IN04-SLTI/MPOG;

11.1.4. Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência observando-se o disposto nos artigo s 19 e 33 da IN04-SLTI/MPOG;

11.1.5. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas, de acordo com o disposto no artigo 21 da IN04-SLTI/MPOG;

11.1.6. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando se tratar de contrato oriundo de Ata de Registro de Preços;

11.1.7. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

11.1.8. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação;

11.1.9. Definir produtividade ou capacidade mínima de fornecimento da Solução de Tecnologia da Informação por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

11.1.10. Realizar, no momento da licitação e sempre que possível, diligências e/ou Prova de Conceito com o licitante classificado provisoriamente em primeiro lugar, para fins de comprovação de atendimento das especificações técnicas, exigindo, no caso de fornecimento de bens, a descrição em sua proposta da marca e modelo dos bens ofertados;

11.1.11. A CONTRATANTE se reserva o direito a qualquer momento de realizar diligências junto à CONTRATADA e aos fabricantes para esclarecimento de dúvidas;

11.1.12. Faculta-se ao CONTRATANTE e à CONTRATADA, sempre quando necessário, agendar reuniões periódicas de caráter gerencial ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato.

11.1.13. Efetuar o pagamento de acordo com as normas orçamentárias e financeira da ATI.

11.2. OBRIGAÇÕES DA CONTRATADA

11.2.1. Cumprir fielmente o Contrato de modo que o serviço se realize com esmero e perfeição, executando-os sob sua inteira e exclusiva responsabilidade;

11.2.2. Cumprir rigorosamente as normas e regulamentos pertinentes à solução objeto deste Termo de Referência;

11.2.3. Garantir o perfeito funcionamento da solução objeto deste Termo de Referência, através de equipe técnica dimensionada de forma a atender as solicitações dentro dos prazos necessários ao cumprimento dos cronogramas estabelecidos;

11.2.4. Emitir, sempre que solicitado pela ATI, relatórios gerenciais e/ou técnicos referentes aos serviços produzidos;

11.2.5. Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na implantação da solução, bem como, prestar esclarecimentos que forem solicitados pela ATI;

11.2.6. Utilizar profissionais devidamente capacitados e habilitados para os serviços contratados, impondo-lhes rigorosos padrões de qualidade, segurança e eficiência, correndo por sua conta todas as despesas com salários, impostos, contribuições previdenciárias, encargos trabalhistas, seguros e outras correlatas;

11.2.7. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados;

11.2.8. Refazer serviços nos prazos estabelecidos, quando apresentarem padrões de qualidade inferiores aos definidos, sem ônus para a ATI;

11.2.9. Disponibilizar os Serviços para uso pela contratante dentro do prazo pactuado pela CONTRATANTE;

11.2.10. Disponibilizar aplicações de monitoramento da solução para os técnicos da ATI;

11.2.11. Manter a qualidade dos Serviços dentro dos padrões estabelecidos;

11.2.12. Atender a reclamações da contratante sobre falhas nos Serviços;

11.2.13. Fazer diagnóstico das falhas dos Serviços, eliminando os defeitos nos componentes sob sua responsabilidade;

11.2.14. Atender a reclamações ou pedidos de esclarecimentos da CONTRATANTE sobre cobrança dos Serviços;

11.2.15. Tomar todas as providências necessárias para a fiel execução deste Instrumento;

11.2.16. Toda solução a que se refere este documento deverá estar implementada, assim como, os profissionais, devidamente habilitados, referidos neste termo aptos em até 10 (dez) dias corridos após a assinatura do contrato;

11.2.17. A CONTRATADA deverá garantir o serviço de suporte à customização, à parametrização e à configuração voltadas à utilização de funcionalidades disponibilizadas na versão apresentada ou em versões superiores do sistema utilizado durante a vigência do contrato;

11.2.18. A CONTRATADA deverá garantir que, durante a vigência do contrato, quando da descontinuidade de um produto e lançamento de outro, o CONTRATANTE passará a ter direito de uso do produto mais recente (sucessor) e a documentação completa sem custos adicionais. Além disso, o produto mais recente deverá possuir substancialmente o mesmo nível de características, valores e funcionalidades do anterior. Caso o novo produto seja um software desenvolvido no âmbito da execução do Objeto;

11.2.19. Caso haja atualização de release do software, a CONTRATADA deverá manter o funcionamento do ambiente durante a vigência do contrato ininterruptamente;

11.2.20. A manutenção deverá incluir o acesso, livre de qualquer ônus, ao website e à base de conhecimento da solução ofertada, bem como ao seu repositório de programas contendo correções, atualizações recentes, "drivers", programas de controle e informações;

11.2.21. Nos casos em que as manutenções necessitarem de paradas das soluções, o CONTRATANTE deverá ser imediatamente no ficado para que se proceda à aprovação da manutenção ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

11.2.22. Correrá por conta exclusiva da CONTRATADA a responsabilidade pelo deslocamento de sua equipe aos locais de prestação dos serviços, bem como as despesas de transporte, frete e seguro correspondente, quando acionado pelo CONTRATANTE e não resolvido remotamente;

11.2.23. Caso haja migração da solução, todo o processo se dará sem ônus para o CONTRATANTE;

11.2.24. Em caso de remanejamento ou de mudança física do ambiente de produção, a CONTRATADA deverá realizar a orientação na utilização, o acompanhamento pós-instalação, a orientação e a execução do planejamento de migração;

11.2.25. A CONTRATADA deverá solucionar problemas inerentes a todos os produtos e garantir que possam ser instalados em outro ambiente de produção desde que este ambiente esteja na sua matriz de compatibilidade e suportabilidade, em qualquer das unidades funcionais do CONTRATANTE;

11.2.26. A CONTRATADA prestará toda orientação técnica necessária para a perfeita utilização dos produtos, para obtenção do máximo desempenho destes durante o período de vigência do contrato, conforme definido abaixo:

11.2.26.1. Identificar e corrigir problemas de funcionamento;

11.2.26.2. Apoio nas definições do produto para composição de soluções;

11.2.26.3. Apoio na customização do produto para melhor adequação às necessidades do CONTRATANTE e para composição de soluções;

11.2.26.4. Avaliações, diagnósticos e proposições de soluções de melhoria em ambiente de produção.

11.2.26.5. A CONTRATADA deverá garantir a priorização de correções e melhorias dentro dos níveis de serviços estabelecidos no contrato;

11.2.26.6. A CONTRATADA deverá prestar orientações para identificação de causa de falhas da solução e seus componentes e apoio na recuperação de ambientes em caso de panes ou perda de dados;

11.2.26.7. A CONTRATADA deverá garantir disponibilização de correções e upgrade de versões e releases durante a vigência do contrato.

11.3 DAS OBRIGAÇÕES DE SIGILO

11.3.1 A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela ATI, tais documentos.

11.3.2 A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto sem autorização por escrito da ATI, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

11.3.3 Cada profissional deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não divulgar nenhum assunto tratado nas dependências da ATI ou a serviço desses, salvo se expressamente autorizado.

11.3.4 Cada profissional deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela ATI não poderá ser utilizada para fins par celulares e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da ATI, ou acessadas a partir dos seus equipamentos, poderão ser auditadas.

11.3.5 Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na ATI.

11.3.6 Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. Abrange toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE.

11.3.7 As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto.

11.3.8 As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que sejam comprovadamente de domínio público no momento da revelação, tenham sido comprovadas e legitimamente recebidas de terceiros e estranhos, sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido no ficadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

11.3.9 A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

11.3.10 A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO sobre a existência deste TERMO bem como da natureza sigilosa das informações.

11.3.11 A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

11.3.12 A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

12. VALOR ESTIMADO DA CONTRATAÇÃO (REFERENCIAL)

LOTE UNICO	Descrição do Item (Objeto)	Critério	Quantidade	Valor (R$)	
				Unitário	Total
1	Solução de segurança para Desktops(Endpoint)	Média	8.100	R$ 266,82	R$ 2.161.269,00
2	Solução de segurança completa para Desktops(Completa)	Média	8.100	R$ 522,86	R$ 4.235.166,00
3	Solução de Segurança para ambiente virtualizado, datacenter e nuvem	Mediana	825	R$ 5.478,00	R$ 4.519.350,00
4	Solução de proteção contra ameaças avançadas - 4Gbps	Média	3	R$ 2.352.606,32	R$ 7.057.818,95
5	Solução de anti-spam (gateway de e-mail)	Mediana	5.100	R$ 138,00	R$ 703.800,00
6	Proteção de Filtro WEB	Média	5.100	R$ 301,98	R$ 1.540.098,00
7	Pacote de Instalação(40 horas)	Média	19	R$ 30.436,67	R$ 578.296,73
8	Treinamento(Hands-on)(40 horas)	Média	17	R$ 15.550,00	R$ 264.350,00
9	Operação assistida/HORAS (pacotes de 40 horas)	Média	20	R$ 10.943,33	R$ 218.866,60
Global					**R$ 21.279.015,28**

13. DO PAGAMENTO E DO REAJUSTE

13.1 O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo CONTRATADO.

13.2 O preço consignado no contrato será corrigido anualmente, observado o interregno mínimo de um ano, contado a partir da data limite para a apresentação da proposta, pela variação do **Índice Nacional de Preços ao Consumidor Amplo – IPCA** divulgado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ou outro índice que venha a substituí-lo exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

14. DOS RECURSOS ORÇAMENTÁRIOS

14.1 Por se tratar de procedimento licitatório com Sistema de Registro de Preços, os recursos para custeio das despesas decorrentes da contratação que se seguir à licitação de que trata este Termo de Referência correrão à conta das dotações orçamentárias de cada Órgão/Ente do Estado participante do Registro, para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, a cargo do CONTRATANTE, cujos programas de trabalho e elementos de despesas específicos constarão da respectiva Nota de Reserva.

15. DAS DISPOSIÇÕES GERAIS

15.1 O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato ou da prestação dos serviços, sem prejuízo das demais sanções cabíveis;

15.2 As normas que disciplinam este procedimento licitatório serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação;

15.3 A participação do proponente neste certame implica em aceitação de todos os termos deste Termo de Referência.

15.4 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Termo de Referência será o do Município de Teresina – Piauí.

Teresina - Piauí

(documento assinado e datado eletronicamente)

ANEXO I DO TERMO DE REFERÊNCIA - PLANO DE GERENCIAMENTO DE PROJETO

1 PLANO MACRO DE IMPLANTAÇÃO

Ordem	Órgão	Segurança para desktops (completa)	Segurança para servidores	Solução ameaças avançadas
1	ATI	100	600	2
2	Secretaria de Educação	5000	225	1
3	SEADPREV	3000	0	0
	Total	8100	825	3

2 Agência de Tecnologia da Informação - ATI

Solução de Segurança para ambiente virtualizado, datacenter e nuvem	600
Solução de anti-spam (gateway de e-mail)	100
Proteção de Filtro WEB	100
Solução de proteção contra ameaças avançadas	2
Duração estimada (em dias)*:	101

* Considerando atividades que serão executadas em paralelo e operação assistida

Atividades	Duração (em dias)
0. Projeto de implantação das soluções de segurança	
1. Iniciação do projeto	
1.1. Reunião de kick-off	1
2. Planejamento do projeto	
2.1. Desenhar arquitetura e fornecer especificações dos servidores	1
2.2. Disponibilizar pré-requisitos	1
2.3. Definição das políticas de segurança	2
3. Implantação de segurança completa para Desktops (completa)	
3.1. Preparar componentes das soluções e integrações	1
3.2. Gerência centralizada	
3.2.1. Instalação e configuração da gerência centralizada da solução	1
3.3. Antimalware	
3.3.1. Instalação e configuração da solução antimalware	1
3.3.2. Homologação da instalação dos agentes em 100 estações Windows e MacOS	4
3.3.3. Instalação do agente antimalware nas demais estações de acordo com as ondas definidas	2
3.4. Funcionalidade de Host IPS/IDS	
3.4.1. Habilitar funcionalidade de host IPS/IDS em 100 estações	1
3.4.2. Acompanhar resultados	1
3.4.3. Replicar funcionalidade para demais estações do parque	2
3.5. Funcionalidade de controle de aplicações	

Atividades	Duração (em dias)
3.5.1. Configurar políticas de controle de aplicações permitidas e bloqueadas	1
3.5.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.5.3. Replicar política para demais estações do ambiente	4
3.6. Funcionalidade de DLP	
3.6.1. Configurar políticas de vazamento de informações	1
3.6.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.6.3. Replicar política para demais estações do ambiente	4
3.7 Módulo de criptografia	
3.7.1. Definir notebooks que serão criptografados	1
3.7.2. Preparar notebooks	2
3.7.3. Criptografar 10 dispositivos para homologação	2
3.7.4. Replicar política para demais dispositivos	8
3.7.5. Repasse de conhecimento	1
3.8. Módulo de proteção para smartphones e tablets	
3.8.1. Definir dispositivos que serão protegidos	1
3.8.3. Instalar 100 dispositivos para homologação	4
3.8.4. Replicar política para demais dispositivos	1
3.8.5. Repasse de conhecimento	1
3.9. Solução de anti-spam (gateway de e-mail)	
3.9.1. Instalar e configurar console de gerência	1
3.9.2. Configurar políticas de filtragem de e-mail	1
3.9.3. Desviar fluxo de e-mail (Office 365 ou Exchange)	2
3.9.4. Operação assistida	5
3.9.5. Repasse de conhecimento	1
3.10. Proteção de Filtro WEB	
3.10.1. Instalação e configuração da console de gerência	1
3.10.2. Configuração das políticas de acesso	1
3.10.3. Homologação das políticas com uma amostra dos usuários	3
3.10.4. Aplicação das políticas para os demais usuários	2
3.10.5. Operação assistida	5
3.10.6. Repasse de conhecimento	1
4. Implantação da Solução de segurança para ambiente virtualizado	
4.1. Instalação e configuração da console de gerência	1
4.2. Configuração das políticas de acesso	1
4.3. Instalação da solução nos servidores definidos	4
4.4. Aplicação da política para monitoramento	1
4.5. Operação assistida	5
4.6. Alteração da política para controle dos ataques	1
4.7. Repasse de conhecimento	1
5. Implantação da Solução de proteção contra ameaças avançadas	
5.1. Fornecer pré-requisitos de rede	1
5.2. Alocar equipamento físico na rede	1
5.3. Iniciar inspeção de rede	1
5.4. Integrar com demais soluções de segurança	2
5.5. Aprimorar detecções	3
5.6. Configurar relatórios	1
5.7. Repasse de conhecimento	1
Homologação do projeto de implantação	1

3 SEDUC - Educação

Soluções contratadas	Quantidade:
Solução de segurança completa para Desktops(Completa)	5000
Solução de anti-spam (gateway de e-mail)	5000
Proteção de Filtro WEB	5000

Soluções contratadas	Quantidade:
Duração estimada (em dias)*:	103

* Considerando atividades que serão executadas em paralelo e operação assistida

Atividades	Duração (em dias)
0. Projeto de implantação das soluções de segurança	
1. Iniciação do projeto	
1.1. Reunião de kick-off	1
2. Planejamento do projeto	
2.1. Desenhar arquitetura e fornecer especificações dos servidores	1
2.2. Disponibilizar pré-requisitos	1
2.3. Definição das políticas de segurança	2
3. Implantação de segurança completa para Desktops (completa)	
3.1. Preparar componentes das soluções e integrações	1
3.2. Gerência centralizada	
3.2.1. Instalação e configuração da gerência centralizada da solução	1
3.3. Antimalware	
3.3.1. Instalação e configuração da solução antimalware	1
3.3.2. Homologação da instalação dos agentes em 100 estações Windows e MacOS	4
3.3.3. Instalação do agente antimalware nas demais estações de acordo com as ondas definidas	20
3.4. Funcionalidade de Host IPS/IDS	
3.4.1. Habilitar funcionalidade de host IPS/IDS em 100 estações	1
3.4.2. Acompanhar resultados	1
3.4.3. Replicar funcionalidade para demais estações do parque	5
3.5. Funcionalidade de controle de aplicações	
3.5.1. Configurar políticas de controle de aplicações permitidas e bloqueadas	1
3.5.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.5.3. Replicar política para demais estações do ambiente	4
3.6. Funcionalidade de DLP	
3.6.1. Configurar políticas de vazamento de informações	1
3.6.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.6.3. Replicar política para demais estações do ambiente	5
3.7 Módulo de criptografia	
3.7.1. Definir notebooks que serão criptografados	1
3.7.2. Preparar notebooks	2
3.7.3. Criptografar 10 dispositivos para homologação	2
3.7.4. Replicar política para demais dispositivos	14
3.7.5. Repasse de conhecimento	1
3.8. Módulo de proteção para smartphones e tablets	
3.8.1. Definir dispositivos que serão protegidos	1
3.8.3. Instalar 100 dispositivos para homologação	4
3.8.4. Replicar política para demais dispositivos	2
3.8.5. Repasse de conhecimento	1
3.9. Solução de anti-spam (gateway de e-mail)	
3.9.1. Instalar e configurar console de gerência	1
3.9.2. Configurar políticas de filtragem de e-mail	1
3.9.3. Desviar fluxo de e-mail (Office 365 ou Exchange)	2
3.9.4. Operação assistida	5
3.9.5. Repasse de conhecimento	1
3.10. Proteção de Filtro WEB	
3.10.1. Instalação e configuração da console de gerência	1
3.10.2. Configuração das políticas de acesso	1
3.10.3. Homologação das políticas com uma amostra dos usuários	3
3.10.4. Aplicação das políticas para os demais usuários	2
3.10.5. Operação assistida	5
3.10.6. Repasse de conhecimento	1
Homologação do projeto de implantação	1

4 SEADPREV - SECRETARIA DE ADMINISTRAÇÃO E PREVIDÊNCIA DO ESTADO DO PIAUÍ

Soluções contratadas	Quantidade:
Solução de segurança completa para Desktops(Completa)	3000
Solução de anti-spam (gateway de e-mail)	0
Proteção de Filtro WEB	0
Duração estimada (em dias)*:	65

* Considerando atividades que serão executadas em paralelo e operação assistida

Atividades	Duração (em dias)
0. Projeto de implantação das soluções de segurança	
1. Iniciação do projeto	
1.1. Reunião de kick-off	1
2. Planejamento do projeto	
2.1. Desenhar arquitetura e fornecer especificações dos servidores	1
2.2. Disponibilizar pré-requisitos	1
2.3. Definição das políticas de segurança	2
3. Implantação de segurança completa para Desktops (completa)	
3.1. Preparar componentes das soluções e integrações	1
3.2. Gerência centralizada	
3.2.1. Instalação e configuração da gerência centralizada da solução	1
3.3. Antimalware	
3.3.1. Instalação e configuração da solução antimalware	1
3.3.2. Homologação da instalação dos agentes em 100 estações Windows e MacOS	4
3.3.3. Instalação do agente antimalware nas demais estações de acordo com as ondas definidas	14
3.4. Funcionalidade de Host IPS/IDS	
3.4.1. Habilitar funcionalidade de host IPS/IDS em 100 estações	1
3.4.2. Acompanhar resultados	1
3.4.3. Replicar funcionalidade para demais estações do parque	5
3.5. Funcionalidade de controle de aplicações	
3.5.1. Configurar políticas de controle de aplicações permitidas e bloqueadas	1
3.5.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.5.3. Replicar política para demais estações do ambiente	4
3.6. Funcionalidade de DLP	
3.6.1. Configurar políticas de vazamento de informações	1
3.6.2. Aplicar funcionalidade para 100 estações e acompanhar resultados	2
3.6.3. Replicar política para demais estações do ambiente	5
3.7 Módulo de criptografia	
3.7.1. Definir notebooks que serão criptografados	1
3.7.2. Preparar notebooks	2
3.7.3. Criptografar 10 dispositivos para homologação	2
3.7.4. Replicar política para demais dispositivos	12
3.7.5. Repasse de conhecimento	1
3.8. Módulo de proteção para smartphones e tablets	
3.8.1. Definir dispositivos que serão protegidos	1
3.8.3. Instalar 100 dispositivos para homologação	4
3.8.4. Replicar política para demais dispositivos	2
3.8.5. Repasse de conhecimento	1
Homologação do projeto de implantação	1

Documento assinado eletronicamente por **ANTONIO TORRES DA PAZ - Matr.0333972-6**, **Diretor Geral**, em 06/05/2021, às 11:35, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1510207** e o código CRC **3C2DE3B8**.

Referência: Processo nº 00117.001755/2019-32 SEI nº 1510207