Conass Documenta n. 33

Manual de Contratação de Serviços e Aquisição de Soluções em Tecnologia da Informação para a Gestão Estadual do SUS

Anexo I – Edital Base para Antivírus

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO — MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

TERMO DE REFERÊNCIA

(Processo Administrativo SEI/MP n.° 04310.000167/2018-65)

CONTRATAÇÃO DE SOLUÇÕES ANTIVÍRUS/ANTIMALWARE E ANTISPAM

1. DO OBJETO

1.1. Contratação de soluções integradas de seguranças do tipo endpoint protection (antivirus/antimalware) e de gateway de e-mail (antispam), incluindo serviços de instalação, suporte técnico on-site, repasse de conhecimento hands-on, garantia e atualização por 36 (trinta e seis) meses, conforme condições, quantidades, exigências e estimativas, inclusive as encaminhadas pelos órgãos e entidades participantes, estabelecidas neste instrumento.

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	IDENTIFICAÇÃO CATSER	UNIDADE DE MEDIDA	VALOR UNITÁRIO MÁXIMO
1	Solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware), incluindo instalação, suporte técnico on-site, repasse de conhecimento, garantia e atualização por 36 (trinta e seis meses)	24333 – Serviço de licença pelo uso de software	UN	R$ 101,90
2	Solução Antispam para Correio Eletrônico (Gateway de E-mail), incluindo instalação, suporte técnico on-site, repasse de conhecimento, garantia e atualização por 36 (trinta e seis meses)	24333 – Serviço de licença pelo uso de software	UN	R$ 75,00

1.2. O objeto desta licitação é divisível por itens, podendo ser adjudicado a mais de um proponente, conforme o menor preço unitário ofertado para cada item.

1.3. Os quantitativos para o órgão gerenciador e órgãos partícipes estão detalhados na tabela abaixo:

UASG	**ÓRGÃO**	**Quantidade Estimada**	
		ITEM 01	**ITEM 02**
201004	MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO.	4.500	4.500
26201	COLÉGIO PEDRO II	2.380	-
26406	INST.FED.DE EDUC., CIENC. E TEC. DO ESP. SANTO	8.000	5.000
154359	FUNDAÇÃO UNIVERSIDADE FEDERAL DO PAMPA	3.500	-
240127	CENTRO DE TECNOLOGIA MINERAL - CETEM - RJ	500	500
Total:		***18.880***	***10.000***

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

2.1. As soluções integradas de seguranças do tipo *endpoint protection* (antivirus) e de *gateway* de e-mail (antispam) possuem as seguintes características gerais:

2.2. SOLUÇÃO DE ANTIVÍRUS

2.2.1. O serviço deve ser provido por meio da implantação de tecnologia que possua capacidade de gerenciar de forma centralizada os clientes instalados nas estações de trabalho, utilizando-se de licença de *software* com função de Antivírus, AntiSpyware, *Firewall*, Proteção Contra Intrusos (HIPS), Controle de Dispositivos, Controle de Aplicações, entre outras. As licenças que serão ativadas nos servidores de gerência deverão ser flutuantes entre, no mínimo, dois nós em *cluster* e caso isso não seja possível, cada um dos componentes deve ser licenciado para que as funcionalidades permaneçam ativas no caso de indisponibilidade de um dos nós.

2.2.2. A solução que suportará os serviços deve ainda ser implantada nos dois datacenters do MP, localizados em Brasília, em ambiente virtualizado, sendo que na gerência da solução que for implantada no datacenter da Esplanada dos Ministérios devem ser ativadas 4.100 licenças e no datacenter do prédio da SEPN 516 Norte devem ser ativadas 400 licenças, totalizando a proteção de 4.500 *endpoints*. Ainda neste contexto, as gerências centralizadas devem ser independentes para cada datacenter e a implantação dos serviços deve contemplar a desinstalação completa de quaisquer soluções similares atualmente existentes nas estações de trabalho do MP.

2.2.3. O projeto de implantação deve evidenciar as estações de trabalho das unidades descentralizadas do MP que forem elencadas a

Centros de Distribuição de vacinas e devido ao grande número de clientes a serem gerenciados no datacenter da Esplanada dos Ministérios, e com o objetivo de garantir um bom desempenho ao servidor de gerência deste localidade, o banco de dados da solução de Proteção de *Endpoints* deve utilizar servidor distinto da aplicação.

2.2.4. Em resumo os serviços devem ser entregues de modo a prover segurança na camada de usuário, mitigando riscos capazes de impactar a produtividade dos colaboradores do Ministério e degradar o desempenho dos sistemas e redes corporativas.

2.3. SOLUÇÃO DE ANTISPAM

2.3.1. A solução de *Gateway* de e-mail (Antispam) deve ser instalada no datacenter principal da CONTRATANTE, localizado na Esplanada dos Ministérios, de modo a prover segurança de e-mail conforme topologia de rede já instalada.

2.3.2. A licença da solução com função de *Gateway Antispam* deverá ser flutuante entre, no mínimo, dois nós em *cluster* e caso isso não seja possível, cada um dos componentes deve ser licenciado para que as funcionalidades permaneçam ativas no caso de indisponibilidade de um dos nós.

2.3.3. O projeto de implantação deve prever a publicação da solução nos dois *links* de Internet da CONTRATANTE;

2.3.4. A CONTRATADA poderá fornecer solução em hardware específico (*appliance*) ou em *appliance* virtual a ser instalado no ambiente de virtualização da CONTRATANTE".

2.3.5. Em resumo os serviços devem ser entregues de modo a prover filtragem e segurança de e-mail, bem como bloqueio de e-mails não solicitados capazes de impactar a produtividade dos colaboradores do Ministério e degradar o desempenho dos sistemas e redes corporativas, sendo que o conjunto dos requisitos especificados podem ser atendidos por meio de outros equipamentos e softwares.

2.4. Fazem parte da contratação, visando a efetiva operacionalização e funcionamento das respectivas soluções:

2.4.1. Implantação e configuração da solução;

2.4.2. Garantia e Atualização por 36 (trinta e seis) meses;

2.4.3. Suporte técnico on-site por 36 (trinta e seis) meses;

2.4.4. Repasse de conhecimento.

2.5. O repasse de conhecimento deverá ser executado nas dependências da CONTRATANTE, por um período de até 2 (duas) horas, e compreende a apresentação do projeto de implantação da solução, indicando todas as licenças de softwares envolvidas, assim como explanação das principais funcionalidades da solução.

3. CLASSIFICAÇÃO DOS BENS COMUNS

3.1. Os bens a serem adquiridos enquadram-se na classificação de bens comuns, nos termos da Lei n° 10.520, de 2002.

3.2. Os bens considerados comuns são aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo ato convocatório, por meio de especificações usuais do mercado, independentemente de sua complexidade.

3.3. As soluções de software Antivírus e AntiSpam são considerados comuns pois suas características são definidas de forma objetiva e amplamente praticadas pelo mercado especializado.

4. ESPECIFICAÇÕES TÉCNICAS

4.1. REQUISITOS COMUNS

4.1.1. As soluções devem fazer parte do catálogo de produtos comercializados e não ter sido descontinuados;

4.1.2. A solução fornecida não deve estar relacionada em listas "*end of sale*" e "*end of support*" do site do fabricante;

4.1.3. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados neste termo especificados de maneira ininterrupta, irrestrita e sem necessidade de licenciamentos ou ônus adicionais durante o prazo de vigência do contrato.

4.1.4. Todas as licenças referentes aos sistemas operacionais, bancos de dados e softwares componentes da solução adquirida, inclusive os que forem implantados em ambiente virtualizado, devem estar em nome da CONTRATANTE, legalizado, não sendo admitidas versões "*shareware*" ou "*trial*";

4.1.5. A solução deverá ser composta de todos componentes necessários à sua completa instalação, configuração e operação, bem como a respectiva garantia;

4.1.6. Deverão ser fornecidos todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação da solução; A documentação e manuais técnicos deverão estar em Português. Deverão ser fornecidos materiais técnicos e manuais em formato digital que permita a importação para base de conhecimento online (Microsoft Word, PDF, HTML etc.);

4.1.7. A solução deverá ter capacidade para operar com todas as capacidades e funções solicitadas neste termo, inclusive com mais de uma capacidade ou função simultaneamente.

4.2. ITEM 1 – SOLUÇÃO ANTIVÍRUS

4.2.1. Deve suportar os seguintes requisitos mínimos:

4.2.1.1. Reputação de Arquivos, tanto locais como no acesso web;
4.2.1.2. IPS de Próxima Geração (*Next Generation IPS*);
4.2.1.3. Proteção de Navegadores (*Browser Protection*);
4.2.1.4. Aprendizado de Máquinas (*Machine Learning*);
4.2.1.5. Análise Comportamental (*Behavioral Analysis*);
4.2.1.6. Mitigação da Exploração de Memória (*Memory Exploit Mitigation*);
4.2.1.7. Controle de Aplicações (*Application Control*);
4.2.1.8. Controle de Dispositivos (*Device Control*);
4.2.1.9. Emulação para Malware (*Emulation for Malware*);
4.2.1.10. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas (*Exploit Mitigation*).

4.2.2. Deve ter a capacidade de implementar a funcionalidade de "*Machine Learning*" utilizando como-fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos, como também as características de boa pontuação:
4.2.2.1. Exploração de navegadores com reputação de URL;
4.2.2.2. Websites infectados com reputação de URL;
4.2.2.3. Office Exploits com reputação de URL;
4.2.2.4. Arquivos anexos com reputação de arquivos;
4.2.2.5. Download de arquivos com reputação de arquivos;
4.2.2.6. Instalação de software com as técnicas de SAPE — *Static Attribute Protection Engine*;
4.2.2.7. Instalação de software com as técnicas de Malheur;
4.2.2.8. Cópia de arquivos com as técnicas de SAPE — *Static Attribute Protection Engine*;
4.2.2.9. Cópia de arquivos com as técnicas de Malheur;
4.2.2.10. Execução do instalador de software com classificação comportamental do instalador (boa e ruim);
4.2.2.11. Execução do malware de software com classificação comportamental do instalador (boa e ruim);
4.2.2.12. A funcionalidade de "*Machine Learning*" deve trabalhar baseado no mínimo nas seguintes premissas:
4.2.2.12.1. Atualização da base de reputação das URL's com a periodicidade mínima de 2,5 horas;
4.2.2.12.2. Bloqueio de URL's de má reputação;
4.2.2.12.3. Bloqueio das instruções de "*Command & Control*";
4.2.2.12.4. Atualização da base de reputação de Arquivos com a periodicidade mínima de 2,5 horas;
4.2.2.12.5. Bloqueio das ameaças polimorfas mesmo que arquivos desconhecidos;
4.2.2.12.6. Prevenção de Falso Positivos;
4.2.2.12.7. Bloqueio de malwares desconhecidos e suas variantes;
4.2.2.12.8. Implementar a classificação comportamental dos arquivos;

4.2.2.12.9. “Aprendizado” a partir dos indicadores de compromisso (IOC).

4.2.3. A funcionalidade de "Machine Learning" deve ter a capacidade de implementar uma análise em tempo real correlacionando entre:

4.2.3.1. Veredicto das análises entre usuários da plataforma de segurança do mesmo fabricante;

4.2.3.2. Arquivos de softwares mundialmente espalhados na rede mundial de computadores;

4.2.3.3. Sites Web mundialmente espalhados pela rede mundial de computadores.

4.2.4. A funcionalidade de emulação para malware deve a partir do software de proteção de endpoint, implementar a emulação em um ambiente virtual (local) possibilitando detectar e impedir as técnicas de evasão de detecção, mesmo que utilizando polimorfismo no seu empacotamento;

4.2.5. A funcionalidade de emulação para malware deve ter suporte para as plataformas Windows (32 e 64 bits) e Linux (64 bits);

4.2.6. O software de proteção dos endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:

4.2.6.1. Adobe PDF;

4.2.6.2. Flash;

4.2.6.3. Java;

4.2.6.4. Navegadores (Internet Explorer, Microsoft Edge, Chrome e Firefox).

4.2.7. O software de proteção do endpoint deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:

4.2.7.1. SEHOP - *Structured Exception Handler Overwrite Protection*;

4.2.7.2. *Heap Spray* (Exploits que iniciam através do HEAP);

4.2.7.3. *Java Exploit Protection.*

4.2.8. O software de proteção do endpoint deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" para as aplicações;

4.2.9. O software de proteção do endpoint deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros, possibilitando no mínimo:

4.2.9.1. Capturas de Login e Logout na Gerência Central;

4.2.9.2. Captura dos detalhes das máquinas protegidas;

4.2.9.3. Captura dos detalhes de Domínios implementados pelo software;

4.2.9.4. Captura dos detalhes de Grupos implementados pelo software;

4.2.9.5. Captura da lista de "*Fingerprint*" de aplicações (*Blacklisting*);

4.2.9.6. Captura da atualização da lista de "*Fingerprint*" de aplicações (Blacklisting);
4.2.9.7. Captura dos detalhes das políticas aplicadas;
4.2.9.8. Captura das atualizações dos detalhes das políticas aplicadas;
4.2.9.9. Captura da lista dos usuários administradores da solução;
4.2.9.10. Criação de novos administradores da solução;
4.2.9.11. Capacidade de mover clientes de endpoints entre grupos lógicos.

4.2.10. O software de proteção do endpoint deve ter a capacidade de receber instruções de comando e ações diretamente do módulo de proteção contra ataques de APT (*Advanced Persistent Threats*), sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos;

4.2.11. A solução deve ter capacidade de implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

4.2.12. Deve possuir Console de Gerenciamento Centralizado:
4.2.12.1. O gerenciamento deve estabelecer uma correlação de eventos entre os softwares gerenciados, possibilitando priorização nas ações a serem tomadas;
4.2.12.2. Administração centralizada por console única de gerenciamento acessível através de tecnologia Web HTTPS;
4.2.12.3. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, Controle de Dispositivos e Controle de Aplicações deverão ser realizadas para máquinas físicas e virtuais através da mesma console;
4.2.12.4. A solução que será implantada para prestar os serviços deverá funcionar com agente único a ser instalado em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
4.2.12.5. Deve possuir mecanismo de comunicação (via *push*) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;
4.2.12.6. Deve possuir mecanismo de comunicação randômico (via *pull*) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;
4.2.12.7. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;
4.2.12.8. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 ou superior;
4.2.12.9. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32 bits e 64 bits

suportando, no mínimo, ambiente virtual VMware e Microsoft Hyper-V;

4.2.12.10. Possuir integração com LDAP, inclusive com o serviço de diretório Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

4.2.12.11. Possibilidade de aplicar regras diferenciadas baseando-se na localidade lógica da rede;

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

4.2.12.12.1. IP e range de IP;

4.2.12.12.2. Endereço de Servidores de DNS, DHCP e WINS;

4.2.12.12.3. Conexão com o servidor de gerência;

4.2.12.12.4. Conexões de rede como VPN, Ethernet e Wireless.

4.2.12.13. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

4.2.12.14. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;

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

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

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

4.2.12.18. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;

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

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

4.2.12.21. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

4.2.12.22. O console de gerenciamento deve permitir travar as configurações por senha nos clientes, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

4.2.12.23. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada um dos subitens de acesso as configurações do cliente;

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

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

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

4.2.12.27. Utilizar comunicação segura (criptografada) entre o servidor de gerenciamento e o cliente gerenciado;

4.2.12.28. Deverá fornecer acesso gráfico aos problemas, eventos e alertas detectados, com opção de salvaguardar os logs ou direcioná-los para um servidor syslog, além de oferecer mecanismos de emissão de alarmes via correio eletrônico, syslog e traps SNMPv3;

4.2.12.29. Todos os eventos gerados pela solução devem ser armazenados por um período configurável;

4.2.12.30. Deverá ser possível a criação, edição, habilitação, desativação e deleção de alertas customizados, com emissão via SNMPv3, para integração com outros sistemas de gerenciamento;

4.2.12.31. Deverá possuir integração com sistemas SIEM, para possibilitar coleta de logs de gerenciamento e correlação em “real-time”;

4.2.13. Atualização de Vacinas:

4.2.13.1. Atualização incremental, remota e em tempo real das vacinas do Antivírus e mecanismo de verificação (Engine) dos clientes da rede;

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

4.2.13.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

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

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

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

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

4.2.13.8. Possuir um único e mesmo arquivo de vacina de vírus para todas as plataformas Windows e versões do antivírus.

4.2.14. Quarentena:

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

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

4.2.14.3. Envio automático dos arquivos da área de isolamento para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. O recebimento da vacina deverá ocorrer da mesma forma que foi enviada e logo em seguida deverá ser aplicada nas estações de trabalho;

4.2.15. Cliente Gerenciado

4.2.15.1. Deve ter a capacidade de compor de forma nativa com a solução de APT do mesmo fabricante, sem a necessidade da implementação de scripts, utilizando apenas configurações realizadas no console padrão do produto;

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

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

4.2.15.3.1. Windows 7 ou superior;

4.2.15.3.2. Debian 8.0 ou superior;

4.2.15.3.3. Ubuntu 16.04 LTS ou superior.

4.2.15.4. O cliente para instalação em servidores deverá possuir compatibilidade com os sistemas operacionais:

4.2.15.4.1. Windows 2008 e superiores;

4.2.15.4.2. Debian;

4.2.15.4.3. Ubuntu Server;

4.2.15.4.4. CentOS 6 e superiores.

4.2.16. Deve possuir funcionalidade de Firewall e de Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

4.2.16.1. Suporte aos protocolos TCP, UDP e ICMP;

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

4.2.16.3. Possuir proteção contra exploração de buffer overflow;

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

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

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

4.2.16.7. Possibilidade de criar regras diferenciadas por aplicações;

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

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

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

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

4.2.16.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;

4.2.16.13. Gerenciamento integrado à console de gerência da solução.

4.2.17. Funcionalidade de Antivírus e AntiSpyware:

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

4.2.17.2. Proteção antispyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;

4.2.17.3. As configurações do antispyware deverão ser realizadas através da mesma console de todos os itens da solução;

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

4.2.17.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;

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

4.2.17.7. Permitir configurar a verificação contra ameaças para ser executada de maneira manual, agendada e em Tempo Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;

4.2.17.8. Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;

4.2.17.9. Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear;

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

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

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

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

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

4.2.17.15. Possuir funcionalidades de otimização de verificação (scaneamento) em ambientes virtuais, contemplando, no mínimo, as soluções de virtualização VMWare e Microsoft Hyper-V, para no mínimo:

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

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

4.2.17.15.2.1. Proteção de Antivírus e AntiSpyware;

4.2.17.15.2.2. Proteção de heurística e reputação de arquivos em tempo real (realtime);

4.2.17.15.2.3. Proteção de IPS de rede e "host";

4.2.17.15.2.4. Controle de dispositivos e aplicações;

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

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

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

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

4.2.17.18. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo às seguintes características:

4.2.17.18.1. Origem confiável;

4.2.17.18.2. Origem não confiável;

4.2.17.18.3. Tempo de existência do arquivo na internet;

4.2.17.18.4. Comportamento do arquivo;

4.2.17.18.5. Quantidade mínima de usuários que baixaram o arquivo da internet.

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

4.2.17.20. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados no cliente;

4.2.17.21. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;

4.2.17.22. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;

4.2.17.23. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados nos formatos ZIP, ARJ, LHA, RAR, TAR, GZIP e Microsoft Compress, no mínimo em 10 níveis de compactação;

4.2.17.24. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;

4.2.17.25. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;

4.2.17.26. Gerenciamento integrado à console de gerência da solução;

4.2.17.27. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

4.2.17.28. Capacidade de executar varreduras em tempo real (real time) contra ataques dirigidos a vulnerabilidades do navegador (browser);

4.2.17.29. Detecção e remoção de vírus de macro em tempo real;

4.2.18. Detecção Proativa de reconhecimento de novas ameaças:

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

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

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

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

4.2.18.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;
4.2.18.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Pró-Ativa com a base de reputação do fabricante;
4.2.18.7. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
4.2.18.8. Possibilidade de agendar o escaneamento da detecção Pró-Ativa com periodicidade mínima por minuto e em todos os novos processos;

4.2.19. Funcionalidade de Controle de Dispositivos e Aplicações:
4.2.19.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);
4.2.19.2. Controlar o uso de dispositivos com comunicação infravermelho, firewire, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;
4.2.19.3. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;
4.2.19.4. Gerenciamento integrado a console de gerência da solução;
4.2.19.5. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
4.2.19.6. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;
4.2.19.7. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para leitura, escrita e execução em Windows 7 e superiores, para no mínimo:
4.2.19.7.1. USB;
4.2.19.7.2. Firewire;
4.2.19.7.3. CD/DVD/BR;
4.2.19.7.4. SD Card;
4.2.19.7.5. eSATA.
4.2.19.8. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para Windows 7 e superiores, possibilitando regras de "white list" e "black list" utilizando expressões regulares, assim como, possibilidade de implementar teste de regras sem impactar na produção;
4.2.19.9. O software de proteção do endpoint deve ter a capacidade de implementar controle de dispositivos para Windows 7 e superiores, possibilitando administração por parte dos usuários e administração remota, com a possibilidade de monitoração e relatórios a partir da console de administração;

4.2.20. As funcionalidades de emissão de Relatórios e Monitoramento da solução deve possuir:

4.2.20.1. Pelo menos 25 tipos de relatórios diferentes, permitindo a exportação para os formatos PDF e HTML;

4.2.20.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

4.2.20.3. A capacidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status etc.);

4.2.20.4. A capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

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

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

4.2.20.4.3. Localização dos códigos maliciosos;

4.2.20.4.4. Sumários das ações realizadas;

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

4.2.20.4.6. Códigos maliciosos detectados.

4.2.21. Console avançada de distribuição e Relatórios

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

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

4.2.21.3. Detectar e desinstalar soluções de antivírus de no mínimo o seguinte fabricante:

4.2.21.3.1. F-Secure;

4.2.21.3.2. Kaspersky;

4.2.21.3.3. McAfee;

4.2.21.3.4. Sophos;

4.2.21.3.5. Symantec;

4.2.21.3.6. Trend Micro.

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

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

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

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

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

4.2.21.8.1. Alertas;

4.2.21.8.2. Clientes;

4.2.21.8.3. Políticas;
4.2.21.8.4. Rastreamento;
4.2.21.9. Exportar os relatórios criados nos formatos PDF e HTML.

4.2.22. Funcionalidades do Controle de Acesso à Rede:
4.2.22.1. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:
4.2.22.1.1. Computador deve possuir antivírus, atualizado e ativo;
4.2.22.1.2. Computador deve possuir firewall ativo;
4.2.22.1.3. Computador deve possuir antispyware, atualizado e ativo;
4.2.22.1.4. Computador deve possuir patches instalados, ativos e atualizados.
4.2.22.2. Deve ter a capacidade de iniciar à autorremediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;
4.2.22.3. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso à rede;
4.2.22.4. A auto remediação deve suportar download de programas e arquivos por links de HTTP, FTP e UNC;
4.2.22.5. Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação;
4.2.22.6. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não utilizam o agente (Máquinas não gerenciadas);
4.2.22.7. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não estiverem em conformidade com as políticas do controle de acesso à rede;

4.3. ITEM 2 – SOLUÇÃO ANTISPAM PARA CORREIO ELETRÔNICO (GATEWAY DE E-MAIL)

4.3.1. A Solução para Proteção de Gateway de E-mail deve integrar a captura eficiente de spams com baixa taxa de categorização das mensagens como falsos positivos. Implementado como gateway de e-mails, deve proteger e-mails e mensagens instantâneas contra vírus, spams, *phishing*, botnets e outros e-mails indesejados. Deve incorporar recursos flexíveis para o gerenciamento de spams e atualizações automatizadas de filtros.
4.3.2. Cada um dos nós com função de Gateway Antispam deve suportar os seguintes requisitos mínimos:

4.3.2.1. Função de Relay SMTP (*Simple Mail Transfer Protocol*), com recurso de antispam;
4.3.2.2. Capacidade de *throughput* de 4.000 (quatro mil) conexões SMTP simultâneas;
4.3.2.3. Capacidade de atendimento ao tráfego de e-mail gerado a partir 10.000 (dez mil) caixas postais de correio eletrônico, com taxa média de 15.000 (quinze mil) mensagens encaminhadas por hora;
4.3.2.4. Controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor;
4.3.2.5. Inspeção e bloqueio de mensagens baseados em tamanho de mensagem, volume de mensagens por período, número de destinatários por mensagem, número de destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP;
4.3.2.6. Implementação da tecnologia SPF (*Sender Policy Framework*), de modo a evitar que outros domínios enviem e-mails não autorizados em nome de um domínio;
4.3.2.7. Implementação da tecnologia DKIM (*Domain Keys Identified Mail*), de modo a prover mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas;
4.3.2.8. Proteção contra ataques de diretório (*Directory Harvest Attack*), técnica de busca, descoberta e validação de endereços de e-mail no domínio por força bruta;
4.3.2.9. Implementação de recursos de controle de taxa (*E-mail Throttling*), limitando a quantidade de e-mail aceitos de um emissor específico durante um período de tempo;
4.3.2.10. Implementação de recursos de verificação de DNS reverso para validação de domínio;
4.3.2.11. Filtragem de conteúdo de e-mails por meio de assinaturas para corpo e anexos de mensagens, heurística, filtro de reputação, URLs e filtros antiphishing;
4.3.2.12. Filtragem de conteúdo de e-mails, permitindo a concatenação por operações booleanas de regras de expressões regulares nos campos de cabeçalho SMTP, corpo, tamanho e anexos da mensagem;
4.3.2.13. Filtragem de e-mails baseada em lista negra e lista branca, globais e por usuário;
4.3.2.14. Remoção de corpo e anexos de mensagens;
4.3.2.15. Categorização de mensagens de saída a partir de políticas preestabelecidas;
4.3.2.16. Implementação de recurso de antivírus nativo;
4.3.2.17. Tratamento de mensagens com anexos contendo vírus, possibilitando o encaminhamento da mensagem sem o anexo infectado, bloqueio da mensagem e alerta ao destinatário do ocorrido;

4.3.2.18. Detecção de arquivos anexos, baseada em tipo, nome, extensão e formato MIME (*Multipurpose Internet Mail Extensions*);
4.3.2.19. Detecção de anexos compactados, em até 10 (dez) camadas de compactação, incluindo formatos ZIP e RAR, permitindo definir a ação a ser executada;
4.3.2.20. Detecção de anexos criptografados, permitindo definir a ação a ser executada;
4.3.2.21. Detecção de reputação de links que estejam dentro do corpo de mensagens;
4.3.2.22. Configuração de sensibilidade de risco de cada mensagem, permitindo definir limites para encaminhamento, "tageamento", não aceitação e quarentena de mensagens;
4.3.2.23. Implementação de recurso de quarentena por usuário, integrado e autenticado no Microsoft Active Directory;
4.3.2.24. Implementação de recurso de envio de notificação periódica para usuários acerca de mensagens de spam e em quarentena;
4.3.2.25. Implementação de recurso que permita o usuário administrar a sua própria quarentena;
4.3.2.26. Implementação de recurso de cadastro de lista negra branca pelo próprio usuário;
4.3.2.27. Implementação de configuração para bloqueio, encaminhamento, marcação e quarentena pelo próprio usuário;
4.3.2.28. Implementação de inserção de carimbo no assunto de mensagens e de texto no corpo de mensagens;
4.3.2.29. Implementação de inserção de header personalizado (*x-header*);
4.3.2.30. Gerenciamento por CLI (*Command-line interface*), SSH (*Secure Shell*), WebUI (*WEB User Interface*) via HTTPS (*Secure Hypertext Transfer Protocol*) e console gráfica centralizada;
4.3.2.31. Gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;
4.3.2.32. A solução pode ser instalada em ambiente virtualizado do CONTRATANTE ou disponibilizada por meio de hardware dedicado (*appliance*) fornecido pela CONTRATADA;
4.3.2.33. Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios;
4.3.2.34. Gerenciamento com visualização de status de serviços;
4.3.2.35. Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, *throughput* e desempenho dos serviços;
4.3.2.36. Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;
4.3.2.37. Gerenciamento com recurso de replicação de configurações e atualização de software;

4.3.2.38. Gerenciamento com recurso de monitoramento de logs e *debugging*;

4.3.2.39. Gerenciamento com recurso de backup e importação de arquivos de configuração;

4.3.2.40. Gerenciamento com recurso de emissão de relatórios, incluindo informações de quantidade de conexões, endereços IP, quantidade de e-mails, quantidade de spams, quantidade de vírus, volume de tráfego, performance, processamento e armazenamento;