

## ANEXO I

### 1. QUANTITATIVOS

#### 1.1. Serviços que compõem a solução:

Item	Descrição	Quantidade	Prazo
1	Serviços de suporte técnico, atualização de versões, correção de bugs, atualização de padrões de vírus e atualização de regras de filtragem de e-mails abrangendo as licenças da solução Symantec Protection Suite em uso na Polícia Federal (renovação), conforme requisitos descritos neste Termo de Referência.	Para 15.000 licenças.	12 meses

- 1.2. A justificativa da relação entre a demanda e a quantidade de serviço a ser contratada, nos termos do art. 15, §7º, inc. II, da IN nº 02/08 SLTI – MPOG, consta da Informação nº 0785308/2016-SST/DINF/CGTI/DLOG/PF, parte integrante dos autos.

### 2. REQUISITOS TECNOLÓGICOS DA SOLUÇÃO

- 2.1. Administração centralizada por console única de gerenciamento.
- 2.2. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, Controle de Dispositivos, Controle de Aplicações e Controle de Acesso a Rede deverão ser realizadas através da mesma console.
- 2.3. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos ou virtuais a fim de diminuir o impacto ao usuário final.
- 2.4. Console de gerenciamento via tecnologia Web (HTTP e HTTPS).
- 2.5. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.
- 2.6. Mecanismo de comunicação (via pull) em tempo determinado pelo administrador entre os clientes e servidor, para consulta de novas configurações e assinaturas.
- 2.7. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows 2003 Server R2, SP1 ou superior e Microsoft Windows Server 2008, 2008 R2 ou superior.
- 2.8. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32-bit e 64-bit suportando ambiente virtual VMWARE.
- 2.9. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos administradores.

- 2.10. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.
- 2.11. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:
  - 2.11.1. IP e range de IP;
  - 2.11.2. Endereço de Servidores de DNS, DHCP e WINS;
  - 2.11.3. Conexão com o servidor de gerência;
  - 2.11.4. Conexões de rede como VPN, Ethernet, Wireless e Modem.
- 2.12. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas.
- 2.13. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2005, 2008 e 2014.
- 2.14. Possuir recursos para a criação e agendamento periódicos de backups da base de dados.
- 2.15. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover.
- 2.16. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs).
- 2.17. 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.
- 2.18. Descobrir automaticamente as estações da rede que não possuem o cliente instalado.
- 2.19. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado, com opção de instalação remota.
- 2.20. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicas e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente.
- 2.21. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação.
- 2.22. Instalação e atualização do software sem a intervenção do usuário.
- 2.23. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha.
- 2.24. Suportar redirecionamentos dos logs para um servidor de Syslog.
- 2.25. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado.
- 2.26. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
- 2.27. Deve possuir integração com Active Directory, para autenticação de usuários da

solução.

- 2.28. Deve ter a capacidade de realizar atualização de versão e patches nos componentes da solução através da console de gerenciamento.
- 2.29. Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação.
- 2.30. Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes.
- 2.31. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados.
- 2.32. Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema.
- 2.33. Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados.
- 2.34. Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados.
- 2.35. Deve possuir logs detalhados de auditoria de alterações de políticas.
- 2.36. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas.
- 2.37. Permitir a instalação de Servidores de Gerenciamento adicionais, fornecendo assim a possibilidade de trabalho em redundância onde, no caso de falha de um dos servidores, o outro assume todas as funções da solução, sem provocar indisponibilidade para os endpoints.
- 2.38. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade no mínimo com os seguintes sistemas operacionais:
  - 2.38.1. Windows Server 2003 e superior;
  - 2.38.2. Windows Server 2008 e superior, 32 e 64 bits;
  - 2.38.3. Windows Server 2012 e superior, 32 e 64 bits;
  - 2.38.4. Windows XP, 32 e 64 bits;
  - 2.38.5. Windows Vista, 32 e 64 bits;
  - 2.38.6. Windows 7, 32 e 64 bits;
  - 2.38.7. Windows 8 e 8.1, 32 e 64 bits;
  - 2.38.8. Windows 10, 32 e 64 bits.
- 2.39. Os clientes gerenciados devem possuir certificação FIPS 140-2.
- 2.40. O fabricante deverá possuir as 30 últimas certificações VB100% (Vírus Bulletin) no mínimo nas plataformas Windows XP, Windows Vista, Windows 2003, 2008, 2008 R2, 2012, 7, 8, 8.1 e 10.
- 2.41. Permitir a instalação em máquinas virtuais sem impor nenhuma restrição ao

funcionamento e aos recursos e funcionalidades.

- 2.42. Caso a solução ofertada utilize SGBD – Sistema Gerenciadores de Bancos de Dados, este deverá ser fornecido como bundle, ou seja, já embutido no custo da solução.
- 2.43. Possibilitar o estabelecimento de alvos de políticas por filtros baseados em qualquer informação disponível sobre os clientes. Exemplos: configurações de sistema operacional, hardware, componentes, softwares e versões.
- 2.44. Clientes devem ser atualizados automaticamente nos grupos de políticas conforme a inclusão ou exclusão de clientes ou da mudança de suas configurações.
- 2.45. Implementar, na própria solução, código único para clientes, garantindo consistência para a base de dados mesmo com mudanças de hostname, endereço MAC da placa de rede, endereço IP ou outras informações nos clientes evitando a criação de registros duplicados.
- 2.46. Permitir forçar comunicação dos clientes a partir da console para atualizar as políticas e inventário.
- 2.47. Permitir a ativação e desativação do software cliente por meio da console de gerenciamento, sem necessidade de reinicialização do endpoint.
- 2.48. Permitir integração da solução com o Microsoft Active Directory, possibilitando, no mínimo, as seguintes tarefas:
  - 2.48.1. Importação e sincronização de usuários, computadores, sites, unidades organizacionais e grupos do Active Directory;
  - 2.48.2. Permitir ao administrador criar agendamentos e definir horários ou frequência de importação;
  - 2.48.3. Permitir a importação e sincronização diferencial, ou seja, apenas dos dados que apresentarem modificações em relação à última sincronização realizada, mantendo a alteração mais recente;
  - 2.48.4. Permitir autenticação de usuários da solução, permitindo atribuir papéis na utilização da console de gerência.
- 2.49. Aplicação de políticas baseadas em grupos de Active Directory.
- 2.50. Instalação automática do software cliente em computadores de grupos pré-definidos do Active Directory que ainda não estejam sendo gerenciados.
- 2.51. Permitir o agendamento de instalação, atualização e desinstalação do software cliente via políticas no servidor a partir da console de gerenciamento da solução sem necessidade de reinício (boot) dos endpoints e de forma silenciosa, ou seja, sem interação com usuário.
- 2.52. Flexibilidade para definição da frequência de comunicação cliente-servidor.

- 2.53. Controlar banda de rede utilizada pelo cliente na sua comunicação com o servidor utilizando:
  - 2.53.1. Configurações diferenciadas por faixa de horário;
  - 2.53.2. Bloquear a comunicação por faixa de horário para comunicação total entre cliente-servidor e download;
  - 2.53.3. Permitir configurar exceções para políticas.
- 2.54. Gerenciar a comunicação cliente-servidor com computadores:
  - 2.54.1. Na LAN e/ou WAN;
  - 2.54.2. Na Internet via VPN;
  - 2.54.3. Na Internet.
- 2.55. Suporte a múltiplos domínios independente de sua estrutura ou relacionamento de confiança.
- 2.56. Deverá permitir a definição de política geral que se aplique aos usuários que não estejam conectados à rede gerenciada pela instituição, para no mínimo:
  - 2.56.1. Prover capacidade de habilitar somente os aplicativos homologados pela instituição, enquanto conectados à rede gerenciada;
  - 2.56.2. Prover capacidade de separar a utilização dos aplicativos privados dos corporativos homologados.
- 2.57. Atualização incremental, remota e em tempo-real, das referências dos antivírus (assinaturas de vírus e outros códigos maliciosos) e do mecanismo de verificação (engine) dos clientes da rede.
- 2.58. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e servidores de gerenciamento, site do fabricante e via servidor de atualização interno, podendo eleger qualquer cliente gerenciado para distribuição das atualizações.
- 2.59. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função.
- 2.60. Atualização remota e incremental da versão do software cliente instalado.
- 2.61. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e nem requerer reinicialização do computador ou serviço para aplicá-la.
- 2.62. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.
- 2.63. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor,

utilizando opção e comando da console, podendo utilizar a arquitetura de grupos lógicos da console.

- 2.64. Um único e mesmo arquivo de definições de vírus para todas as plataformas Windows e versões do antivírus.
- 2.65. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede.
- 2.66. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento.
- 2.67. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as seguintes funcionalidades:
  - 2.67.1. Suporte aos protocolos TCP, UDP e ICMP;
  - 2.67.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;
  - 2.67.3. Possuir proteção contra exploração de buffer overflow;
  - 2.67.4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;
  - 2.67.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;
  - 2.67.6. Possibilidade de agendar a ativação da regra de Firewall;
  - 2.67.7. Possibilidade de criar regras diferenciadas por aplicações;
  - 2.67.8. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede, baseado no fingerprint do arquivo;
  - 2.67.9. Proteger o computador através da criação de um código digital (“digital fingerprint”) para cada executável existente no sistema, para que somente as aplicações que possuam esse código digital executem no computador;
  - 2.67.10. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;
  - 2.67.11. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
  - 2.67.12. Bloqueio de ataques baseado na exploração da vulnerabilidade;
  - 2.67.13. Gerenciamento integrado à console de gerência da solução;
  - 2.67.14. Possibilidades de criação de assinaturas de ataques no formato similar ao SNORT.
- 2.68. As funcionalidades de firewall pessoal e proteção de intrusão (IDS/IPS) deverão ser

nativos do cliente de gerenciamento, sem a necessidade de plugin, módulos ou agentes adicionais.

2.69. Funcionalidade de antivírus e anti-spyware as seguintes características:

- 2.69.1. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
- 2.69.2. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;
- 2.69.3. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;
- 2.69.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (adware, ferramentas hacker, acesso remoto, spyware, trackware e outros);
- 2.69.5. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixo, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;
- 2.69.6. Permitir verificação das ameaças de maneira manual, agendada e em tempo-real, detectando ameaças no nível do kernel do sistema operacional, fornecendo a possibilidade de detecção de rootkits;
- 2.69.7. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;
- 2.69.8. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook e POP3/SMTP;
- 2.69.9. Capacidade de detecção em tempo real de vírus novos, de assinatura desconhecida, com opção de seleção da sensibilidade da detecção (baixo, médio e alto);
- 2.69.10. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou IP da origem, com opção de bloqueio da comunicação via rede;
- 2.69.11. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;
- 2.69.12. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e Microsoft, para no mínimo:
  - 2.69.12.1. Diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;
  - 2.69.12.2. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas,

para no mínimo:

- 2.69.12.2.1.1. Proteção de antivírus e anti-spyware;
- 2.69.12.2.1.2. Proteção de heurística e reputação de arquivos em tempo real (real-time);
- 2.69.12.2.1.3. Proteção de IPS de rede e “host”;
- 2.69.12.2.1.4. Controle de dispositivos e aplicações.
- 2.69.13. Cache local de reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;
- 2.69.14. Capacidade de verificar “templates” de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (template);
- 2.69.15. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
- 2.69.16. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
- 2.69.17. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:
  - 2.69.17.1. Origem confiável;
  - 2.69.17.2. Origem não confiável;
  - 2.69.17.3. Tempo de existência do arquivo na internet;
  - 2.69.17.4. Comportamento do arquivo;
  - 2.69.17.5. Quantidade mínima de usuários que baixaram o arquivo da internet;
- 2.70. Capacidade de implementar regras distintas por grupo (ex. departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo.
  - 2.70.1. Funcionalidade de detecção proativa de reconhecimento de novas ameaças, com as seguintes funcionalidades:
  - 2.70.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória, por comportamento dos processos e arquivos das aplicações;
  - 2.70.3. Não utilizar a assinatura de vírus para esta funcionalidade e realizar atualização periódica das técnicas de detecção;
  - 2.70.4. Capacidade de detecção de keyloggers, trojans, spyware e worms por comportamento dos processos em memória, com opção de seleção de sensibilidades distintas de detecção;



- 2.70.5. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo hosts;
  - 2.70.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção proativa com base na reputação do fabricante;
  - 2.70.7. Possibilidade de agendar o escaneamento da detecção proativa com periodicidade mínima por minuto e em todos os novos processos;
  - 2.70.8. As funcionalidades da detecção proativa deverão ser nativas do cliente, sem a necessidade de plugin, módulos ou agentes adicionais.
- 2.71. Funcionalidade de Controle de Dispositivos e Aplicações:
- 2.71.1. 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 pen drive);
  - 2.71.2. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;
  - 2.71.3. Gerenciamento integrado à console de gerência da solução;
  - 2.71.4. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
  - 2.71.5. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação.
- 2.72. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:
- 2.72.1. As 10 máquinas com maior ocorrência de códigos maliciosos;
  - 2.72.2. Os 10 usuários com maior ocorrência de códigos maliciosos;
  - 2.72.3. Localização dos códigos maliciosos;
  - 2.72.4. Sumários das ações realizadas;
  - 2.72.5. Número de infecções detectadas diário, semanal e mensal;
  - 2.72.6. Códigos maliciosos detectados;
  - 2.72.7. Os arquivos mais bloqueados;
  - 2.72.8. As chaves de registro mais bloqueadas;
  - 2.72.9. Os processos mais bloqueados;
  - 2.72.10. Os dispositivos mais bloqueados;
  - 2.72.11. As dll's mais bloqueadas.
- 2.73. Funcionalidade de Controle de Acesso a Rede com os seguintes requisitos:
- 2.73.1. Verificar periodicamente, em intervalos definidos pelo administrador, se o

computador possui antivírus, firewall, antispyware e patches instalados e atualizados, de acordo com a política definida, realizando o bloqueio de acesso à rede aos computadores que não estiverem de acordo com essa política;

- 2.73.2. Capacidade de iniciar a auto-remediação do computador que falhou a verificação, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;
  - 2.73.3. As funcionalidades do controle de acesso à máquina deverão ser nativas do cliente de gerenciamento, sem a necessidade de plugin, módulos ou agentes adicionais;
  - 2.73.4. Se necessário o uso de appliance o mesmo deverá ser fornecido sem custo adicional;
  - 2.73.5. Deverá possuir integração nativa na mesma console de gerenciamento do antivírus permitindo as funcionalidades de deployment, upgrade e relatórios;
  - 2.73.6. Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso a rede;
  - 2.73.7. Deve permitir verificar se o firewall está instalado e inicializado na máquina cliente;
  - 2.73.8. Deve possibilitar as verificações customizadas, minimamente com operadores lógicos, “IF”, “ELSE”, “THEN”, “AND”, “OR e NOT”, para no mínimo, os seguintes critérios:
    - 2.73.8.1. Pesquisa de chave de registro;
    - 2.73.8.2. Versão do sistema operacional;
    - 2.73.8.3. Idioma do sistema operacional;
    - 2.73.8.4. Patch instalado;
    - 2.73.8.5. Comparar versão, data, tamanho e "fingerprint" de arquivos;
    - 2.73.8.6. Além dos quesitos onde mencionam verificações de firewall e antivírus nos itens e subitens acima.
  - 2.73.9. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não utilizam o agente (máquinas não gerenciadas);
  - 2.73.10. Deve ter a possibilidade de não aceitar a comunicação ponto a ponto entre máquinas que não estiverem em conformidade com as políticas de controle de acesso à rede.
- 2.74. Proteção de mensagens corporativas (e-mails):
- 2.74.1. Deve suportar Cluster Ativo/passivo da solução Exchange;
  - 2.74.2. Deve ser compatível com Exchange Server 2007, 2010 e 2013;

- 2.74.3. Deve ser compatível com VSAPI versões 2.0, 2.5 e 2.6;
- 2.74.4. Deve ser compatível com ambientes virtuais VMWARE;
- 2.74.5. Deve permitir instalação remota;
- 2.74.6. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para mensagem específica, sem necessidade de integração com produtos de terceiros ou “open source”;
- 2.74.7. Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior, em todos os appliances/equipamentos da solução ofertada;
- 2.74.8. Deve permitir realizar o rastreamento da mensagem, conforme citado anteriormente, utilizando caracteres double-byte para línguas estrangeiras;
- 2.74.9. Deve possuir funcionalidade de criação de alias e mascaramento de endereço;
- 2.74.10. Deve ser possível realizar notificação do administrador por email caso os filtros antispam não recebam atualizações por um determinado período de tempo;
- 2.74.11. Deve ser capaz de integração com LDAP, Microsoft Active Directory 2008 e Microsoft Active Directory 2012 para sincronização e autenticação;
- 2.74.12. Deve permitir a criação de políticas diferenciadas para tratamento de spam, vírus, filtragem de conteúdo e controle de reputação, de acordo com o destinatário da mensagem e reputação de origem;
- 2.74.13. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento de usuários válidos e ações de vírus, spam e filtragem de conteúdo diferenciadas por grupo do LDAP;
- 2.74.14. Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos e possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;
- 2.74.15. Deve possuir mecanismos de backup/restore da configuração existente na solução;
- 2.74.16. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;
- 2.74.17. Deve permitir a criação de pastas de conformidade ("compliance folders"), para armazenagem de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo administrador;
- 2.74.18. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for

categorizada como spam ou violação dos filtros de conteúdo, entre elas:

- 2.74.18.1. Apagar mensagem;
  - 2.74.18.2. Enviar para quarentena;
  - 2.74.18.3. Encaminhar mensagem;
  - 2.74.18.4. Encaminhar em BCC;
  - 2.74.18.5. Gravar mensagem em disco;
  - 2.74.18.6. Gravar em pasta de conformidade;
  - 2.74.18.7. Modificar o assunto;
  - 2.74.18.8. Adicionar informações ao cabeçalho;
  - 2.74.18.9. Deferir a mensagem;
  - 2.74.18.10. Rejeitar a mensagem.
- 2.74.19. Deve ter a capacidade de verificação em tempo real de SMTP;
- 2.74.20. Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;
- 2.74.21. Deve ter a capacidade de verificação manual dos message stores;
- 2.74.22. Deve ter a capacidade de verificação agendada dos message stores;
- 2.74.23. Deve permitir verificar mailbox stores e public folders;
- 2.74.24. Deve permitir definir a “idade mínima” das mensagens a serem verificadas;
- 2.74.25. Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:
- 2.74.25.1. Tempo máximo de verificação;
  - 2.74.25.2. Número máximo de decomposição de arquivos compactados recursivamente;
  - 2.74.25.3. Tamanho máximo do arquivo descompactado;
  - 2.74.25.4. Número máximo de arquivos descompactados.
- 2.74.26. Deve ser capaz de, quando a mensagem for gravada em pasta de conformidade, permitir definir ações distintas para as mensagens aprovadas e reprovadas;
- 2.74.27. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;
- 2.74.28. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);
- 2.74.29. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);
- 2.74.30. Deve possuir centro especializado, com funcionamento 24 horas por dia, 7 dias por semana, com monitoramento de mais de 2 milhões de mailboxes, para processamento de spams recebidos e criação automática de novos filtros/assinaturas;

- 2.74.31. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;
- 2.74.32. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;
- 2.74.33. Deve ter a capacidade de bloquear mensagens consideradas como spam baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);
- 2.74.34. Deve ter a capacidade de reconhecimento de ameaças dia-zero, com assinatura de suspeitos de vírus;
- 2.74.35. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:
  - 2.74.35.1. Assinaturas para corpo da mensagem e anexos;
  - 2.74.35.2. Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;
  - 2.74.35.3. Filtros de reputação local (criados automaticamente através da análise das mensagens recebidas) e global (criados pela rede de monitoramento do fornecedor da solução);
  - 2.74.35.4. Identificação de idiomas;
  - 2.74.35.5. Filtros de URLs;
  - 2.74.35.6. Filtros anti-phishing.
- 2.74.36. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;
- 2.74.37. Deve possuir tecnologia para detecção de ataques de spam, vírus e diretório (usuários inválidos);
- 2.74.38. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;
- 2.74.39. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o controle do percentual de mensagens que serão recusadas;
- 2.74.40. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;
- 2.74.41. Deve possuir tecnologia para prevenção de ataques de “Bounce Messages”;
- 2.74.42. Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;
- 2.74.43. Deve possuir a capacidade para criação de regras baseadas no tipo de arquivo

anexado;

- 2.74.44. Deve possuir a capacidade para criação de regras baseadas na detecção por “wildcard”;
- 2.74.45. Deve possuir a capacidade para criação de regras baseadas na detecção por expressões regulares;
- 2.74.46. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);
- 2.74.47. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;
- 2.74.48. Deve ter capacidade de detecção de pelo menos os idiomas Inglês, Francês, Espanhol, Árabe e Português, permitindo o bloqueio de mensagens escritas nos idiomas não desejados;
- 2.74.49. Deve possuir capacidade de criar uma lista de IP’s confiáveis baseada no comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;
- 2.74.50. Deve possuir a capacidade de atualização automática periódica da lista de IP’s confiáveis, citada no item anterior;
- 2.74.51. Deve ter a capacidade de deleção total de mensagens enviadas por “Mass-Mailing Worms”, com opção de ações diferenciadas por tráfego de entrada e saída;
- 2.74.52. Deve ter a capacidade de reconhecimento de spywares e adwares;
- 2.74.53. Deve possuir recurso para detecção dos ataques de duas escalas para vírus e diretório (LDAP), capaz de suspender a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;
- 2.74.54. Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;
- 2.74.55. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo;
- 2.74.56. Deve ter a capacidade de implementar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são spam, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;
- 2.74.57. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica

para os usuários, informando as mensagens consideradas como spam que foram inseridas na quarentena (“digest”);

- 2.74.58. Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;
- 2.74.59. Deve permitir que o usuário cadastre endereços de e-mail em listas negras/listas brancas pessoais;
- 2.74.60. Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do órgão;
- 2.74.61. Deve ter capacidade de integração com servidor de criptografia, para criptografar mensagens e anexos;
- 2.74.62. Deve ter a capacidade de permitir ou não endereços de e-mail com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8 bits;
- 2.74.63. Deve ter a capacidade de rejeitar conexões que tentem ser abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS;
- 2.74.64. Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;
- 2.74.65. Deve ter a capacidade de implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual;
- 2.74.66. Deve ter a capacidade de instalar servidores de gerenciamento, monitores e scanners adicionais, fornecendo assim a possibilidade de trabalhar em Load Balance e Failover;
- 2.74.67. Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;
- 2.74.68. Deve ter a capacidade de integração com solução de Data Loss Prevention, para os e-mails de saída, possibilitando utilização de mais de um servidor de DLP, para um mesmo Gateway de SMTP;
- 2.74.69. Deve ter a capacidade de priorização de servidores de DLP utilizados na integração com o Gateway de SMTP, possibilitando balancear o tráfego a ser analisado.

### **3. TRANSFERÊNCIA DE TECNOLOGIA**

- 3.1. A presente contratação visa manter a continuidade de serviços atualmente prestados, portanto, não há necessidade de transferência de tecnologia.

#### 4. NÍVEIS DE SERVIÇO E PENALIZAÇÕES

4.1. A CONTRATADA deverá atender aos Níveis de Serviços apresentados na tabela a seguir, com prazos definidos segundo a severidade do chamado/solicitação:

Severidade	Descrição	Prazo máximo para resposta inicial	Prazo máximo para restauração do serviço	Prazo máximo para fornecimento de solução mais completa e/ou permanente
Severidade 1 (Alta)	<p>Sistema parado ou produto inoperante com impacto nas operações críticas de negócio.</p> <p><u>Exemplos:</u></p> <ul style="list-style-type: none"> <li>- Servidor de produção, sistema ou serviço importante está inativo.</li> <li>- Parte significativa de dados importantes corre risco de perda ou corrupção.</li> <li>- Operações relacionadas ao negócio da Polícia Federal foram severamente afetadas.</li> <li>- A solução causa falha na rede ou sistema que compromete a integridade do sistema ou dos dados, causando impacto significativo nas operações em curso em ambiente de produção da Polícia Federal.</li> </ul>	Em até 15 minutos um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Até 8 (oito) horas.	Até 6 (seis) dias.
Severidade 2 (Média/Alta)	<p>Alto impacto no ambiente de produção ou grande restrição de funcionalidade.</p> <p><u>Exemplo:</u></p> <ul style="list-style-type: none"> <li>- Problema no qual uma funcionalidade importante foi severamente debilitada. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.</li> </ul>	Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Até 24 (vinte e quatro) horas.	Até 10 (dez) dias.
Severidade 3 (Média/Baixa)	<p>O problema não gera alto impacto ao negócio.</p> <p><u>Exemplo:</u></p> <ul style="list-style-type: none"> <li>- Problema que causou impacto negativo limitado nas operações relacionadas ao negócio da Polícia Federal.</li> </ul>	Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	—	Até 15 (quinze) dias e/ou na próxima atualização de software.



Severidade 4 (Baixa)	<p>O problema é pequeno ou de documentação.</p> <p><u>Exemplos:</u></p> <ul style="list-style-type: none"> <li>- O problema não afetou negativamente as operações relacionadas ao negócio da Polícia Federal;</li> <li>- Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento da solução contratada.</li> </ul>	No próximo dia útil	_____	Até 20 (vinte) dias ou considerado para as próximas atualizações de software.
-------------------------	---	---------------------	-------	---

- 4.2. Em caso de não atendimento por parte da CONTRATADA de prazos definidos na tabela de Nível de Serviços (item anterior), devem ser aplicadas as penalizações à CONTRATADA definidas na tabela a seguir, até o limite mensal de 30% do valor mensal do Contrato, sem prejuízo das demais sanções contratuais:

Criticidade	Penalização
1	1,00 % do valor mensal do contrato por cada hora que exceder o prazo de 8 (oito) horas para a restauração do serviço.
	0,50 % do valor mensal do contrato por cada dia que exceder o prazo de 6 (seis) dias para o fornecimento de solução mais completa e/ou permanente para o problema.
2	0,60 % do valor mensal do contrato por cada hora que exceder o prazo de 24 (vinte e quatro) horas para a restauração do serviço.
	0,30 % do valor mensal do contrato por cada dia que exceder o prazo de 10 (dez) dias para o fornecimento de solução mais completa e/ou permanente para o problema.
3	-----
4	-----

- 4.3. Não serão computados nos prazos para a resposta a incidentes nas soluções contratadas previstos na tabela do item 4.1 o tempo dispendido em ações necessárias para viabilizar o atendimento que sejam de responsabilidade exclusiva do CONTRATANTE.