# PROJETO BÁSICO

## SUPES - 02174/2017

**Consulta pública para Aquisição de Solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound).**

### 1.0 Objeto

**1.1.** Aquisição de Solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound).

### 2.0 Especificação do objeto a ser contratado

**2.1.** Aquisição de Solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound) com as seguintes características:
2.1.1. Deverá integrar a captura eficiente de spams com baixa taxa de categorização das mensagens como falsos positivos;
2.1.2. Implementado como gateway de segurança de e-mails, a solução deve proteger e-mails contra malware, vírus, spams, phishing, business e-mail compromise ataques (BEC) e outras ameaças inerente ao ambiente de mensagens eletrônicas;
2.1.3. Tratar e analisar mensagens originadas e recebidas (inbound e outbound), no mesmo equipamento, possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego.
2.2. Serão necessárias 110.000 (cento e dez mil) licenças para atender o atual ambiente de correio eletrônico, para atender o SERPRO e clientes, com previsão de crescimento;

> OBSERVAÇÃO: Será tratado durante a consulta pública com os participantes o modelo de contratação para definição, ou não, da previsão de crescimento.

**2.3.** O licenciamento deverá ser por caixas postais de usuário, não considerando listas, grupos de distribuição e e-mails de sistemas, assim como o fluxo de recebimento e envio;

**2.4.** A solução deverá permitir nativamente o roteamento de mensagens eletrônicas entre tecnologias e servidores de e-mail distintos, respondendo pelo mesmo domínio, ou seja, ex: usuário A@dominio.gov.br utiliza um correio X e o usuário B@dominio.gov.br utiliza um correio Y, onde ambos respondem pelo mesmo domínio.

**2.5.** Permitir a autorização de quantidade ilimitada de endereços de IPs no ambiente para envio de mensagens (Relay).

**2.6.** A solução deverá ser apresentada na forma de Appliance Virtual (conjunto de máquina virtual, sistema operacional e aplicação) compatível com a plataforma VMWARE:
2.6.1.1. Deverá suportar plataforma de virtualização VMWARE VSphere versão 6 ou superior;
2.6.1.2. A solução deverá ser composta por sistema operacional dedicado e otimizado para esta finalidade , desenvolvido e licenciado pelo próprio fabricante.
2.6.1.3. As atualizações de software e segurança de todos os softwares que compõem a solução (Aplicações e Sistema Operacional) deverão ser homologadas e disponibilizadas pelo fabricante;
2.6.1.4. Deverá ser escalável e não ter custo adicional caso seja necessário instalar vários appliances virtuais para agregar desempenho ou alta disponibilidade à solução.

**2.7.** Deve permitir alta disponibilidade das funções de filtragem de maneira assegurar que não haja interrupção no serviço por falha da solução;

**2.8.** Capacidade de replicação automática das configurações entre os agentes de roteamento de mensagens e consoles de gerência e balanceamento de carga, de forma nativa;

**2.9.** Disponibilizar, durante a vigência da licença, o upgrade para a última versão estável do produto, sem custos adicionais;

**2.10.** A solução entregue deverá suportar a expansão de funcionalidades tais como: Data Loss Prevention (DLP),compliance e criptografia por meio de aquisição e ativação de licenças, sem a necessidade de aquisição de novos equipamentos de hardware e software de terceiros.

**2.11. Características gerais da solução**
2.11.1. Suportar no mínimo 10.000 (dez mil) conexões do protocolo Simple Mail Transfer Protocol (SMTP) simultâneas;
2.11.2. Processar, no mínimo, 100.000 (cem mil) mensagens por hora, com filtros básicos, mais funcionalidades de AntiVírus e filtro de reputação, levando em conta um tamanho médio de mensagem de 15 Kbytes;
2.11.3. Prover um mecanismo de proteção multicamadas que permita a análise de conexão, consulta de reputação global, bem como análise de conteúdo e estatística;
2.11.4. Inspecionar as mensagens eletrônicas, no mínimo, por meio dos seguintes métodos:
2.11.4.1. Assinaturas de URL;
2.11.4.2. Filtros de vírus;
2.11.4.3. Filtros de anexos;
2.11.4.4. Filtros de phishing;
2.11.4.5. Endereço IP;
2.11.4.6. Análise de reputação do remetente;
2.11.4.7. Análise heurística;
2.11.4.8. Análise do envelope, cabeçalho, corpo, estrutura, conteúdo não estruturado e formatação, bem como anexo das mensagens;
2.11.4.9. Análise contextual, léxico e baseado em imagem;
2.11.4.10. Suporte a vários idiomas, dentre eles os de dois bytes (double byte);
2.11.4.11. E-mail bounce (retorno de mensagem não enviada pelo usuário);
2.11.4.12. Dicionários pré-definidos e customizados com palavras e expressões regulares.
2.11.5. Permitir configurar o “greeting” SMTP e definição de timeout de conexão SMTP;
2.11.6. Capaz de limitar o número máximo de conexões simultâneas e por Daemon SMTP;
2.11.7. Possuir habilidade de controlar as sessões SMTP e limitar o tráfego de mensagens, baseado em endereço IP, Range de IPs, Subnet IP, nome de domínio, nome parcial de domínio e reputação do emissor;
2.11.8. Possibilitar rate limit controlado por endereço de IP, domínio ou reputação do emissor;
2.11.9. A solução deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um IP, fazendo a função de “SMTP Rate Control” com base em: volume de vírus, de spam e de remetentes inválidos, permitindo ao administrador configurar a sensibilidade de cada um dos gatilhos.
2.11.10. Deve ser capaz de controlar o número máximo de destinatários de um determinado emissor, por endereço IP, domínio, nome reverso, saudação SMTP ou país;
2.11.11. Capaz de restringir conexões baseado em tamanho máximo de mensagem, número máximo de destinatários por mensagem, número máximo de mensagens por conexão, número máximo de conexões simultâneas por IP;
2.11.12. Possibilitar a verificação de DNS reverso para conexões;
2.11.13. A solução deve ofertar possibilidade de ter domínio mascarado (Masquerade Domains);
2.11.14. Possuir integração com serviço de diretórios padrão protocolo LDAP - Lightweight Directory Access Protocol (Request For Coments 4511) para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack”), sem a necessidade de modificar os parâmetros “default” do serviço de diretórios;

2.11.15. Permitir a utilização de mais de um servidor de LDAP, para autenticação dos usuários, caso ocorra indisponibilidade do servidor primário de LDAP;
2.11.16. Deve possuir capacidade de implementar comunicação segura via Transport Layer Security (TLS);
2.11.17. Deverá ser capaz de bloquear ataques de negação de serviço (Denial of Service) diretamente na solução;
2.11.18. Rejeitar a conexão SMTP que se caracterize como "flooding";
2.11.19. Permitir a inclusão de múltiplas listas de remetentes bloqueados em tempo real ("real-time black list-RBL"), permitindo regras de bloqueio se o IP estiver presente em “n” listas, configurável pelo administrador;
2.11.20. Possuir funcionalidade de verificação de SPF (Sender Policy Framework), permitindo regras individuais e customizadas para usuários ou grupos de usuários, permitindo criar ações específicas para “fail” e “soft fail”, conforme descrito pelo Comitê Gestor da Internet no Brasil, no sítio: http://www.antispam.br/admin/spf;
2.11.21. Possuir controle de e-mail bounce (retorno de mensagem não enviada pelo usuário), passível de configuração pelo administrador;
2.11.22. Ter capacidade de bloquear conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, armazenagem e otimização do processamento, em especial baseado em lista local de bloqueio, RBLs e SPF;
2.11.23. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
2.11.24. Deve permitir a instalação automática ou manual de patches de sistema e/ou segurança;
2.11.25. A atualização automática das definições de malware, SPAM e outros módulos, em intervalo de tempo configurado pelo administrador, permitindo atualizações de no mínimo, 5 em 5 minutos;
2.11.26. Deve possuir mecanismos de backup e restore da configuração existente na solução, com possibilidade de enviar a um servidor remoto através da interface gráfica.

**2.12. Gerenciamento**
2.12.1. O gerenciamento de políticas de segurança, políticas de anti-spam, URLs, filtros, domínios, diretórios e rastreamento de mensagens deve ser realizado através de interface gráfica web única, de forma segura (HTTPS) sem a necessidade de utilizar linha de comando.
2.12.2. A solução deve possuir console de gerenciamento através de linha de comando segura (SSH),nativo do sistema operacional, para todas as funcionalidades e o SERPRO poderá ter acesso de “super usuário” para identificação de problemas e criação de scripts;
2.12.3. A solução deve possuir console de gerenciamento através de linha de comando segura (SSH), nativo do sistema operacional, para todas as funcionalidades;
2.12.4. Suportar o gerenciamento e replicação de políticas do cluster (servidores interligados formando uma estrutura de computação) de forma centralizada a múltiplos appliances virtuais através de uma única interface gráfica;
2.12.5. A solução deverá permitir a criação de novos administradores com privilégios de gerenciamento granular a pelo menos os seguintes módulos:
2.12.5.1. Administração;
2.12.5.2. Antispam;
2.12.5.3. Antivírus,
2.12.5.4. Filas de processamento de mensagens eletrônicas;
2.12.5.5. Filtro de conteúdo;
2.12.5.6. Módulo de anexos;
2.12.5.7. E-mail firewall.
2.12.6. Tratar e analisar mensagens originadas e recebidas (inbound e outbound), no mesmo appliance, possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;
2.12.7. A solução deverá permitir a administração granular por Virtual IP e Virtual Host com as seguintes funcionalidades:
2.12.7.1. Possuir a capacidade de criação de endereços IP virtuais para os fluxos de mensagens de entrada e de saída;
2.12.7.2. Permitir que um único appliance possa segmentar o fluxo de e-mail por diferentes IPs

Virtuais e Domínios;
2.12.7.3. Permitir múltiplos domínios por endereço IP, ou múltiplos domínios utilizando diferentes IPs no mesmo appliance;
2.12.8. Prover funcionalidade de cópia de segurança e restauração das configurações da solução;
2.12.9. Prover funcionalidade de armazenagem e retorno de, no mínimo, as 5 (cinco) últimas mudanças de configuração, sem interrupção (restauração de backup) do serviço;
2.12.10. Permitir importar as contas dos administradores através do Microsoft Active Directory (AD) e outros diretórios padrão protocolo LDAP com capacidade de sincronização das senhas;
2.12.11. Permitir o rastreamento de mensagens, independente de qual appliance processou, de forma centralizada e por meio da interface gráfica de gerenciamento HTTPS;
2.12.12. O rastreamento deve ser possível através do: remente, destinatário, assunto da mensagem, nome do anexo, nome do vírus, regra de bloqueio, identificador da mensagem (ID), host ou IP de envio e horário de entrega da mensagem, com a possibilidade de customizações;
2.12.13. O resultado do rastreamento deve informar: o remetente e destinatários da mensagem, o servidor de origem, se foi quarentenada, se continha vírus, a regra que atuou, o tamanho da mensagem e se foi entregue;
2.12.14. O rastreamento deve apresentar o registro de log com as evidências da entrega da mensagem, ou erros caso não tenha sido entregue;
2.12.15. Capacidade de auditar as ações realizadas pelos administradores da solução, independente do perfil;
2.12.16. A solução deverá disponibilizar configuração de alertas por meio da interface gráfica e enviá-los por mensagens de correio eletrônico;
2.12.17. Os alertas enviados deverão ser no mínimo os listados abaixo:
2.12.17.1. Componentes da solução não estão respondendo ou funcionando;
2.12.17.2. Espaço em disco;
2.12.17.3. Alertas de hardware;
2.12.17.4. Problemas relacionados a fila de entrada e saída, bem como quantidade de mensagens em fila;
2.12.17.5. Erros de sincronização com os serviços de diretórios;
2.12.17.6. Falhas relacionadas a atualização de patchs e base de assinaturas de spam e vírus;
2.12.17.7. Erros na consulta de reputação.
2.12.18. A solução deverá prover funcionalidade de configuração do nível de registro de logs ("log level") das ocorrências geradas pela solução (Crítico, Erro, Informação ou Detalhado);
2.12.19. Deverá prover a capacidade de exportar os logs para produção de relatórios por outros programas;
2.12.20. A solução deverá prover suporte a Syslog e a capacidade de encriptação dos dados no envio por meio do protocolo Transport Layer Security (TLS);
2.12.21. Deverá possuir sistema de diagnóstico na interface gráfica, contendo os seguintes testes:
2.12.21.1. Conectividade por IP ou hostname;
2.12.21.2. Envio de mensagem eletrônica;
2.12.21.3. Teste de lookup de email, via LDAP (para verificação de conectividade com servidor LDAP ou AD);
2.12.21.4. Status do sistema (Principais logs de eventos, uso de memória, disco, lista de processos do sistema e configuração de rede).

**2.13. Recursos de proteção e higienização**
2.13.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de proteção contra ameças, executando simultaneamente;
2.13.2. Na análise de SPAM deve resultar a probabilidade heurística da mensagem ser no mínimo:
2.13.2.1. SPAM;
2.13.2.2. E-mail Marketing (Bulk ou Graymail).
2.13.3. Possibilitar o bloqueio de maus remetentes e definir políticas individuais por remetente (tanto externo quanto interno) baseado em:
2.13.3.1. IP emissor;
2.13.3.2. Range de IP;

2.13.3.3. Domínio;
2.13.3.4. Reputação do emissor;
2.13.3.5. Verificação DNS.
2.13.4. A solução deve conter proteção específica para ataques do tipo “Phishing”;
2.13.5. Permitir a aplicação de políticas de SPAM diferentes por Nome de Domínio do destinatário, Grupo de destinatários e por destinatário específico, integrando-se com AD, Azure AD, Domino Directory e outros diretórios que atendam ao protocolo LDAP;
2.13.6. Suportar filtros de conexões providos pelo próprio fabricante, que deverão ser executados no início da conversação SMTP, com recomendações de, no mínimo: passar, rejeitar, tentar novamente e atrasar entrega;
2.13.7. Permitir filtros internos de “lista branca” e “lista negra” por endereços IP, Nome Reverso, bem como domínio e endereço, tanto de remetente, quanto de destinatário, permitindo o uso de expressões regulares;
2.13.8. Permitir regras para aumentar ou diminuir a probabilidade de identificar o SPAM, com base em critérios internos, permitindo definir, no mínimo: idioma da mensagem, país de origem, endereço de domínio, IP e reverso do remente;
2.13.9. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, podendo ser habilitados simultaneamente ou não;
2.13.10. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail);
2.13.11. Possuir módulo de detecção “Zero Day” para a identificação de novas ameaças desconhecidas pelo antivírus, colocando em determinada área da quarentena por período de tempo customizável, até nova verificação pelo antivírus, após disponibilização de vacina;
2.13.12. Permitir regras específicas e distintas para bloqueio de surtos de vírus (outbreak);
2.13.13. Capacidade de realizar em caso de vírus no mínimo as seguintes ações simultaneamente:
2.13.13.1. Alterar o assunto da mensagem;
2.13.13.2. Adicionar cabeçalhos e etiquetas para rastreamento;
2.13.13.3. Descartar a mensagem;
2.13.13.4. Mover para área específica de quarentena conforme configurado pelo administrador da solução;
2.13.13.5. Notificar o remetente e/ou destinatário com uma mensagem customizável, informando o nome do vírus.
2.13.14. Possibilitar quarentena automática de anexos criptografados;
2.13.15. Criar rota customizada para permitir entrada de anexos criptografados para entrega a determinados grupos de e-mails;
2.13.16. Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com diretórios que utilizam o protocolo LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas;
2.13.17. Possibilitar customizações de regras e políticas por usuários ou grupos;
2.13.18. Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de antivírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários;
2.13.19. A solução deverá permitir a configuração do intervalo de sincronismo entre a solução antispam e o serviço de diretório;
2.13.20. Prover mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente;
2.13.21. Prover suporte ao envio e recebimento de mensagens utilizando protocolo TLS e SSL, permitindo configurar domínios onde TLS é mandatório;
2.13.22. Prover a assinatura das mensagens de saída com chave DKIM;
2.13.23. Fazer a análise de cabeçalho (header) nos padrões RFC 822;
2.13.24. Permitir a aplicação de regras baseadas no idioma que as mensagens foram escritas, com capacidade para, no mínimo, identificar Português, Inglês e Espanhol;
2.13.25. Permitir a aplicação de regras baseadas no país de origem do e-mail;
2.13.26. Controlar mensagens com base em dicionário de palavras com suporte a expressão regular e pontuação máxima por palavra, atuando de forma independente no conteúdo do anexo, do corpo do e-mail e do assunto;

2.13.27. Controlar conexões nos seguintes níveis, mediante configuração:
2.13.27.1. Número de mensagens por conexão;
2.13.27.2. Número de conexões simultâneas;
2.13.27.3. Número de destinatários por mensagem;
2.13.27.4. Tamanho das mensagens;
2.13.27.5. Tempo de processamento da mensagem;
2.13.27.6. Controlar mensagens com anexos com base em:
2.13.27.6.1. Mime Type (Tipo de extensões “Multi função” para mensagens de Internet);
2.13.27.6.2. Tipo real do arquivo;
2.13.27.6.3. Nome do arquivo;
2.13.27.6.4. Tamanho de anexo;
2.13.27.6.5. Quantidade de anexos;
2.13.27.6.6. Anexos compactados com senha;
2.13.27.6.7. Quantidade de camadas de arquivos compactados, um dentro do outro;
2.13.27.6.8. Todas as configurações devem ser granulares para domínios, grupos e usuários específicos;
2.13.27.6.9. Tomar, no mínimo, as seguintes ações:
2.13.27.6.9.1. Remover o anexo;
2.13.27.6.9.2. Alterar o assunto da mensagem;
2.13.27.6.9.3. Adicionar cabeçalhos para rastreamento;
2.13.27.6.9.4. Descartar a mensagem;
2.13.27.6.9.5. Colocar em uma determinada área da quarentena definida pelo administrador;
2.13.27.6.9.6. Notificar o remetente e/ou destinatário com uma mensagem customizável;
2.13.27.6.9.7. Solução deverá prover a funcionalidade de incluir avisos (disclaimers) no início ou no rodapé das mensagens enviadas;
2.13.27.6.9.8. A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório padrão protocolo LDAP;
2.13.27.6.9.9. A solução deverá suportar a configuração dos “disclaimers” em formato html ou texto;
2.13.28. Deverá possuir funcionalidade de bloqueio de servidores Spammers através dos recursos de Domain Keys Identified Mail (DKIM) e Sender Policy Framework (SPF);
2.13.29. Deverá implementar o padrão Domain-based Message Authentication, Reporting and Conformance (DMARC);
2.13.30. Rejeitar mensagens para destinatários inválidos durante o diálogo SMTP, para prevenir NonDelivery Report Attack;
2.13.31. Suportar o gerenciamento de bounces permitindo a criação de regras específicas, bem como a possibilidade do o uso de chaves criptográficas para assinar as mensagens de saída;
2.13.32. Suporte ao recurso Bounce Address Tag Validation (BATV) para etiquetar as mensagens de saída e validar os NDRs e garantir proteção contra inundações de bounce.

**2.14. Quarentena**
2.14.1. Possuir áreas de quarentena no próprio appliance de acordo com as políticas de proteção, contendo no mínimo as seguintes áreas:
2.14.1.1. Spam;
2.14.1.2. Bulk OU Graymail;
2.14.1.3. Phish;
2.14.1.4. Malware;
2.14.1.5. Vírus;
2.14.1.6. Anexos;
2.14.1.7. Audit;
2.14.1.8. Spoofed;
2.14.1.9. Zerohour.
2.14.2. Suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos;
2.14.3. O tempo de armazenamento da quarentena deve ser configurável e individual por área de quarentena;
2.14.4. Possibilitar ao administrador selecionar o período de expiração das mensagens na

quarentena, na qual o sistema automaticamente começará a apagar os e-mails mais antigos, de acordo com a configuração (nunca, dias, horas, semanas ou mês);
2.14.5. Possibilitar a visualização do resumo de todas as áreas da quarentena, informando o tamanho de cada área, volume de mensagens e tempo de expiração;
2.14.6. Permitir ao administrador da solução executar pesquisa nas mensagens em quarentena de todos os usuários através de interface web segura (HTTPS), acessando a própria solução, sem necessidade de nenhum software ou hardware adicional;
2.14.7. Possibilitar o gerenciamento da quarentena pelo administrador, com a identificação do motivo do bloqueio, origem e destino da mensagem, data, assunto, IP do host que enviou, a mensagem e seu tamanho, podendo liberar, excluir, mover ou processar novamente as mensagens;
2.14.8. Para garantir o sigilo da informação, permitir que determinadas áreas de quarentena somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas áreas.

**2.15. Relatórios e estatísticas**
2.15.1. Capacidade de gerar diversos relatórios da solução de forma centralizada e por uma única console;
2.15.2. Permitir gerar e enviar por e-mail relatórios automatizados, por meio de agendamento;
2.15.3. Permitir seleção de dados para geração de relatórios por data específica ou intervalo de tempo, com granularidade de hora;
2.15.4. Possibilidade de configurar o período de retenção de dados para produção de relatórios;
2.15.5. Os relatórios devem ser disponibilizados em formato de gráfico, bem como em tabelas com dados dispostos em linhas e colunas;
2.15.6. Disponibilizar, pelo menos, os seguintes tipos de relatórios:
2.15.6.1. Relatórios sobre volume e tipo de spam recebido;
2.15.6.2. Maiores domínios que enviam spam;
2.15.6.3. Maiores remetentes de vírus;
2.15.6.4. Maiores remetentes de spam por conexão IP;
2.15.6.5. Endereços de e-mails que mais recebem spam;
2.15.6.6. Volume de conexões por agentes de roteamento de mensagens;
2.15.6.7. Relatório de throughput de mensagens;
2.15.6.8. Rejeitadas por reputação e controle de conexão;
2.15.6.9. Número total de mensagens em quarentena;
2.15.6.10. Usuários que mais liberam mensagens.
2.15.7. Sumário com o total de mensagens que foram classificadas:
2.15.7.1. Spam;
2.15.7.2. Vírus
2.15.7.3. Bloqueadas por políticas;
2.15.7.4. Mensagens válidas.
2.15.8. Possuir funcionalidade de exibição de estatísticas no formato “dashboard” para acompanhamento do fluxo de e-mails, com a possibilidade de customizar quais gráficos serão exibidos de maneira individual para cada administrador da ferramenta, contendo no mínimo:
2.15.8.1. Informações sobre recursos do appliance;
2.15.8.2. Informações sobre a “estado” dos agentes, serviços e módulos que compõem a solução;
2.15.8.3. Informações sobre mensagens, conexões, bem como bloqueio de spam e vírus.

**2.16. Resumo de Bloqueio de Mensagens (Digest)**
2.16.1. O envio do Digest deverá ocorrer em dias e horários estabelecidos e configurados pelo administrador;
2.16.2. O Digest deverá ser enviado em Língua Portuguesa do Brasil e seu conteúdo ter a possibilidade de customização;
2.16.3. Suporte para no mínimo as seguintes línguas: Português do Brasil, Inglês e Espanhol;
2.16.4. Suporte a Digest responsivo;
2.16.5. O Digest deverá permitir ao usuário liberar a mensagem bloqueada;
2.16.6. A interface do usuário final deverá estar no idioma “Português do Brasil”;
2.16.7. Capacidade em definir perfis e políticas de filtragem de SPAM por usuário ou grupo de

usuários, bem como quais usuários receberão ou não o resumo de e-mails bloqueados;
2.16.8. Possuir interface Web de administração segura (HTTPS) para que o usuário final possa administrar suas opções pessoais, sem que estas opções interfiram na filtragem dos demais usuários;
2.16.9. O usuário final poderá incluir e remover endereços em sua lista pessoal de bloqueio (“Lista negra”) ou de liberação de e-mails (“Lista branca);
2.16.10. O usuário final poderá visualizar as mensagens bloqueadas e liberá-las, a seu critério.

**2.17. Sistema de Segurança contra Ataques Dirigidos**
2.17.1. O fabricante da solução deverá possuir um centro de pesquisa e desenvolvimento em segurança focado em identificação de vulnerabilidades, manutenção de inteligência de segurança em escala global, descoberta de ameaças exploradas e criação de mecanismos de contenção e resposta a ataques;
2.17.2. O sistema de proteção contra ataques dirigidos deverá implementar:
2.17.2.1. Análise de e-mail em tempo real incluindo as propriedades da mensagem;
2.17.2.2. Assegurar que links de URLs suspeitas sejam dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto, deverá ser exibido uma notificação de bloqueio;
2.17.2.3. A inspeção de URLs deve utilizar várias fontes de informação, incluindo o centro de inteligência do fabricante;
2.17.2.4. Realizar análises de anomalias e de malware e aplicar controles adicionais às mensagens suspeitas.
2.17.3. A solução deve suportar análise dinâmica ou sandboxing inclusive, em ambiente segregado da rede cliente, entregando um resumo e relatório completo da análise realizada;
2.17.4. Caso o processo de análise dinâmico seja realizado em infraestrutura em nuvem do fabricante, este deve explicar como a privacidade das informações é mantida;
2.17.5. Deve suportar análise dinâmico ou sandboxing que seja resistente a técnicas de evasão e, quando observadas tais tentativas, deve reportar a ocorrência nas amostras avaliadas;
2.17.6. Suportar a detecção de todos os tipos de malwares, ambos conhecidos e desconhecidos. Capacidade de rastrear o movimento de todos os malwares e reportar de forma detalhada.
2.17.7. A solução deverá oferecer serviços de reputação de conteúdo Web e identificação de ameaças Zero Day com recurso centralizado de inteligência em nuvem (cloud);
2.17.8. Deverá possuir filtro de reputação com as funcionalidades:
2.17.8.1. O sistema de reputação deverá checar a reputação dos remetentes em redes participantes com cobertura global;
2.17.9. Os filtros de reputação baseados em URL, deverão permitir:
2.17.9.1. Verificação de reputação e categoria de URLs incluídas nas mensagens enviadas e recebidas, como critério adicional na ajuda da detecção de spams e conteúdos maliciosos;
2.17.10. Permitir modificar as URLs nas mensagens, impossibilitando o clique do usuário, substituindo por texto ou redirecionando para proxy de avaliação da URL antes da liberação ou bloqueio do acesso, caso seja considerado malicioso ou contra a política de acesso;
2.17.11. Possibilitar o controle de tráfego de e-mail por reputação atribuída pela rede de reputação, de cada IP que solicitou uma conexão;
2.17.12. As informações da rede de reputação devem ser utilizadas durante a análise das mensagens pelo filtro de anti-spam;
2.17.13. A solução deverá colocar em quarentena mensagens que contenham um anexo, compactados ou não, com código de vírus desconhecido e automaticamente remover a mensagem da quarentena se não houver detecção utilizando as mais novas atualizações (incluindo recursos dinâmicos) do mecanismo contra infecções;
2.17.14. Deverá permitir de forma automática um processo de análise contínuo de arquivos utilizando atualizações do centro de inteligência contra ameaças para identificar mudanças no veredito de arquivos analisados previamente;
2.17.15. A solução deverá ser capaz de rastrear os movimentos de malware, conhecidos ou não, com relatórios detalhados com suporte a pesquisa e análise contínua para auxiliar análise de incidentes;
2.17.16. Deverá ser possível habilitar ou desabilitar a proteção URL baseada em rotas específicas configuradas no mínimo pelas seguintes condições: Sender, Recipient, Dominios, Sender IP

Address, ou usuários via LDAP;
2.17.17. A proteção de URL deverá identificar se URL é maliciosa e redirecionar o usuário para uma página com uma notificação de bloqueio e ter a opção para descartar o e-mail;
2.17.18. A proteção de URL deverá ser capaz de reescrever os links do e-mail, inclusive os que foram classificados como suspeitos, e a cada clique, após a exibição de uma tela de notificação, a solução deverá analisar a URL e, contatando que não são maliciosos, redirecionar para a URL original;
2.17.19. A proteção de URL deverá ser capaz de analisar a categoria do conteúdo e redirecionar o usuário para uma tela de notificação. Essa funcionalidade deve ser implementada inclusive quando a URL não puder ser classificada e a solução deverá classificar a cada clique;
2.17.20. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site será bloqueado no navegador;
2.17.21. Cada mensagem deverá consultar o serviço na nuvem para testes em sandbox que definirá uma pontuação (score) para a mensagem;
2.17.22. A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita;
2.17.23. A proteção de URL deverá reescrever links para os protocolos HTTP, HTTPS e FTP, URL's que comecem com “www” independente do protocolo.
2.17.24. A solução deverá permitir que o administrador gerencie quais URL's serão reescritas e como serão exibidas nas mensagens de e-mail;
2.17.25. A solução deverá permitir que o administrador configure o sistema de proteção URL reescrevendo todas as mensagens que contiverem URL e redirecionando para um serviço de inspeção e bloqueio, em caso de conteúdo malicioso, ou liberação que deverá ser registrada;
2.17.26. Permitir lista de exceções de URL para que não sejam reescritas;
2.17.27. Deverá ser possível configurar a reescrita de URLs em mensagens de e-mail com base na pontuação, com objetivo de encontrar um equilíbrio entre segurança e usabilidade;
2.17.28. Capacidade de reescrever URLs com base no modulo de detecção de anomalias nas mensagens que contenham link;
2.17.29. O relatório deverá fornecer visibilidade sobre ataques identificados com base em URL e ameaças de malware.
2.17.30. O relatório deverá prover painel (dashboard) que destaque todos os ataques e ameaças de malware detectados, podendo ser filtrados por período de tempo, exibindo a quantidade de mensagens bloqueadas, liberadas, URLs reescritas e bloqueadas, quando na tentativa de acesso pelo usuário;
2.17.31. O Dashboard deverá exibir a linha do tempo (timeline) das ameaças, exibindo o período que foi recebida, identificada e quando foi clicada ou liberada;
2.17.32. Deverá ser possível buscar o rastreamento a partir de uma URL ou malware presentes em mensagens com informações detalhadas;
2.17.33. Capacidade de disponibilizar sistema de coleta de amostra para o centro mundial de inteligência contra ameaças do fabricante para análises;
2.17.34. O sistema deverá gerar relatório das ameaças e enviar por e-mail. O relatório deverá exibir informações resumidas de todas as principais ameaças detectadas no momento da geração do mesmo.

**2.18. Funcionalidades compatíveis com a solução**
2.18.1. Suportar a implantação de módulo de compliance que permita aplicar tratamentos para mensagens que violarem as regras definidas, com as ações de bloqueio, quarentena e auditoria;
2.18.2. Suportar a implantação de módulo de compliance que possua a funcionalidade de cadastrar um determinado dicionário, a escolha do administrador, bem como, possuir dicionários pré-configurados, na própria solução, para controles das regras;
2.18.3. Suportar a implantação de módulo de compliance que possibilite alteração de cabeçalho da mensagem, quando violarem as regras;
2.18.4. Suportar a implantação de modulo de criptografia na saída de e-mails, que trabalhe de maneira transparente ao usuário, sem a necessidade de instalação de plugins, agentes ou outro tipo de software e possua interface para o destinatário customizável;

2.18.5. Suportar a implantação de módulo de criptografia com logs de auditoria de todas as transações envolvendo mensagens criptografadas;
2.18.6. Possibilitar ao administrador definir qual mensagem deverá ser criptografada, com base, no mínimo, em assunto, destinatário, remetente e anexo;
2.18.7. Possibilitar ao administrador integrar o DLP com a criptografia, de modo a que os e-mails sigilosos somente sejam enviados criptografados;
2.18.8. Permitir a utilização de criptografia das mensagens, geradas por chaves independentes;
2.18.9. Impossibilitar o uso de cache de browser para acesso as mensagens criptografadas;
2.18.10. O sistema deverá permitir que o modelo das mensagens criptografadas possam ser customizadas;
2.18.11. Ser capaz de criptografar mensagens localmente através de criação de regras que especifiquem quais mensagens devem ser criptografadas. As regras deverão ser de acordo com a necessidade do domínio, no mínimo por destinatário, remetente, conteúdo de anexos ( no mínimo PDF, Word, Excel ), assunto ou corpo do e-mail, caracteres no header da mensagem;
2.18.12. Possibilidade de criar perfis diferentes para cada regra específica de mensagens a serem criptografadas;
2.18.13. O método de criptografia utilizado não deve depender da instalação de softwares ou plugins na máquina do remetente ou do destinatário;
2.18.14. Permitir gerar chaves por mensagem impossibilitando que a chave de uma mensagem possa abrir outra mensagem, mesmo que para o mesmo destinatário;
2.18.15. Possibilitar que a mensagem seja entregue em um anexo criptografado e somente a chave deverá ser transmitida entre o servidor e o destinatário em um acesso seguro do tipo Secure Socket Layer (SSL);
2.18.16. Suportar 2 (dois) níveis de segurança de acesso na leitura das mensagens criptografadas:
2.18.16.1. Nível alto: O receptor da mensagem deverá entrar com as credenciais de senha todas as vezes que abrir a mensagem, mesmo que a senha esteja em cache;
2.18.16.2. Nível Baixo: A senha não é requisitada se estiver em cache, ou seja, caso o receptor tenha aberta a mensagem uma vez, não será necessário digitar novamente ao reabrir a mensagem enquanto a senha estiver em cache.
2.18.17. Suportar no mínimo os seguintes algoritmos de criptografias:
2.18.17.1. AES 192 bits;
2.18.17.2. RC4 160 bits.
2.18.17.3. Suportar o padrão Federal Information Processing Standards (FIPS);
2.17.17.4. Permitir que os receptores das mensagens criptografadas possam responder e/ou encaminhar à mensagem de forma criptografada, para garantir a segurança da informação;
2.18.17.5. As regras de mensagens a serem criptografadas devem estar de acordo com as normas de conformidade, tais como:
2.18.17.5.1. Health Insurance Portability and Accountability Act (HIPAA);
2.18.17.5.2. Sarbanes Oxley (SOX);
2.18.17.5.3. Gramm-Leach-Blilley Act (GLB);
2.18.17.5.4. Personal Information Protection and Electronic Documents Act (PIPEDA);
2.18.18. O sistema deverá suportar os seguintes controles das mensagens enviadas:
2.18.18.1. O remetente poderá cancelar a chave da mensagem antes mesmo que o destinatário receba a mensagem;
2.18.18.2. O remetente poderá configurar um tempo de expiração da chave e, caso o tempo tenha expirado, a mensagem não poderá ser aberta;
2.18.18.3. O sistema deverá enviar notificação de leitura da mensagem, assim que o destinatário acesse a chave para abertura da mensagem;
2.18.18.4. As mensagens não deverão ser armazenadas no servidor de chaves ou no appliance de criptografia;
2.18.18.5. Possuir console única de gerenciamento para interface de criptografia, compliance, antispam e antivírus, ou seja, para todos os módulos exigidos e suportáveis da solução.

2.19. Local da Instalação:

REGIONAL BRASÍLIA/DF
ENDEREÇO: SGAN AV. L2 NORTE, QUADRA 601 MÓDULO “G” - BRASÍLIA/DF
CEP: 70.836-900
CNPJ: 33.683.111/0002-80

## 3.0 Níveis de serviço e sancionamentos

**3.1.** Para as licenças instaladas serão prestados serviços de manutenção, atualização e suporte técnico pelo período de 36 (trinta e seis) meses a partir do recebimento definitivo.

3.1.1. Possuir atendimento, durante a vigência da prestação de serviços, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana (à exceção dos chamados de Severidade 4).

3.1.2. O atendimento aos chamados deverá obedecer a seguinte classificação quanto ao nível de severidade:

| Severidade | Descrição | Tipo de Atendimento | Tempo de Atendimento | Tempo de Solução ou Solução de contorno | Observações | Penalidades |
|---|---|---|---|---|---|---|
| 1 - Crítica | Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado | Remoto / On-Site | No máximo 1 (uma) hora após a abertura do chamado | No máximo 12 (doze) horas após a abertura do chamado | Se após 1 (uma) hora de iniciado o atendimento remoto ao chamado o ambiente afetado não estiver restabelecido, a CONTRATADA deverá iniciar, em até 2 (duas) horas do início do atendimento remoto, o atendimento presencial por um especialista devidamente habilitado, que trabalhará o tempo que for necessário para a solução do problema, sem ônus para o SERPRO.<br><br>O atendimento não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda em | O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,5% (cinco décimos por cento) do valor anual do item no contrato, por hora ou fração de hora de atraso. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | períodos noturnos e dias não úteis. | |
| 2 - Alta | Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho | Remoto / On-Site | No máximo 2 (duas) horas após a abertura do chamado | No máximo 48 (quarenta e oito) horas após a abertura do chamado | Se após 2 (duas) horas de iniciado o atendimento remoto ao chamado o ambiente afetado não estiver restabelecido, a CONTRATADA deverá iniciar, em até 2 (duas) horas a contar do início desse prazo de 48 (quarenta e oito) horas, o atendimento on-site por um especialista devidamente habilitado, que trabalhará o tempo que for necessário para a solução do problema, sem ônus para o SERPRO.<br><br>O atendimento não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda em períodos noturnos e dias não úteis. | O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,4% (quatro décimos por cento) do valor anual do item no contrato, por hora ou fração de hora de atraso. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 - Média | Chamados referentes a situações de baixo impacto, ou para aqueles problemas que se apresentem de forma intermitente | Remoto | No máximo 4 (quatro) horas após a abertura do chamado | No máximo 72 (setenta e duas) horas após a abertura do chamado | Os chamados classificados com severidade 3 serão atendidos em horário comercial, ou seja, das 8 às 18 horas, de segunda-feira a sexta-feira, horário local. | O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,2% (dois décimos por cento) do valor anual do item no contrato, por hora ou fração de hora de atraso. |
| 4 - Baixa | Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto | Remoto | No máximo 24 (vinte e quatro) horas após a abertura do chamado | No máximo 120 (cento e vinte) horas após a abertura do chamado | Os chamados classificados com severidade 4 serão atendidos em horário comercial, ou seja, das 8 às 18 horas, de segunda-feira a sexta-feira, horário local. | O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,1% (um décimos por cento) do valor anual do item no contrato, por hora ou fração de hora de atraso. |

3.1.3. Em quaisquer casos, e quando necessário, a CONTRATADA deverá assistir remotamente na instalação e no uso das licenças instaladas, fornecendo orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs. Nos casos de defeitos não conhecidos, as documentações enviadas pelo SERPRO (tais como: traces, dumps e logs) deverão ser encaminhadas aos laboratórios dos produtos a fim de que sejam fornecidas as devidas correções.

3.1.4. Em quaisquer casos, e quando necessário, a CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção.

3.1.5. Quando necessário, a CONTRATADA deverá fornecer auxílio na solução de problemas relativos à instalação, customização e performance do Sistema Operacional, Sistema Gerenciador de Banco de Dados e demais opcionais ofertados.

**3.2. Canais de atendimento:**

3.2.1. Atendimento e chamado técnico através de canal telefônico gratuito 0800, ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e por meio de site na Internet para o chamado técnico.

**3.3. Entrega mensal de relatórios.**

3.3.1. Mensalmente deverá ser entregue um relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período, por regional, com no mínimo as seguintes informações: número do contrato, período de referência, número de acionamento, descrição da ocorrência, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora do início de atendimento local, se for o caso, data e hora de encerramento ou contorno e descrição da resolução adotada. O relatório deverá ser entregue mesmo quando não houver chamados no período.

**3.4. Monitoramento do atendimento dos chamados**

3.4.1. Todos os chamados deverão ser controlados por sistema de informação da CONTRATADA.

3.4.2. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

3.4.3. A CONTRATADA deverá cadastrar pelo menos duas pessoas, indicadas pelo SERPRO, apenas essas pessoas estarão autorizadas a abrir e fechar os chamados.

## 4.0 Especificação de valores e forma de pagamento

**4.1.** O valor total estimado para a contratação das licenças, para o período de 36 (trinta e seis) meses, é de R$ xxxxxxxxxxxxxxxxxxxxxxxx

**4.2.** Os pagamentos referentes às contratações serão efetuados no 1º (primeiro) dia útil após o 20º (vigésimo) dia corrido da data do recebimento definitivo dos produtos, referentes a(s) nota(s) fiscal(is) entregue(s) no Protocolo Geral do SERPRO ou por meio do endereço eletrônico a ser informado pelo Gestor do Contrato.

OBSERVAÇÃO: Será tratado durante a consulta pública com os participantes o modelo de contratação por uso (on-demand), ou seja, para pagamento mensal das licenças utilizadas em nosso parque.

**4.3. Local de Pagamento**

REGIONAL BRASÍLIA/DF

ENDEREÇO: SGAN AV. L2 NORTE, QUADRA 601 MÓDULO “G” - BRASÍLIA/DF

CEP: 70.836-900

TELEFONE: (61) 2021-9000

FAX: (61) 2021-9806

INSCRIÇÃO ESTADUAL:  07334743/002-94

INSCRIÇÃO MUNICIPAL: 07334743/002-94

CNPJ: 33.683.111/0002-80

## 5.0 Justificativa da contratação

5.1. Esta consulta pública está autorizada pelo SISCOR SUPES 038259/2017-71 (cópia em anexo).

5.2. A presente consulta pública tem como objetivo prospectar junto ao mercado a contratação de uma solução de segurança de e-mail (Secure E-mail Gateway do tipo enterprise, com recursos de AntiSpam, AntiPhishing e AntiMalware.

5.3. Por meio da Consulta Pública, visamos obter feedback do mercado quanto ao atendimento dos requisitos funcionais e não funcionais desejados pelo SERPRO para a aquisição uma solução de segurança de e-mail (Secure E-mail Gateway do tipo enterprise, com recursos de AntiSpam, AntiPhishing e AntiMalware.

5.4. Do exposto e considerando que a realização de uma consulta ao Mercado seja de extrema importância para a continuidade e sucesso do Projeto, bem como para garantir os princípios da contratação pública, tais como o da publicidade (ampla concorrência), da isonomia (igualdade), da economicidade, da eficiência e do interesse público, entre outros, peço deferimento da presente solicitação.

## 6.0 Seleção do fornecedor (

### 6.1. Modalidade da Contratação

6.1.1. Em atendimento ao estabelecido na Lei 10.520/2002, no que couber, à Lei 13.303/2016, Art. 32, Inciso IV, assim entendido por decorrência dos padrões de desempenho e qualidade estarem objetivamente definidos por meio de especificações usuais do mercado, a contratação deverá ser na Modalidade de Pregão, na forma Eletrônica.

6.1.2. Será considerada ganhadora do processo licitatório a LICITANTE que estiver habilitada e apresentar a proposta com o menor preço global para o total de licenças contratadas, baseando-se na tabela de referência.

### 6.2. Da comprovação e documentação

6.2.1. Fornecer, junto com a proposta, documento em papel timbrado da empresa vencedora, relacionando os nomes dos produtos ofertados, especificar agentes caso sejam fornecidos, tipo de licenciamento de cada produto e agente, part number (quando for o caso), quantidades, valor

unitário, valor total de cada produto, bem como dos serviços e demais componentes ofertados se for o caso, valor total da proposta, local, data e assinatura, a qual deverá ser parte integrante do contrato.

6.2.2. Fornecer, junto com a proposta, atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove a aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação.

6.2.3. Fornecer, junto com a proposta, comprovação por meio de declaração, com firma reconhecida do signatário, de que a LICITANTE é revenda autorizada do fabricante para fornecer o licenciamento objeto deste processo.;

6.2.4. A CONTRATADA deverá comprovar, por ocasião da entrega, a origem dos bens importados e a quitação dos respectivos tributos de importação, sob pena das sanções previstas em contrato.

## 7.0 Justificativa para aceitação de preços

Não se Aplica

## 8.0 Gerenciamento contratual

### 8.4. OBRIGAÇÕES DA CONTRATADA

8.4.1. Cada licença dos produtos que constam na presente contratação deverão ter a suas respectivas identificações COA. (Certificate of Authenticity).

8.4.2. A CONTRATADA deverá garantir ao SERPRO o direito de todas as atualizações das ferramentas adquiridas e descritas.

8.4.3. A CONTRATADA fornecerá ao SERPRO as licenças contratadas e deverá permitir a aplicação de patches, fixes e demais correções para as versões adquiridas, bem como atualização de versões durante o prazo de prestação de serviços das licenças contratadas;

8.4.4. A vigência deste contrato será de 36 (trinta e seis) meses, prorrogáveis até o limite de 60 (sessenta) meses.

8.4.4.1 A prestação de serviços será de 36 (trinta e seis) meses a partir do recebimento definitivo, e não se confunde com a vigência do contrato.

8.4.5. Juntamente com as licenças, a CONTRATADA disponibilizará ao SERPRO acesso eletrônico ao site oficial internet do fabricante dos produtos ofertados, com acesso à documentação técnica completa e atualizada dos produtos, manuais técnicos, guias de instalação, inicialização, operação, adequação, implementação de segurança e criptografia, mensagens auxiliares para solução de problemas, diagnósticos, especificações e outros pertinentes, todos redigidos em português do Brasil ou em inglês. A CONTRATADA deverá informar endereço eletrônico.

8.4.6. O resultado das análises, todas as informações levantadas dos serviços realizados, bem como as soluções implementadas pelo SERPRO, em caráter algum, poderão ser divulgados.

8.4.7. Para atualizações de programas disponíveis, a CONTRATADA enviará no endereço especificado pelo SERPRO ou disponibilizará para baixar (download) uma cópia de atualização para cada sistema operacional suportado, desde que previamente solicitados pelo SERPRO e desde que os serviços de atualizações de Licenças de Software e Suporte estejam em vigor. O SERPRO fará a instalação das atualizações.

8.4.8. Prestar orientações em casos de problemas em programas e diagnóstico para auxiliar na identificação da causa de um problema, devendo fornecer informações sobre correções ou a própria correção, e nos casos dos defeitos não conhecidos, reenviar as documentações recebidas aos laboratórios dos produtos a fim de que os mesmos possam fornecer as devidas soluções ou soluções de contorno dentro dos prazos estabelecidos.

8.4.9. Entregar anualmente à Gestão de Contratos Relatório de Atualizações, listando o histórico, orientado pela data mais recente, de todas as atualizações das licenças contratadas destinadas por direito ao SERPRO.

**8.5.** O SERPRO poderá fazer a migração das licenças contratadas para uso em qualquer uma das suas regionais, sede e escritórios, bem como utilizar as licenças em qualquer servidor de qualquer localidade de sua capilaridade, respeitando a quantidade de licenças adquiridas.

**8.6.** O SERPRO não assinará qualquer contrato adicional com o fabricante para o recebimento das licenças decorrentes deste processo, ficando a CONTRATADA obrigada a efetuar os seus pedidos cientes desta condição. O único contrato a ser assinado será o administrativo com a CONTRATADA.

## 9.0 Considerações gerais

9.1. A consulta pública será acompanhada pelos empregados:

9.1.1. Herlon Clayton Paggi Hernandes, Matrícula: 2105402-9, Ramal: (11) 2173-1247, Email:. herlon.hernandes@serpro.gov.br;

9.1.2. Fernando Antonio Marques, telefone (61) 2021-8382, e-mail: fernando.marques@serpro.gov.br;

9.1.3. Francisco do Nascimento Silva Junior, telefone (61) 2021-8608, email: francisco.silva@serpro.gov.br.