

**Termo de Referência SUPES 02019/2019****Título****Consulta Pública para Aquisição de Solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound)****1ª Versão****Vinculação com Documento de Oficialização de Demanda**

Número DOD	Título da Demanda	Número do Item	Nome do Objeto	Descrição
2018-00019	INSTRUMENTO CONTRATUAL SEM ÔNUS E CONSULTA PÚBLICA	2	CONSULTA PÚBLICA	

**1.0 Objeto**

Consulta Pública para 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. 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;

2.1.2. 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 100.000 (cem mil) licenças para atender o atual ambiente de correio eletrônico, para atender o SERPRO e clientes, com 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 de forma nativa o roteamento de mensagens eletrônicas, entre tecnologias e servidores de e-mail distintos, respondendo pelo mesmo domínio, ou seja, ex: usuário user1@dominio.gov.br utiliza um correio de fabricante X e o usuário user2@dominio.gov.br utiliza um correio de fabricante Y, onde ambos respondem pelo mesmo domínio (dominio.gov.br).

2.5. Permitir o cadastro ilimitado de endereços IPs na solução para autorização de envio de mensagens (Allow Relay).

2.6. A solução deverá ser apresentada na forma de Appliance Virtual (conjunto de máquina virtual, sistema operacional e sistema aplicativo) compatível com o virtualizador VMWARE:

2.6.1.1. Deverá suportar plataforma de virtualização VMWARE ESXi versão 6.5 ou superior;

2.6.1.2. A solução deverá ser composta por sistema operacional dedicado e otimizado para esta finalidade (embarcado), customizado e licenciado pelo próprio fabricante, tendo como base os sistemas Unix ou Linux like;

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. Deverá permitir alta disponibilidade, no mínimo, das funções de filtragem de maneira assegurar que não haja interrupção no serviço por falha da solução;

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

2.9. Disponibilizar, durante a vigência do contrato, upgrade para a última versão estável e releases do produto, sem custos adicionais;

2.10. A solução entregue deverá suportar a inclusão e expansão de funcionalidades nativas em soluções desta natureza, sem impactos na interoperabilidade e gestão da solução;

2.10.1. O modelo de implementação após as possíveis inclusões e expansão não poderão gerar impactos no ambiente produtivo, seja ele de desempenho, gestão e segurança da implementação;

2.11. A solução deverá suportar a gestão de perfis de usuários, gravação de logs de administração e processamento de mensagens e envio para Syslog;

## 2.12. Características gerais da solução

- 2.12.1. Suportar no mínimo 10.000 (dez mil) conexões do protocolo Simple Mail Transfer Protocol (SMTP) simultâneas;
- 2.12.2. 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;
- 2.12.3. Prover um mecanismo de proteção multicamadas que permita a análise de conexão, consulta de reputação global, bem como análise de conteúdo e estatística;
- 2.12.4. Inspeccionar as mensagens eletrônicas, no mínimo, por meio dos seguintes métodos:
  - 2.12.4.1. Assinaturas de URL;
  - 2.12.4.2. Filtros de vírus;
  - 2.12.4.3. Filtros de anexos;
  - 2.12.4.4. Filtros de phishing;
  - 2.12.4.5. Endereço IP;
  - 2.12.4.6. Análise de reputação do remetente;
  - 2.12.4.7. Análise heurística;
  - 2.12.4.8. Análise do envelope, cabeçalho, corpo, estrutura, conteúdo não estruturado e formatação, bem como anexo das mensagens;
  - 2.12.4.9. Análise contextual, léxico e baseado em imagem;
  - 2.12.4.10. Suporte a vários idiomas, dentre eles os de dois bytes double byte character set (DBCS);
  - 2.12.4.11. E-mail bounce (retorno de mensagem não enviada pelo usuário);
  - 2.12.4.12. Dicionários pré-definidos e customizados com palavras e expressões regulares.
- 2.12.5. Permitir configurar o “greeting” SMTP e definição de timeout de conexão SMTP;
- 2.12.6. Capaz de limitar o número máximo de conexões simultâneas e por Daemon SMTP;
- 2.12.7. 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;
- 2.12.8. Possibilitar rate limit controlado por endereço de IP, domínio ou reputação do emissor;
- 2.12.9. 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.
- 2.12.10. Deve ser capaz de controlar o número máximo de destinatários de um determinado emissor, por endereço IP, domínio, nome reverso, saudação SMTP ou país;
- 2.12.11. 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;
- 2.12.12. Possibilitar a verificação de DNS reverso para conexões;
- 2.12.13. A solução deve ofertar possibilidade de ter domínio mascarado (Masquerade Domains);
- 2.12.14. Possuir integração com serviço de diretórios padrão protocolo LDAP - Lightweight Directory Access Protocol LDAP (Request For Comments RFC 4511) para obtenção de informações de usuários e validação de destinatário, configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack”), sem a necessidade de modificar os parâmetros “default” do serviço de diretórios;
- 2.12.15. Permitir a utilização de mais de um servidor de LDAP, para autenticação dos usuários, caso ocorra indisponibilidade do servidor primário de LDAP;
- 2.12.16. Deve possuir capacidade de implementar comunicação segura via Transport Layer Security (TLS);
- 2.12.17. Deverá ser capaz de bloquear ataques de negação de serviço (Denial of Service) diretamente na solução;
- 2.12.18. Rejeitar a conexão SMTP que se caracterize como “flooding”;
- 2.12.19. 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;
- 2.12.20. 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>;
- 2.12.21. Possuir controle de e-mail bounce (retorno de mensagem não enviada pelo usuário), passível de configuração pelo administrador;
- 2.12.22. Ter capacidade de bloquear conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, uso de armazenamento e otimização do processamento, em especial baseado em lista local de bloqueio, RBLs e SPF;
- 2.12.23. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);
- 2.12.24. Permitir a instalação automática ou manual de patches de sistema e/ou segurança;
- 2.12.25. Deverá possuir atualização automática das definições de malware, SPAM e outros módulos, em intervalo de tempo configurado pelo administrador;

2.12.26. Possuir mecanismos de backup e restore da configuração existente na solução, com possibilidade de enviar a um servidor remoto por meio da interface gráfica.

## 2.13. Gerenciamento

2.13.1. Deverá possuir console de gerenciamento Multi-tenancy, que permita atender de forma segregada, várias entidades (tenants), cada qual com seus administradores e usuários, permitindo que os próprios tenants administrem seus usuários e políticas e o SERPRO administre todos os seus tenants no nível Master ou super Administrador;

2.13.2. O gerenciamento de políticas de segurança, políticas de antispam, URLs, filtros, domínios, diretórios e rastreamento de mensagens deverá ser realizado por meio de interface gráfica web única e centralizada, de forma segura (HTTPS), sem a necessidade de utilizar linha de comando.

2.13.3. A solução deverá possuir console de gerenciamento por meio de linha de comando segura (SSH), nativo do sistema operacional, para todas as funcionalidades e o SERPRO poderá ter acesso de “super usuário” para correção de problemas e criação de scripts de manutenção;

2.13.4. Suportar o gerenciamento e replicação de políticas do cluster, de forma centralizada, a múltiplos appliances virtuais por meio de uma única interface gráfica web (HTTPS);

2.13.5. A solução deverá permitir a criação de usuários com diferentes níveis de privilégios de gerenciamento, com granularidade de permissões de acesso para cada módulo que compõe a solução;

2.13.6. 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;

2.13.7. A solução deverá permitir a administração granular por Virtual IP e Virtual Host com as seguintes funcionalidades:

2.13.7.1. Possuir a capacidade de criação de endereços IP virtuais para os fluxos de mensagens de entrada e de saída;

2.13.7.2. Permitir que um único appliance possa segmentar o fluxo de e-mail por diferentes IPs Virtuais e Domínios;

2.13.7.3. Permitir múltiplos domínios por endereço IP, ou múltiplos domínios utilizando diferentes IPs no mesmo appliance;

2.13.8. Prover funcionalidade de cópia de segurança e restauração das configurações da solução por meio da interface gráfica web;

2.13.9. Prover funcionalidade de armazenamento e retorno, em caso de falha, das últimas mudanças de configuração, sem interrupção e restauração de backup do serviço;

2.13.10. Permitir importar as contas dos administradores por meio do Microsoft Active Directory (AD) e outros diretórios padrão, protocolo LDAP, com capacidade de sincronização das senhas;

2.13.11. Permitir o rastreamento de mensagens, de forma centralizada e por meio da interface gráfica de gerenciamento web (HTTPS), independente do agente (appliance) que tenha processado;

2.13.12. Deverá permitir o rastreamento por: remetente, destinatário, assunto da mensagem, nome do anexo, nome da ameaça, regra de bloqueio, identificador da mensagem (ID), host ou IP de envio e horário de entrega da mensagem, com a possibilidade de customizações dos períodos de tempo;

2.13.13. O resultado do rastreamento deverá informar no mínimo: o remetente, destinatários da mensagem, o servidor de origem, malware, regra ou política utilizada, tamanho da mensagem e ação executada (entrega, quarentena, bloqueio, falha e/ou rejeitada);

2.13.14. O rastreamento deverá apresentar o registro de log com as evidências referente ao tratamento e ação realizada;

2.13.15. Capacidade de auditar as ações realizadas pelos administradores da solução, independente do perfil;

2.13.16. A solução deverá disponibilizar configuração de alertas por meio da interface gráfica e enviá-los por mensagens de correio eletrônico ou traps SNMP;

2.13.17. Os alertas enviados deverão ser no mínimo os listados abaixo:

2.13.17.1. Componentes da solução não estão respondendo ou funcionando;

2.13.17.2. Espaço em disco;

2.13.17.3. Alertas de hardware;

2.13.17.4. Problemas relacionados a fila de entrada e saída, bem como quantidade de mensagens em fila;

2.13.17.5. Erros de sincronização com os serviços de diretórios;

2.13.17.6. Falhas relacionadas a atualização de patches e base de assinaturas de spam e vírus;

2.13.17.7. Erros na consulta de reputação.

2.13.18. 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);

2.13.19. Deverá prover a capacidade de exportar os logs para produção de relatórios por outros programas;

2.13.20. A solução deverá prover suporte a Syslog;

2.13.20.1. A solução deverá possuir a possibilidade de habilitação de encriptação do tráfego de Syslog;

2.13.21. Deverá possuir sistema de diagnóstico na interface gráfica.

## 2.14. Recursos de proteção e higienização

- 2.14.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de proteção contra ameaças, executando simultaneamente;
- 2.14.2. A análise de SPAM deverá resultar a probabilidade heurística da mensagem, no mínimo:
  - 2.14.2.1. SPAM;
  - 2.14.2.2. E-mail Marketing (Bulk ou Graymail).
- 2.14.3. Possibilitar o bloqueio de maus remetentes e definir políticas individuais por remetente (tanto externo quanto interno) baseado, no mínimo em:
  - 2.14.3.1. IP emissor;
  - 2.14.3.2. Range de IP;
  - 2.14.3.3. Domínio;
  - 2.14.3.4. Reputação do emissor;
  - 2.14.3.5. Verificação DNS.
- 2.14.4. A solução deverá conter proteção específica para ataques do tipo “Phishing”, “Spear Phishing” e Business E-mail Compromise ataques (BEC);
- 2.14.5. 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;
- 2.14.6. 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;
- 2.14.7. 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;
- 2.14.8. Suportar 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;
- 2.14.9. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail);
- 2.14.10. 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;
- 2.14.11. Permitir regras específicas e distintas para bloqueio de surtos de vírus (outbreak);
- 2.14.12. Capacidade de realizar em caso de ameaça no mínimo as seguintes ações simultaneamente:
  - 2.14.12.1. Alterar o assunto da mensagem;
  - 2.14.12.2. Adicionar cabeçalhos e etiquetas para rastreamento;
  - 2.14.12.3. Descartar a mensagem;
  - 2.14.12.4. Mover para área específica de quarentena conforme configurado pelo administrador da solução;
  - 2.14.12.5. Notificar o remetente e/ou destinatário com uma mensagem customizável, informando o nome do vírus.
- 2.14.13. Possibilitar quarentena automática de anexos criptografados;
- 2.14.14. Criar rota customizada para permitir entrada de anexos criptografados para entrega a determinados grupos de e-mails;
- 2.14.15. 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;
- 2.14.16. Possibilitar customizações de regras e políticas por usuários ou grupos;
- 2.14.17. 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;
- 2.14.18. A solução deverá permitir a configuração do intervalo de sincronismo entre a solução antispam e o serviço de diretório;
- 2.14.19. Prover mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente;
- 2.14.20. Prover suporte ao envio e recebimento de mensagens utilizando protocolo TLS e SSL, permitindo configurar domínios onde TLS é mandatório;
- 2.14.21. Prover a assinatura das mensagens de saída com chave DKIM;
- 2.14.22. Fazer a análise de cabeçalho (header) nos padrões RFC 822;
- 2.14.23. Permitir a aplicação de regras baseadas no idioma que as mensagens foram escritas, com capacidade para, no mínimo, identificar Português, Inglês e Espanhol;
- 2.14.24. Permitir a aplicação de regras baseadas no país de origem do e-mail;
- 2.14.25. 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;
- 2.14.26. Controlar conexões nos seguintes níveis, mediante configuração:

- 2.14.26.1. Número de mensagens por conexão;
- 2.14.26.2. Número de conexões simultâneas;
- 2.14.26.3. Número de destinatários por mensagem;
- 2.14.26.4. Tamanho das mensagens;
- 2.14.26.5. Tempo de processamento da mensagem;
- 2.14.26.6. Controlar mensagens com anexos com base em:
  - 2.14.26.6.1. Mime Type (Tipo de extensões “Multi função” para mensagens de Internet);
  - 2.14.26.6.2. Tipo real do arquivo;
  - 2.14.26.6.3. Nome do arquivo;
  - 2.14.26.6.4. Tamanho de anexo;
  - 2.14.26.6.5. Quantidade de anexos;
  - 2.14.26.6.6. Anexos compactados com senha;
  - 2.14.26.6.7. Quantidade de camadas de arquivos compactados, um dentro do outro;
  - 2.14.26.6.8. Todas as configurações deverão ser granulares para domínios, grupos e usuários específicos;
  - 2.14.26.6.9. Tomar, no mínimo, as seguintes ações:
    - 2.14.26.6.9.1. Remover o anexo;
    - 2.14.26.6.9.2. Alterar o assunto da mensagem;
    - 2.14.26.6.9.3. Adicionar cabeçalhos para rastreamento;
    - 2.14.26.6.9.4. Descartar a mensagem;
    - 2.14.26.6.9.5. Colocar em uma determinada área da quarentena definida pelo administrador;
    - 2.14.26.6.9.6. Notificar o remetente e/ou destinatário com uma mensagem customizável;
    - 2.14.26.6.9.7. A solução deverá prover a funcionalidade de incluir avisos (disclaimers) no início ou no rodapé das mensagens enviadas;
    - 2.14.26.6.9.8. A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes por meio da integração com o serviço de diretório padrão protocolo LDAP;
    - 2.14.26.6.9.9. A solução deverá suportar a configuração dos “disclaimers” em formato html ou texto;
- 2.14.27. Possuir funcionalidade de bloqueio de servidores Spammers por meio dos recursos de Domain Keys Identified Mail (DKIM) e Sender Policy Framework (SPF);
- 2.14.28. Implementar o padrão Domain-based Message Authentication, Reporting and Conformance (DMARC);
- 2.14.29. Rejeitar mensagens para destinatários inválidos durante o diálogo SMTP, para prevenir NonDelivery Report Attack;
- 2.14.30. Suportar o gerenciamento de bounces permitindo a criação de regras específicas, bem como a possibilidade do uso de chaves criptográficas para assinar as mensagens de saída;
- 2.14.31. 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.

## 2.15. Quarentena

- 2.15.1. Possuir áreas de quarentena no próprio appliance de acordo com as políticas de proteção, contendo no mínimo as seguintes áreas já criadas por padrão: Spam, Bulk, Graymail, Phishing e Vírus;
- 2.15.2. Suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos;
- 2.15.3. Deverá permitir configurar o tempo de armazenamento da quarentena;
- 2.15.4. Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, na qual o sistema automaticamente executará as ações configuradas (delete, delivery, delay delivery);
- 2.15.5. Possibilitar a visualização do resumo de todas as áreas da quarentena, informando o tamanho de cada área, volume de mensagens e tempo de expiração;
- 2.15.6. Permitir ao administrador da solução executar pesquisa nas mensagens em quarentena de todos os usuários por meio de interface web segura (HTTPS), acessando a própria solução, sem necessidade de nenhum software ou hardware adicional;
- 2.15.7. Possibilitar o gerenciamento da quarentena pelo administrador, com a identificação do motivo do bloqueio, origem e destino da mensagem, data, hora, assunto, IP do host de envio, mensagem, tamanho, podendo executar as ações: liberar, excluir, mover ou processar novamente as mensagens;
- 2.15.8. Para garantir o sigilo da informação, permitir que determinadas áreas de quarentena somente sejam acessíveis a determinados administradores, permitindo a granularidade da permissão de acesso destas áreas.
  - 2.15.8.1. Ainda sobre o sigilo, privacidade e funcionamento da solução, a mesma deve seguir e respeitar a LGPD (Lei Geral de Proteção de Dados) em todos os seus aspectos.

## 2.16. Relatórios e estatísticas

- 2.16.1. Capacidade de gerar diversos relatórios na console web centralizada da solução;
- 2.16.2. Permitir gerar e enviar por e-mail relatórios automatizados, por meio de agendamento;
- 2.16.3. Permitir seleção de dados para geração de relatórios por data específica ou intervalo de tempo, com granularidade de hora;
- 2.16.4. Possibilidade de configurar o período de retenção de dados para produção de relatórios;
- 2.16.5. Os relatórios deverão ser disponibilizados em formato de gráfico, bem como em tabelas com dados dispostos em linhas e colunas;
- 2.16.6. Disponibilizar, pelo menos, os seguintes tipos de relatórios:
  - 2.16.6.1. Relatórios sobre volume e tipo de spam recebido;
  - 2.16.6.2. Maiores domínios que enviam spam;
  - 2.16.6.3. Maiores remetentes de vírus;
  - 2.16.6.4. Maiores remetentes de spam por conexão IP;
  - 2.16.6.5. Endereços de e-mails que mais recebem spam;
  - 2.16.6.6. Volume de conexões por agentes de roteamento de mensagens;
  - 2.16.6.7. Relatório de throughput de mensagens;
  - 2.16.6.8. Rejeitadas por reputação e controle de conexão;
  - 2.16.6.9. Número total de mensagens em quarentena;
  - 2.16.6.10. Usuários que mais liberam mensagens.
- 2.16.7. Sumário com o total de mensagens que foram classificadas:
  - 2.16.7.1. Spam;
  - 2.16.7.2. Vírus
  - 2.16.7.3. Bloqueadas por políticas;
  - 2.16.7.4. Mensagens válidas.
- 2.16.8. 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:
  - 2.16.8.1. Informações sobre recursos do appliance;
  - 2.16.8.2. Informações sobre a “saúde” dos agentes, serviços e módulos que compõem a solução;
  - 2.16.8.3. Informações sobre mensagens, conexões, bem como bloqueio de spam e vírus.

## 2.17. Gerenciamento da quarentena pessoal

- 2.17.1. A solução deverá prover o serviço capaz de enviar para os usuários dos domínios, organizações, sub-organizações e grupos, um resumo de mensagens categorizadas como SPAM (Digest) e permitir o gerenciamento da quarentena pessoal, através da mensagem de e-mail;
- 2.17.2. O envio do Digest deverá ocorrer em dias e horários estabelecidos e configurados pelo administrador;
- 2.17.3. O Digest deverá ser enviado em Língua Portuguesa do Brasil e seu conteúdo ter a possibilidade de customização;
- 2.17.4. Suporte para no mínimo as seguintes linguagens: Português do Brasil, Inglês e Espanhol;
- 2.17.5. Suporte a Digest responsivo;
- 2.17.6. O Digest deverá permitir ao usuário liberar a mensagem bloqueada;
- 2.17.7. A interface do usuário final deverá estar no idioma “Português do Brasil”;
- 2.17.8. 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;
- 2.17.9. 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;
- 2.17.10. O usuário final poderá incluir e remover endereços em sua lista pessoal de bloqueio (“Lista negra”) ou de liberação de e-mails (“Lista branca”);
- 2.17.11. O usuário final poderá visualizar as mensagens bloqueadas e liberá-las, a seu critério.

## 2.18. Sistema de Segurança contra Ataques Dirigidos

- 2.18.1. O fabricante da solução deverá possuir um centro de pesquisa e desenvolvimento em segurança, dedicado à identificação de vulnerabilidades, manutenção de inteligência em segurança de e-mails, descoberta de explorações e ameaças, bem como a criação de mecanismos de contenção e resposta a ataques, com abrangência global;
- 2.18.2. O sistema de proteção contra ataques dirigidos deverá implementar:
  - 2.18.2.1. Análise de e-mail em tempo real incluindo as propriedades da mensagem;
  - 2.18.2.2. Assegurar que links de URLs suspeitas sejam dinamicamente reescritas antes do e-mail ser entregue ao destinatário e que cada vez que um usuário clicar em qualquer link, na rede corporativa ou externa, deverá ser exibida uma notificação de bloqueio. Caso a URL não seja maliciosa a solução deverá redirecionar para a URL original;

- 2.18.2.3. A inspeção de URLs deverá utilizar várias fontes de informação para verificação de ameaças, inclusive o centro de inteligência utilizado pelo fabricante;
- 2.18.2.4. Realizar análises de anomalias e de malware e aplicar controles adicionais às mensagens suspeitas.
- 2.18.3. Suportar análise dinâmica ou sandboxing, em ambiente segregado da rede cliente, entregando um resumo e relatório completo da análise realizada;
- 2.18.4. Caso o processo de análise dinâmica seja realizado em infraestrutura em nuvem do fabricante, este deverá garantir a privacidade das informações;
- 2.18.5. Suportar análise dinâmica ou sandboxing resistente a técnicas de evasão e, quando observadas tais tentativas, reportar a ocorrência nas amostras avaliadas;
- 2.18.6. Suportar a detecção de todos os tipos de malwares, ambos conhecidos e desconhecidos. Capacidade de rastrear a disseminação e trilha de todos os malwares e reportar de forma detalhada;
- 2.17.6.1. Permitir a importação/exportação de hash codes integrado à administração da ferramenta.
- 2.18.7. A solução deverá oferecer serviços de reputação de conteúdo web e identificação de ameaças Zero Day com recurso centralizado de inteligência em nuvem (cloud);
- 2.18.8. Deverá possuir filtro de reputação com as funcionalidades:
  - 2.18.8.1. O sistema de reputação deverá checar a reputação dos remetentes em redes participantes com abrangência global;
  - 2.18.9. Os filtros de reputação baseados em URL, deverão permitir:
    - 2.18.9.1. 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;
  - 2.18.10. 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 contrário à política de acesso;
  - 2.18.11. Possibilitar o controle de tráfego de e-mail por reputação atribuída pela rede de reputação, de cada IP que solicitou uma conexão;
  - 2.18.12. As informações da rede de reputação deverão ser utilizadas durante a análise das mensagens pelo filtro de antispam;
  - 2.18.13. A solução deverá mover para 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;
  - 2.18.14. 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;
  - 2.18.15. A solução deverá ser capaz de rastrear a disseminação e trilha do malware, conhecidos ou não, com relatórios detalhados com suporte a pesquisa e análise contínua para auxiliar análise de incidentes;
  - 2.18.16. Deverá ser possível habilitar ou desabilitar a proteção URL baseada em rotas específicas configuradas no mínimo pelas seguintes condições: Sender, Recipient, Domínios, Sender IP Address, ou usuários via LDAP;
  - 2.18.17. A proteção de URL deverá identificar se a URL é maliciosa e redirecionar o usuário para uma página com uma notificação de bloqueio ;
  - 2.18.18. A proteção de URL deverá ser capaz de analisar a categoria do conteúdo e redirecionar o usuário para uma tela de notificação. Essa funcionalidade deverá ser implementada inclusive quando a URL não puder ser classificada e a solução deverá classificar a cada clique;
  - 2.18.19. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site será bloqueado no navegador;
  - 2.18.20. Cada mensagem deverá consultar o serviço na nuvem para testes em sandbox que definirá uma pontuação (score) para a mensagem;
  - 2.18.21. 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;
  - 2.18.22. A proteção de URL deverá reescrever links para os protocolos HTTP, HTTPS e FTP, URL's que comecem com "www" independente do protocolo;
  - 2.18.23. A solução deverá permitir que o administrador gerencie quais URL's serão reescritas e como serão exibidas nas mensagens de e-mail;
  - 2.18.24. 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;
  - 2.18.25. Permitir lista de exceções de URL para que não sejam reescritas;
  - 2.18.26. 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;
  - 2.18.27. Suportar reescrever URLs com base no módulo de detecção de anomalias nas mensagens que contenham link;

- 2.18.28. O relatório deverá fornecer visibilidade sobre ataques identificados com base em URL e ameaças de malware.
- 2.18.29. 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 da tentativa de acesso pelo usuário;
- 2.18.30. O Dashboard deverá exibir a linha do tempo (timeline) das ameaças, exibindo o período que foi recebida, identificada e quando foi clicada ou liberada;
- 2.18.31. Deverá ser possível rastrear a partir de uma URL ou malware presentes em mensagens com informações detalhadas;
- 2.18.32. Capacidade de disponibilizar sistema de coleta de amostra para o centro mundial de inteligência utilizado pelo fabricante para análises;
- 2.18.33. 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

## 2.19. Funcionalidades compatíveis com a solução

- 2.19.1. Suportar a implantação de módulo de compliance que permita aplicar tratamentos para mensagens que violem as regras de compliance definidas, com as ações de bloqueio, quarentena e auditoria;
- 2.19.2. 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 de regras de compliances;
- 2.19.3. Suportar a implantação de módulo de compliance que possibilite alteração de cabeçalho da mensagem, quando violada alguma regra de compliance;
- 2.19.4. Suportar a implantação de módulo 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;
- 2.19.5. Suportar a implantação de módulo de criptografia com logs de auditoria de todas as transações envolvendo mensagens criptografadas;
- 2.19.6. Possibilitar ao administrador definir qual mensagem deverá ser criptografada, com base, no mínimo, em assunto, destinatário, remetente e anexo;
- 2.19.7. Possibilitar ao administrador integrar o DLP com a criptografia, de modo a que os e-mails sigilosos somente sejam enviados criptografados;
- 2.19.8. Permitir a utilização de criptografia das mensagens, geradas por chaves independentes;
- 2.19.9. Impossibilitar o uso de cache de browser para acesso as mensagens criptografadas;
- 2.19.10. O sistema deverá permitir que o modelo das mensagens criptografadas possam ser customizadas;
- 2.19.11. Ser capaz de criptografar mensagens localmente por meio de criação de regras que especifiquem quais mensagens deverão 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, etc), assunto ou corpo do e-mail, caracteres no header da mensagem;
- 2.19.12. Possibilidade de criar perfis diferentes para cada regra específica de mensagens a serem criptografadas;
- 2.19.13. O método de criptografia utilizado não deverá depender da instalação de softwares ou plugins na máquina do remetente ou do destinatário;
- 2.19.14. Permitir gerar chaves por mensagem impossibilitando que a chave de uma mensagem possa abrir outra mensagem, mesmo que para o mesmo destinatário;
- 2.19.15. Possibilitar que a mensagem seja entregue em um anexo criptografado e somente a chave pública deverá ser transmitida entre o servidor e o destinatário em um acesso seguro do tipo Secure Socket Layer (SSL);
- 2.19.16. Suportar 2 (dois) níveis de segurança de acesso na leitura das mensagens criptografadas:
  - 2.19.16.1. 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;
  - 2.19.16.2. 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.
- 2.19.17. Suportar no mínimo os seguintes algoritmos de criptografias:
  - 2.19.17.1. AES 192 bits;
  - 2.19.17.2. RC4 160 bits.
  - 2.19.17.3. Suportar o padrão Federal Information Processing Standards (FIPS);
  - 2.19.17.4. Permitir que os receptores das mensagens criptografadas possam responder e/ou encaminhar à mensagem de forma criptografada, para garantir a segurança da informação;
  - 2.19.17.5. As regras de mensagens a serem criptografadas deverão estar de acordo com as normas de conformidade, tais como:



- 2.19.17.5.1. Health Insurance Portability and Accountability Act (HIPAA);
- 2.19.17.5.2. Sarbanes Oxley (SOX);
- 2.19.17.5.3. Gramm-Leach-Bliley Act (GLB);
- 2.19.17.5.4. Personal Information Protection and Electronic Documents Act (PIPEDA);
- 2.19.18. O sistema deverá suportar os seguintes controles das mensagens enviadas:
- 2.19.18.1. O remetente poderá cancelar a chave da mensagem antes mesmo que o destinatário receba a mensagem;
- 2.19.18.2. O remetente poderá configurar um tempo de expiração da chave e, caso o tempo tenha expirado, a mensagem não poderá ser aberta;
- 2.19.18.3. O sistema poderá enviar notificação de leitura da mensagem, assim que o destinatário acessar a chave para abertura da mensagem;
- 2.19.18.4. Os servidores ou appliances de chaves ou de criptografia não devem armazenar as mensagens;
- 2.19.18.5. Possuir console única de gerenciamento para interface de criptografia, compliance, antispam e antivírus, ou seja, para todos os módulos exigidos e suportáveis da solução.

### 3.0 Níveis de serviço e sancionamentos

3.1. Para as licenças instaladas:

3.1.1. Para as licenças contratadas e instaladas, serão prestados serviços de manutenção atualização e suporte técnico:

3.1.1.1. Possuir atendimento para as licenças instaladas, durante o período de vigência do contrato, assegurando prazos de atendimento compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, inclusive finais de semana e feriados, à exceção dos chamados de Severidade 4, que serão atendidos em horário comercial, ou seja, das 08:00 h. às 18:00h., de segunda-feira a sexta-feira, horário local, exceto feriados.

3.1.1.2. O atendimento aos chamados deve obedecer à seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução / Contorno	Observações	Penalidades
1 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado	Remoto / On-site	No máximo 1 (uma) hora após a abertura do chamado	No máximo 12 (Doze) horas após o início do atendimento	<p>A CONTRATADA deverá garantir o atendimento do prazo de solução do chamado no seguinte formato:</p> <p>- Atendimento Remoto: Duração de até 6 (seis) horas a contar do início do atendimento;</p> <p>- Atendimento On-site: Início a qualquer momento do período estipulado para atendimento remoto ou em até 2 (duas)</p>	<p>O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,5% (meio por cento) do valor anual do contrato, por hora ou fração de hora de atraso.</p>

					horas após o término do prazo do atendimento remoto.	
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 o início do atendimento	<p>A CONTRATADA deverá garantir o atendimento do prazo de solução do chamado no seguinte formato:</p> <p>- Atendimento Remoto: Duração de até 12 (doze) horas a contar do início do atendimento;</p> <p>- Atendimento On-site: Início a qualquer momento do período estipulado para atendimento remoto ou em até 2 (duas) horas após o término do prazo do atendimento remoto.</p>	<p>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 contrato, por hora ou fração de hora de atraso.</p>
3 - Média	Chamados referentes a situações de baixo impacto, ou para aqueles problemas que se apresentem de forma intermitente	Remoto / On-site	No máximo 4 (quatro) horas após a abertura do chamado	No máximo 72 (Setenta e duas) horas após o início do atendimento	<p>A CONTRATADA deverá garantir o atendimento do prazo de solução do chamado no seguinte formato:</p> <p>- Atendimento Remoto: Duração de até 48 (quarenta e oito) horas a contar do</p>	<p>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 contrato, por hora ou fração</p>

					início do atendimento;  - Atendimento On-site: Início a qualquer momento do período estipulado para atendimento remoto ou em até 2 (duas) horas após o término do prazo do atendimento remoto.	de hora de atraso.
	Chamados com objetivo de atualização de software(s) e firmware(s)	Remoto /On-site	No máximo 4 (quatro) horas após a abertura do chamado	Conforme agendamento	O atendimento deverá ser realizado conforme o agendamento, mesmo que contemple períodos noturnos e dias não úteis.	
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	—	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à CONTRATADA de 0,1% (um décimo por cento) do valor anual do contrato, por hora ou fração de hora de atraso.

3.1.1.3. O atendimento on-site para os chamados de severidade 1, 2 e 3 deverão ser efetuados por um especialista devidamente habilitado, que trabalhará o tempo que for necessário para a solução do problema, sem ônus para o SERPRO e sem prejuízo para os demais prazos.

3.1.1.3.1. O atendimento não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda em períodos noturnos e dias não úteis.

3.1.1.4. Em quaisquer casos e quando necessário, a CONTRATADA deve assistir remotamente na instalação e uso dos software(s) ofertado(s), 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.

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

3.1.1.6. Sistema paralisado é a situação em que há impossibilidade total de uso de um serviço prestado pelo SERPRO em razão de defeito em um ou mais produtos da CONTRATADA.

3.1.1.7. Chamados, Registros e Início de Prazos

3.1.1.7.1. Será aberto um chamado para cada problema reportado.

3.1.1.7.2. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

3.1.1.8. Monitoramento do Atendimento dos Chamados

3.1.1.8.1. Todos os chamados serão controlados por sistema de informação da CONTRATADA.

3.1.1.8.2. O fechamento do chamado poderá se dar quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

3.1.1.8.3. A disponibilização de medida definitiva poderá a critério da CONTRATADA vir a ser incorporada em futuras versões dos módulos.

3.1.1.8.4. Antes do fechamento de cada chamado, a CONTRATADA consultará o SERPRO para validar o fechamento do mesmo.

3.1.1.9. 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.

3.1.1.10. A CONTRATADA manterá cadastro das pessoas indicadas pelo SERPRO que poderão efetuar abertura e autorizar fechamento de chamados.

3.1.1.11. Canais de atendimento:

3.1.1.11.1. O atendimento e os chamados técnicos deverão ser realizados por meio de canal telefônico gratuito 0800 e/ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e/ou site na Internet;

3.1.1.12. Entrega mensal de relatórios

3.1.1.12.1. Deverá ser entregue um relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período, 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 deve ser entregue mesmo quando não houver chamados no período.

3.1.1.12.2. A entrega dos relatórios mensais será condição necessária para o SERPRO realizar o ateste da nota fiscal e/ou fatura, para fins de pagamento dos serviços executados.

#### **4.0 Especificação de valores e forma de pagamento**

4.1. Os pagamentos dos serviços de Manutenção, atualização e suporte técnico para as licenças da Solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound), serão efetuados mensalmente, no 1º (primeiro) dia útil, após o 20º (vigésimo) dia corrido da data do recebimento definitivo dos serviços a serem prestados nos locais indicados nas respectivas notas fiscais e/ou faturas entregues no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato.

4.1.1. O prazo para recebimento definitivo, por parte do SERPRO, é de 5 (cinco) dias úteis contados a partir do recebimento da nota fiscal e/ou fatura e da apresentação de relatório mensal de serviços, pela CONTRATADA.

4.2. O pagamento dos serviços de Operação Assistida, Consultoria e Suporte Técnico On-Site (que ainda serão quantificados) demandados por meio de Ordem de Serviço (OS) serão efetuados em parcela única, no primeiro dia útil após o 20º (vigésimo) dia corrido da data do recebimento definitivo, referentes à(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, condicionados à emissão de Relatório de Conclusão da OS, pelo SERPRO.

4.2.1. O prazo para recebimento definitivo, por parte do SERPRO, é de 5 (cinco) dias úteis contados a partir do recebimento da nota fiscal e/ou fatura e da emissão de Relatório de Conclusão da OS, pelo SERPRO.

#### **5.0 Justificativa da contratação**

5.1. Esta Consulta Pública está autorizada pelo SISCOR SUPES 029357/2019-61 (cópia em anexo).

5.2. Esta Consulta Pública servirá de base para ratificação e/ou retificação das especificações técnicas, elaborada pela SUPCD e SUPES, e atendimento das necessidades empresariais e evoluções.

## 6.0 Seleção do fornecedor

6.1. Modalidade da Contratação.

6.1.1. A Fundamentação Legal para esta contratação encontra fulcro no Art. 32, inciso IV, da Lei 13.303 c/c Lei nº 10.520/2002, na modalidade Pregão Eletrônico.

6.1.2. Será considerada ganhadora do processo licitatório a LICITANTE que apresentar a proposta com o menor preço global.

6.1.3. Apresentar atestado ou declaração do fabricante comprovando vínculo técnico com a LICITANTE.

6.1.4. Apresentar atestado de capacidade técnica para todos os itens.

6.1.5. Apresentar modelo de implementação (Será questionado na consulta pública como o fabricante/integrador garante a privacidade das informações, bem como a topologia e o processo de verificação);

6.2. Matriz de Risco:

TIPO DE RISCO	DESCRIÇÃO	RESPONSABILIDADE		AÇÕES MITIGAÇÃO / CONTINGÊNCIA
		SERPRO	FORNECEDOR	
EXECUÇÃO CONTRATUAL	Atraso na execução do objeto contratual por culpa do Contratado.		X	Diligência do Contratado na execução contratual. / Acompanhamento e gestão do processo e do contrato.
EXECUÇÃO CONTRATUAL	Fatos retardadores ou impeditivos da execução do Contrato próprios do risco ordinário da atividade empresarial ou da execução.		X	Planejamento empresarial. / Acompanhamento e gestão do processo e do contrato.
FINANCEIRO	Fatos retardadores ou impeditivos da execução do Contrato que não estejam na sua área ordinária, tais como fatos do princípio, caso fortuito ou de força maior, bem como o retardamento determinado pelo SERPRO, que comprovadamente repercute no preço do Contratado.	X		Revisão de preço. / Negociação com o contratado.
EMPRESARIAL	Alteração de enquadramento tributário, em razão do resultado ou de		X	Planejamento tributário. / N/A

	mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária.		
EMPRESARIAL	Variação da taxa de câmbio.	X	Instrumentos financeiros de proteção cambial (hedge). / N/A
EMPRESARIAL	Elevação de gastos com viagens superiores ao estimado pelo Contratado.	X	Melhor planejamento contratual. / N/A
EMPRESARIAL	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra.	X	Reajuste anual de preço. / N/A
EMPRESARIAL	Elevação dos custos operacionais definidos na linha anterior, quando superior ao índice de reajuste previsto na Cláusula de Equilíbrio Econômico-Financeiro do Contrato (para os serviços de manutenção e suporte técnico).	X	Planejamento empresarial. / N/A
EMPRESARIAL	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a	X	Planejamento empresarial. / N/A

	execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra (para as demais parcelas não mencionadas na linha anterior).		
TRABALHISTA	Responsabilização do SERPRO por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na execução do objeto contratual.	X	Ressarcimento, pelo Contratado, ou retenção de pagamento e compensação com valores a este devidos, da quantia despendida pelo SERPRO. / N/A
TRIBUTÁRIO	Responsabilização do SERPRO por Recolhimento indevido em valor menor ou Maior que o necessário, ou ainda de Ausência de recolhimento, quando Devido, sem que haja culpa do SERPRO.	X	Ressarcimento, pelo Contratado, ou retenção de pagamento e compensação com valores a este devidos, da quantia despendida pelo SERPRO. / N/A

## 7.0 Justificativa para aceitação de preços

Não se aplica.

## 8.0 Gerenciamento contratual

8.1. A vigência do contrato será de 36 (trinta e seis) meses, podendo ser prorrogado por até 60 (sessenta) meses.

8.2. O SERPRO não assinará qualquer contrato adicional com o fabricante, decorrentes deste processo, ficando a CONTRATADA obrigada a efetuar os seus pedidos cientes desta condição.

8.3. Obrigações da Contratada

8.3.1 Repasse de Conhecimento

8.3.1.1 O repasse de conhecimento deverá ser realizado durante a vigência do contrato, e deverá conter carga horária mínima de 40 (quarenta) horas.

8.3.1.2. A CONTRATADA deverá prover toda a logística e todo o material didático necessário à execução do repasse de conhecimento teórico e prático, ou seja, instalações adequadas, equipamentos, manuais e apostilas.

8.3.1.3 A data de início, será definida pelo SERPRO de acordo com suas necessidades. O SERPRO deverá comunicar formalmente à CONTRATADA com uma antecedência mínima de 10 (dez) dias.

8.3.2. O repasse deverá ser realizado na localidade da prestação dos serviços.

8.3.2.1. Deverá ser realizado com uma turma contendo até 10 (dez) pessoas.

8.3.2.2. Caso haja necessidade de repasse de conhecimento para outras regionais do SERPRO, além da modalidade presencial, a CONTRATADA poderá utilizar a ferramenta Webex.

8.3.3. Deverá ser realizada em dependências providenciadas pela CONTRATADA. Havendo disponibilidade de

infraestrutura, a capacitação poderá ser realizada nas dependências do SERPRO.

8.3.4. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, compatíveis com as mesmas funcionalidades solicitadas nas especificações técnicas.

8.3.5. O repasse deverá ser ministrado por profissional(ais) certificado(s) e/ou autorizado(s) pelo fabricante do(s) equipamento(s), com a devida comprovação.

8.3.6. A CONTRATADA deverá apresentar em até 5 (cinco) dias após o início da vigência do contrato, o(s) certificado(s) solicitado(s) bem como declaração de que a empresa está autorizada pelo fabricante a prestar o repasse.

8.3.7. Deverá ser entregue ao SERPRO, em até 10 (dez) dias após a definição da data do repasse de conhecimento a ser informada pelo SERPRO, a ementa contendo: nome, objetivo, pré-requisitos, conteúdo programático, bem como o material do repasse.

8.3.8. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade da CONTRATADA.

8.3.9. Ao final do repasse de conhecimento, o SERPRO, por meio do formulário “Avaliação de Reação Resultado”, fará a avaliação do repasse ministrado para emissão de termo de aceite, a qual a Contrata deverá obter a média de 70% (setenta por cento) de conceitos “bom e/ou ótimo”.

8.3.9.1. Caso não atinja o conceito mencionado, o SERPRO encaminhará um relatório à CONTRATADA informando o que deverá ser adequado para a realização de um novo repasse.

8.3.9.2. O SERPRO encaminhará as alterações que forem identificadas, para realização de novo repasse e encaminhará à CONTRATADA, que providenciará este novo repasse.

8.3.9.3. Se aprovado, o prazo do novo repasse de conhecimento deverá ser acordado com a equipe do SERPRO.

8.3.10. Após o repasse de conhecimento a CONTRATADA deverá emitir certificado para cada participante, obedecendo ao critério de frequência de 80%. O certificado deverá conter as seguintes informações: Nome completo do participante, Nome responsável do repasse de conhecimento, Período de Realização, Carga Horária e Conteúdo Programático.

8.3.10.1. O(s) Certificado(s) deverá(ão) ser(ão) encaminhado(s) ao responsável da Universidade Corporativa do SERPRO na localidade onde ocorreu o repasse de conhecimento.

## **9.0 Considerações gerais**

Não se aplica.

## **Elaboração**

Data : 29/10/2019

THIAGO VINICIUS VIEIRA DE OLIVEIRA - 21094101

SUPES/ESTAR/ESTAA

## **Anexos**

Arquivo: [SISCOR Solicitação de Autorização Consulta Pública](#)

Arquivo: [SISCOR Resposta Solicitação de Autorização Consulta Pública](#)