MINISTÉRIO DA SAÚDE
FUNDAÇÃO NACIONAL DE SAÚDE
COORDENAÇÃO DE INOVAÇÃO E INFRAESTRUTURA TECNOLÓGICA
Setor de Autarquias Sul (SAUS) – Quadra 4 – Bloco N
Brasília - CEP 70070-040
(61) 3314-6619

# ANEXO I - ESPECIFICAÇÕES TÉCNICAS

1. Este Anexo especifica as características técnicas de licenças de software de solução de gateway de segurança de e-mails, com fornecimento de serviço de instalação e configuração, suporte, manutenção especializada e garantia por 60 meses.

## 2. Solução de Gateway e Segurança de E-mails

### 2.1. Características Gerais

2.1.1. A solução poderá ser capaz ser implementada em:

2.1.2. Ambientes virtuais, no modelo virtual appliance, suportando no mínimo Plataforma VmWare ESX; ou

2.1.3. Ambiente em cloud, provido pelo fabricante da solução, com no mínimo:

2.1.3.1. SLA de disponibilidade de 99.999%;

2.1.3.2. Suporte e monitoramento 24x7.

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

2.1.5. Ocorrência de Falsos-positivos inferior a 0,0004%;

2.1.6. Latência máxima na entrega de mensagens inferior a um minuto;

2.1.7. Sistema operacional da solução deve ser fechado - pre-hardened, com limitação deacesso elevados;

2.1.8. Deve possuir capacidade de configuração em Alta Disponibilidade, caso seja ofertado em modelo on premises;

2.1.9. Se solução for em modo virtual, ela deve ser capaz de ser adicionado appliances adicionais, a fim de obter melhoras de processamento, sem a necessidade de incremento de licenças adicionais;

2.1.10. Deve possuir console de administração via GUI (Graphical User Interface) e CLI(Command Line Interface), este se provido em modelo virtual appliance;

2.1.11. O acesso ao GUI (Graphical User Interface) deve ocorrer através de HTTPS;

2.1.12. A solução deverá possuir console centralizada, incluindo:

2.1.12.1. Configurações de administração;

2.1.12.2. Objetos de política;

2.1.12.3. Objetos suspeitos;

2.1.12.4. Gerenciamento de usuário final;

2.1.12.5. Gerenciamento de diretório;

2.1.12.6. Informações sobre licenciamento;

2.1.12.7. Logs;

2.1.12.8. Relatórios;

2.1.12.9. Visualização de mensagens quarentenadas;

2.1.12.10. Gerenciamento de domínio;

2.1.12.11. Dashboard baseado em gráficos;

2.1.12.12. Rastreamento de E-mails, eventos e Logs.

2.1.13. A solução deverá possuir dashboards possibilitando no mínimo a visualização de ameaças, ransomwares, detalhes de autenticação baseada em domínio, sandbox, BEC, SPAM, principais violações, eventos de DLP, consumo de banda;

2.1.14. Deve ser capaz de prover acessos administrativos granulares à console de administração;

2.1.15. A solução deverá possuir integração com o Active Directory;

2.1.16. Deve suportar Active Directory Federation Services;

2.1.17. Deve realizar integração com soluções externas como OKTA;

2.1.18. A solução deve realizar a integração com SIEM (Security Information and Event Management)através de APIs ou outra tecnologia;

2.1.19. A solução deverá permitir o gerenciamento de múltiplos domínios;

2.1.20. Deve prover a console para que o usuário final visualize as mensagens quarentenadas;

2.1.21. Deve possuir caixa de correio para o usuário interagir;

2.1.22. A console do usuário final deve permitir as seguintes ações:

2.1.23. Deletar mensagem;

2.1.24. Aprovar a entrega da mensagem;

2.1.25. Na console do usuário final deve ser possível visualizar o motivo pelo qual a mensagem foi quarentenada;

2.1.26. A console do usuário final deverá suportar linguagens Português do Brasil e Inglês;

2.1.27. A console do usuário final deve ser acessível via browser, no mínimo:

2.1.27.1. Microsoft Internet Explorer

2.1.27.2. Microsoft Edge 91

2.1.27.3. Mozilla Firefox

2.1.27.4. Google Chrome

2.1.28. Para ambiente em cloud, a solução deve ser provida com: certificação ISO 27000;

2.1.29. Deve possuir regras de permissionamento a acesso a console administrativa distintas podendo ser configuradas conforme a necessidade;

2.1.30. A solução deve ser capaz de configurar políticas distintas de filtragem para entrada e saída de e-mails;

2.1.31. A solução deve possibilitar a configuração de filtragens de entrada e saída de e-mail. Esta configuração deve ocorrer através da mesma console de administração;

2.1.32. A solução deverá suportar: TLS 1.3, TLS 1.2, TLS 1.1;

2.1.33. A solução deverá permitir a configuração da checagem do TLS;

2.1.34. A solução deverá assegurar a comunicação através da utilização do protocolo TLS;

2.1.35. A solução deverá ser capaz de criptografar e-mails baseado em políticas.

2.2. **Criptografia de E-mail**

2.2.1. Deve ser possível realizar a integração da SandBox com o tenant O365 ou G-suíte para visualização de possíveis contas comprometidas ou que estão sendo atacadas em tempo real. Esta integração deve ser via API;

2.2.2. A solução deverá possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas;

2.2.3. A solução deve possuir a capacidade de tentativa de extração de senha em arquivos protegidos através de técnicas de heurística;

2.2.4. A solução deve possuir mecanismo de envio de arquivos e URLs suspeitas para uma Sandbox, com o objetivo de identificar características potencialmente maliciosas;

2.2.5. A solução deverá realizar varreduras em arquivos JSE e VBE para indentificar ameaças de macro;

2.2.6. A solução deverá manter mensagens recebidas por até 10 dias, permitindo o uso ininterrupto do sistema de email, mesmo quando haja uma falha no serviço;

2.2.7. Deve ser possível criar diferentes políticas de proteção para diferentes rotas de email comoinbound e outbound;

2.2.8. Conforme a categorização do malware, deve ser possível tomar diferentes ações;

2.2.9. Deve proteger o fluxo de mensagens inbound e outbound;

2.2.10. Deve possuir no mínimo, 1 (uma) engine de Anti-Malware;

2.2.11. A solução deverá possuir engine própria para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados;

2.2.12. Deve proteger e-mails com arquivos protegidos;

2.2.13. Deve ser possível realizar a limpeza de malwares ou códigos maliciosos, onde o malware pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original;

2.2.14. Deve ser possível criar políticas que executem ações em mensagens que contêm malware, worms ou outros códigos maliciosos;

2.2.15. A solução deverá detectar malwares, worms, e outras ameaças baseadas em assinatura e padrões.

2.3. **Módulo de Anti-Malware**

2.3.1. Deve ser possível configurar chaves DKIM para todos os domínios outbound de email;

2.3.2. Deve possuir suporte a DKIM para assinaturas de e-mails outbound;

2.3.3. Deve possuir regras DKIM pré-definas para bloqueio de mensagens com, no mínimo, nos seguintes status: "TempError";

2.3.4. Deve possibilitar alterar a pontuação do MLX e uma mensagem que possui o status "temperror" ou "Softfail" para que, posteriormente, ela seja analisando conforme os critérios na camada de Antispam;

2.3.5. Deve possibilitar abrir exceções somente para a validação de SPF, possibilitando deixar sempre habilitado este controle;

2.3.6. Deve possuir regras SPF pré-definidas (built-in) para análise de mensagens;

2.3.7. Deve possuir suporte a protocolos de autenticação de email (SPF, DKIM e DMARC);

2.3.8. Deve possuir tecnologia para prevenção de ataques do tipo “Bounce Messages”;

2.3.9. A solução deverá possuir regras de varredura avançadas que permitam especificar as condições que a regra se aplica às mensagens verificadas pela solução;

2.3.10. Entregar agora, realizando o by-pass nos filtros existentes;

2.3.11. Deve possibilitar o descarte de forma silenciosa;

2.3.12. A solução deverá possuir ações através das regras permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra:

2.3.12.1. Criptografar mensagem de email;

2.3.12.2. Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de um cópia oculta (Cco) da mensagem para outras pessoas;

2.3.12.3. Bloqueio, deverá interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e enviar para um destinatário diferente;

2.3.12.4. Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.

2.3.13. Deve ser possível configurar critérios de filtragem de Antispam no mínimo, nos seguintes campos:

2.3.13.1. Tamanho Arquivo Anexo;

2.3.13.2. Tamanho da mensagem;

2.3.13.3. Assunto;

2.3.13.4. Corpo do email;

2.3.13.5. Cabeçalho;

2.3.13.6. Conteúdo do anexo;

2.3.13.7. Nome;

2.3.13.8. Extensão.

2.3.14. A solução deve possibilitar a configuração de políticas de Antispam novas conforme a necessidade;

2.3.15. As mensagens mantidas em quarentena deverão ser revisadas e excluídas manualmente;

2.3.16. A solução deverá possibilitar configurar diferentes tipos de exceções de varredura em um email através de definições de condições e possibilitando executar as ações ou equivalentes de bypass, deleção do email incluindo anexos e quarentenar;

2.3.17. A solução deve prover políticas pré-configuradas de Antispam (built-in) considerando as melhores práticas de segurança para filtragens de e-mails;

2.3.18. A solução deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito;

2.3.19. A solução deverá possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas;

2.3.20. A solução deverá possuir análise de URL's no corpo do e-mail;

2.3.21. A solução deverá possuir Proteção anti-ransomware;

2.3.22. A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações:

2.3.22.1. Remetente;

2.3.22.2. Domínio do destinatário;

2.3.22.3. Data.

2.3.23. Deve possuir lista de bloqueio e lista de permissões (definidas para toda a organização) e pessoais(definidas pelo usuário final);

2.3.24. Deve ser possível criar políticas para classe de IPs, IP, domínios, grupo de usuários e usuários deforma distintas;

2.3.25. Remetentes bloqueados com base no endereço IP, país e região;

2.3.26. Remetentes permitidos com base no endereço IP e país;

2.3.27. A solução deverá ser capaz de permitir a filtragem baseada em reputação IP para no mínimo:

2.3.28. A solução deverá possuir Proteção contra-ataques de Engenharia Social;

2.3.29. A solução deverá fornecer informações detalhadas bem como razões para mensagens de email detectadas como possíveis ataques analisados ou prováveis do Business Email Compromise (BEC);

2.3.30. A solução deverá detectar mensagens de graymail;

2.3.31. A solução deverá ser capaz de detectar spam baseado em assinatura e padrões;

2.3.32. A solução deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que:

2.3.33. Possuam uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de spam;

2.3.34. Possuam uma lista de endereços IP identificados como envolvidos em ransomware ativos, malware ou outras campanhas de ameaças por email;

2.3.35. Possuam uma lista de IPs atribuídos dinamicamente.

2.3.36. A solução deve bloquear mensagens que forem enviadas por IP com baixa reputação ou considerados spammers. A consulta da base de reputação de IP (Blocklist) deve proprietária;

2.3.37. A solução deve possuir um sistema de reputação proprietário para a detecção de spam e phishing, não sendo aceitos sistemas opensource.

2.4. **Módulo de Antispam e Controles de Segurança**

2.4.1. O serviço de continuidade de e-mail deverá fornecer uma caixa de correio para que os usuários possam baixar os e-mails;

2.4.2. Deverá possuir um serviço de continuidade de e-mail para que caso o serviço de e-mail do cliente fique fora do ar ou em manutenção a plataforma armazene os e-mails durante 10 dias;

2.4.3. Deve permitir a criação de políticas baseadas nos níveis de compactação dos anexos;

2.4.4. Deve ter a capacidade de extrair senhas no corpo do e-mail ou no anexo para tentar descriptografar arquivos compactados com senha;

2.4.5. A solução deverá possuir Correspondência de IP do remetente, possibilitando especificar um IP ou um intervalo de endereços IP em um domínio do remetente identificado pelo endereço do cabeçalho da mensagem para permitir mensagens de email apenas desses endereços;

2.4.6. Deve ser capaz de analisar, no mínimo, os arquivos protegidos protegidos por senha, de seguintes extensões:

.ace

.arj

.7z;

.docx

.pdf

.zip

.pptx

.rar

.xlsx

2.4.7. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (TrueType File), Mime Type e nome do arquivo;

2.4.8. Deve seguir RFC 821 (SMTP) para o recebimento e envio de mensagens;

2.4.9. Deve suportar Real-time Blackhole List (RBL);

2.4.10. Deve ser capaz de bloquear e-mails contendo arquivos anexos protegidos por senha ou cifrados;

2.4.11. Deve possuir tecnologia para detecção de ataques de *spoofing* de domínio;

2.4.12. Deve possuir funcionalidade de controle de tráfego SMTP de entrada, realizando a restrição de conexões IP;

2.4.13. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais as regras foram ativadas;

2.4.14. Caso o arquivo e/ou a URL contida no e-mail for considerada maliciosa, eles devem ser bloqueados;

2.4.15. Deve realizar a reescrita das URLs para monitorar o comportamento do usuário interno e bloqueio da página, caso a SandBox deixe passar a ameaça, mas posteriormente a classifique como um phishing direcionado;

2.4.16. Deve suportar a reescrita das URLs contida nos e-mails, caso seja identificada como conteúdo malicioso;

2.4.17. Deve ter a opção de configuração para análise de arquivos protegidos com senha;

2.4.18. A solução deve suportar análise em arquivos nos pacotes Office, PDF e Flash atendendo, no mínimo, as seguintes extensões: .doc, .docx, .xls, .xlsx, .ppt, .pptx, no mínimo;

2.4.19. Quando um arquivo for enviado para análise, o e-mail deve ser retido e não deve ser entregue ao usuário final até que o processo de análise e categorização seja concluído;

2.4.20. O serviço de SandBox deve ser integrado com a console de administração de Antispam;

2.4.21. O serviço de SandBox deve ser proprietário e do mesmo fabricante da solução de Antispam;

2.4.22. Deve realizar a análise comportamental e a análise estática;

2.4.23. Deve realizar a análise do artefato em modo Real-Time;

2.4.24. A solução deve analisar e bloquear possíveis ameaças que utilizam URLs e arquivos anexos desconhecidos;

2.4.25. A solução deve prover o serviço de SandBox, baseado em cloud, para garantir a análise e bloqueio de ameaças conhecidas e desconhecidas incluindo bloqueio de ameaças do tipo zero day, variantes de malwares, phishing, documentos com códigos maliciosos ocultos, entre outros.

2.5. **Módulo de Proteção Avançada (SandBox)**

2.5.1. O número de mensagens bloqueadas porque o número total de mensagens enviadas de um único endereço IP excedeu o limite máximo em um determinado período;

2.5.2. Visão dos usuários que estão em risco;

2.5.3. Visão dos principais 20 usuários mais atacados;

2.5.4. Principais Malwares recebidos versus bloqueados utilizados em URLs maliciosas;

2.5.5. Deverá exibir o número de cliques em cada ameaça;

2.5.6. Número de mensagens bloqueadas porque o endereço de e-mail do remetente foi encontrado na lista de remetentes bloqueados ou na lista de bloqueio global interna;

2.5.7. Número de mensagens bloqueadas porque o endereço de e-mail do destinatário foi encontrado na lista de bloqueio global interna;

2.5.8. Número de ameaças que possuem arquivos detectados como Ransomware;

2.5.9. Número de mensagens com falha de DKIM, SPF e DMARC;

2.5.10. Número de ameaças classificadas como graymail;

2.5.11. Número de ameaças classificadas como SPAM;

2.5.12. Número de ameaças classificadas como phishing;

2.5.13. Número de Arquivos analisados com Malware;

2.5.14. Número de Artefatos analisados pela Sandbox;

2.5.15. Classificação da ameaça;

2.5.16. Visualização de todas as ameaças recebidas;

2.5.17. Deve possuir dashboard com dados dos ataques recebidos e com as seguintes informações:

2.5.18. O dashboard deverá permitir a exportação para formatos JPEG, PNG, PDF e CSV;

2.5.19. A solução deverá possuir dashboards possibilitando no mínimo a visualização de ameaças, ransomwares, detalhes de autenticação baseada em domínio, sandbox, BEC, SPAM, principais violações,eventos de DLP, consumo de banda, proteção Time-of-Click.

2.6. **Dashboard**

2.6.1. A base de inteligência terceira deve ser integrada através dos protocolos TAXII 2.0 ou TAXII 2.1;

2.6.2. Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos:

2.6.2.1. Log;

2.6.2.2. Bloquear/Enviar à quarentena;

2.6.3. Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:

2.6.3.1. Arquivos SHA-1;

2.6.3.2. URLs;

2.6.3.3. IPs;

2.6.3.4. Domínios;

2.6.4. Permitir tomar diferentes ações de resposta no ambiente, no mínimo: bloquear, quarentenar mensagem e deletar mensagem;

2.6.5. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

2.6.6. Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante;

2.6.7. Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta;

2.6.8. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

2.6.9. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação;

2.6.10. Deve ser possível fazer integração com Active Directory;

2.6.11. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

2.6.12. Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente;

2.6.13. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

2.6.14. A solução deve permitir a visualização das estatísticas no dashboard por serviço integrado (Exchange Online, Teams, Onedrive, Sharepoint) ;

2.6.15. Deve ser possível realizar um escaneamento retroativo para identificação de ameaças;

2.6.16. Deve ser possível configurar os destinatários para o recebimento dos resultados do escaneamento;

2.6.17. Deve ser possível realizar escaneamento manual;

2.6.18. Adicionar um objeto suspeito utilizando no mínimo, SHA-1, IP e URL;

2.6.19. Quarantenar uma mensagem considerada maliciosa das caixas de correio de usuários afetas por um phishing;

2.6.20. Após realizar a resposta ao incidente, a solução deve ser capaz de alertar o time de monitoramento e o usuário final, caso este seja configurado;

2.6.21. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo:

2.6.21.1. Status do incidente;

2.6.21.2. Score;

2.6.22. Escopo impactado:

2.6.22.1. Quantidade de contas de e-mail impactadas;

2.6.22.2. Data e hora da detecção;

2.6.22.3. Técnica do MITRE utilizada;

2.6.22.4. Modelo(s) de detecção acionado(s);

2.6.22.5. Objetos detectados dentro de cada modelo.

2.6.23. Será aceito deploy virtual appliance ou SaaS;

2.6.24. Se formato em virtual appliance, deve suportar plataforma de virtualização VmWare ESX/ESXi6.0 no mínimo;

2.6.25. Deve suportar Google G-Suite Gmail App;

2.6.26. Deve suportar Microsoft Office 365;

2.6.27. Solução deve mapear, gerar o incidente e responder de forma automatizada a incidentes relacionados a eventuais fraudes realizadas via email que não tenham sido bloqueadas pela solução de Antispam.

2.7. **Módulo de Análise e Resposta de E-Mails**

2.7.1. **Licenciamento e Garantia**

2.7.2. Todas as licenças deverão ser emitidas pelo Fabricante, com respectivos pacotes de atualização e garantia; Atualização de versão;

2.7.3. Disponibilização de patches corretivos.

2.7.4. Todos os produtos deverão ser fornecidos em sua versão/release mais recente;

2.7.5. A cada nova versão, a CONTRATADA deverá fornecer manuais de uso atualizados da solução, caso existam;

2.7.6. A CONTRATANTE deverá ter como opção executar ou não as atualizações de softwares disponibilizadas;

2.7.7. Os valores referentes ao licenciamento de software e garantia do fabricante, devem estar contidos no valor da solução ofertada.

2.8. **Serviço de Instalação e Treinamento**

2.8.1. A Licitante vencedora será inteiramente responsável pela implantação da solução adquirida, de forma a não comprometer o funcionamento da Solução;

2.8.2. Serão contemplados todos os serviços de instalação de todos os componentes adquiridos;

2.8.3. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos;

2.8.4. Fica a critério do CONTRATANTE, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno. A CONTRATADA deverá comunicar a CONTRATANTE à conclusão da instalação e entregar toda documentação técnica (“As Built”).

2.8.5. Treinamento terá as seguintes características e especificações:

2.8.5.1. O treinamento será realizado online, com a presença de instrutor através deplataforma de vídeo conferência como: Google meeting, Microsoft Teams, ouZoom, possibilitando interação entre participantes;

2.8.5.2. O instrutor deverá realizar o treinamento na língua portuguesa;

2.8.5.3. O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, backup e restauração de configuração, gerenciamento, resolução de problemas e para fins de documentação, caso seja de interesse da administração;

2.8.5.4. Deverá contemplar todos os recursos e configurações existentes na solução ofertada;

2.8.5.5. Deverá ser entregue para a contratante a proposta com o conteúdo do treinamento;

2.8.5.6. É de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização do treinamento;

2.8.5.7. O material didático será fornecido em português, ou inglês, pela contratada, abordando todos os tópicos do curso;

2.8.5.8. A carga horária será de até 40 (quarenta) horas para 1 (uma) turma de até 4 (quatro)alunos;

2.8.5.9. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder carga horária diária de 4 (quatro) horas. Os horários e datas dos treinamentos serão definidos pela equipe técnica da Contratante e comunicados à Contratada com antecedência de 5 (cinco) dias;

2.8.5.10. A Contratante reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo caso não seja satisfatório;

2.8.5.11. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração emitida pelo fabricante;

2.8.5.12. Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

2.9. **Serviço de Suporte Técnico**

2.9.1. O serviço de assistência técnica em GARANTIA deve cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças, ajustes e reparos técnicos em conformidade com manuais e normas técnicas especificadas pelo fabricante;

2.9.2. Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema;

2.9.3. Para efeitos de certificar a garantia, a CONTRATADA deve possuir recurso disponibilizado via web, site do próprio fabricante, que permita verificar a garantia do equipamento através da inserção do seu número de série;

2.9.4. A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia técnica do contrato;

2.9.5. Os serviços de suporte técnico abrangem: Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

2.9.6. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;

2.9.7. Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;

2.9.8. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante;

2.9.9. O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução;

2.9.10. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução;

2.9.11. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão

corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;

2.9.12. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

2.9.13. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

2.9.14. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

2.9.15. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

2.9.16. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web, E-mail, Central 0800 e/ou telefone fixo;

2.9.17. O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete)dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;

2.9.18. O recebimento dos equipamentos será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

2.10. **Vigência do Contrato**

2.10.1. O contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado com base no artigo 57, IV, da Lei 8.666, de 1993, dado que se trata de serviço continuado de utilização de programas de informática.

2.11. **Comprovação de Capacidade Técnica**

2.11.1. Será considerada habilitada, além das exigências administrativas e legais especificadas no edital, a empresa que apresentar atestado de Capacidade Técnico-Operacional, expedido(s) por órgão ou entidade da administração pública ou por empresas privadas, que comprove que a licitante já forneceu e implantou solução de gateway e segurança de e-mails para, pelo menos 40% do quantitativo solicitado. A solução deve possuir a mesma natureza e ser compatível com o objeto descrito no Termo de Referência, incluindo os serviços de configuração, suporte e manutenção da solução;

2.11.2. Os ATESTADOS devem evidenciar explicitamente a execução de objeto compatível ao objeto da presente contratação, de forma aderente às exigências dos requisitos de habilitação técnica;

2.11.3. Diferentes atestados de objetos compatíveis fornecidos por entidades distintas poderão ser somados pelos licitantes;

2.11.4. Declaração do fabricante de solução de gateway e segurança de e-mails informando que o LICITANTE é um parceiro qualificado para comercialização e prestações dos servidos descritos e detalhados no Termo de Referência e anexos.

Documento assinado eletronicamente por **Gleicy Kellen dos Santos Faustino**, **Integrante Técnico**, em 18/10/2022, às 11:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **3966759** e o código CRC **07F78FAF**.

**Referência:** Processo nº 25100.006254/2021-77 SEI nº 3966759