

Nota Técnica nº 115/2026/Diinf/Ctinf-Inmetro

INMETRO/SEI/NÚMERO DO PROTOCOLO
0052600.010616/2025-90Assunto: **ANEXO II - Especificações Técnicas do item 2 - segurança de e-mail (SEG).****1. REQUISITOS GERAIS DE ARQUITETURA, QUANTIDADES E SUPORTE TÉCNICO****1.1. Requisitos Gerais de Arquitetura**

1.2. A solução deverá suportar implantação flexível por meio de Secure Email Gateway virtual dedicado, serviço gerenciado em nuvem e/ou integração via API do mesmo fabricante, conforme a topologia definida pela CONTRATANTE, mantendo o processamento pré-entrega quando exigido e permitindo o uso de serviços cloud do fabricante para sandbox, inteligência de ameaças, proteção de URLs e remediação pós-entrega;

1.3. A solução deverá permitir implementação em ambiente virtual plenamente compatível com VMware ESXi 6.5 ou superior, garantindo o funcionamento estável na infraestrutura de servidores atual da CONTRATANTE, sem exigência de atualizações mandatórias da camada de virtualização;

1.4. A solução deverá prover alta disponibilidade por meio de uma arquitetura resiliente, com múltiplos gateways ou instâncias ativas, distribuíveis entre sites ou zonas, com balanceamento por MX, load balancer ou mecanismo equivalente, continuidade de filas SMTP, failover automático do fluxo de mensagens e administração consistente de políticas. Não será exigido um mecanismo proprietário de cluster lógico estendido quando a disponibilidade for comprovada por um desenho de arquitetura suportado pelo fabricante.

1.4.1. O *appliance* virtual deverá suportar múltiplas interfaces de rede, com no mínimo 3 (três) NICs, permitindo a segregação lógica entre o plano de dados (SMTP), o plano de gerenciamento (GUI/API) e, quando aplicável, uma interface dedicada para sincronização de cluster/alta disponibilidade (HA);

1.4.2. A solução deverá permitir o crescimento horizontal do cluster sem necessidade de adição de novas licenças;

1.5. A solução deverá permitir o processamento e filtragem dos fluxos de e-mail de entrada (*inbound*) e saída (*outbound*) no mesmo cluster de *appliances*, com administração centralizada por meio de um único console de gerenciamento;

1.6. A solução deverá possuir arquitetura que permita futura integração com ambientes de e-mail em nuvem, incluindo Microsoft 365 (Exchange Online) e Google Workspace, possibilitando migração gradual ou coexistência entre ambientes *on-premises* e cloud, sem necessidade de substituição integral da solução;

1.7. A solução deverá utilizar sistema operacional dedicado, fechado e previamente endurecido (*pre-hardened*), com restrição de acesso administrativo ao sistema operacional subjacente, permitindo apenas os acessos necessários à operação da própria solução;

1.8. A solução deverá possuir console de gerenciamento local, hospedado nos appliances implantados no ambiente on-premises da CONTRATANTE, não sendo aceita a dependência exclusiva de console na nuvem do fabricante para a operação básica da solução. É permitido, entretanto, o uso de console específico para acompanhamento das atividades do Sandbox hospedado na nuvem do fabricante;

1.9. A solução deverá operar como Gateway SMTP (MTA - Mail Transfer Agent) e ser tecnicamente compatível com a integração às plataformas de correio eletrônico atualmente utilizadas pela CONTRATANTE, incluindo Microsoft Exchange versão 2010 e Zimbra versão 8.x. A CONTRATADA deverá declarar formalmente a compatibilidade com as versões informadas, responsabilizando-se por eventuais ajustes necessários para plena interoperabilidade;

- 1.10. A solução deverá permitir a proteção e gerenciamento de múltiplos domínios de correio eletrônico por meio de um único console de administração, possibilitando aplicação de políticas específicas por domínio, quando necessário;
- 1.11. A solução deverá permitir a configuração de políticas distintas de filtragem e tratamento para os fluxos de e-mail de entrada (*inbound*) e saída (*outbound*), gerenciados a partir do mesmo console;
- 1.12. A solução deverá possuir console gráfico (GUI) para administração centralizada e acesso ao ambiente de quarentena, com acesso seguro por meio de protocolo HTTPS, garantindo comunicação criptografada entre os administradores (e usuários) e as interfaces;
- 1.13. A solução deverá suportar integração com múltiplos diretórios (Microsoft AD e Linux/LDAP) via os protocolos LDAP e LDAP/LDAPS. Para preservar a estabilidade do ambiente legado, é vedada a instalação de agentes ou qualquer alteração de esquema (schema) nos controladores de domínio da CONTRATANTE;
- 1.14. Todas as funcionalidades da solução deverão ser configuráveis e administráveis por meio da interface gráfica administrativa (GUI), acessível via HTTPS, com controle de perfis e permissões. Não será admitida a necessidade de edição manual de código, scripts, arquivos de configuração internos/externos ou *templates* fora do console de gerenciamento para ativação, parametrização ou manutenção das funcionalidades ofertadas;
- 1.15. Todas as funcionalidades da solução, incluindo mecanismos de detecção, sandbox e inteligência de ameaças, deverão operar de forma integrada e sob responsabilidade técnica e contratual única do fabricante proponente. Não será admitida solução cuja operação dependa da contratação ou do suporte separados de múltiplos fornecedores para o pleno funcionamento das funcionalidades exigidas. Eventuais componentes de terceiros incorporados à solução deverão estar integralmente integrados à plataforma, sob gestão, suporte e SLA unificados pelo fabricante principal, sem ônus adicionais nem necessidade de contratação paralela pela Contratante;
- 1.16. Considerando que soluções de segurança frequentemente declaram o uso de mecanismos de inteligência artificial, a CONTRATADA deverá descrever como tais mecanismos estão integrados à arquitetura da solução ofertada, especificando sua finalidade, o processo de processamento, o fluxo de dados e a responsabilidade pelo tratamento das informações. A utilização de recursos de IA não poderá implicar o encaminhamento não controlado de dados institucionais a serviços externos sem previsão contratual expressa, devendo ser garantidos controles de confidencialidade, integridade e conformidade com a legislação vigente de proteção de dados;
- 1.16.1. Os mecanismos de IA integrados à solução ofertada deverão ser do mesmo fabricante e hospedados no ambiente do fabricante, não sendo permitido o uso de mecanismos de terceiros;
- 1.17. O fabricante deverá disponibilizar guia oficial de dimensionamento (sizing) para appliance virtual, contemplando CPU, memória, armazenamento e rede, de forma a correlacionar a capacidade de processamento com o volume de mensagens da CONTRATANTE;
- 1.18. A solução deverá permitir a realização de backup e restauração completos, incluindo configurações, políticas, listas, perfis, integrações e demais parametrizações, com possibilidade de restauração em novo nó (recovery), bem como suporte ao versionamento de backups;
- 1.19. A solução deverá suportar atualização/upgrade por meio de procedimento controlado em ambiente de cluster ativo-ativo, preferencialmente no modo *rolling upgrade*, de forma a minimizar a indisponibilidade e evitar a necessidade de uma janela de parada total;
- 1.20. A solução deverá oferecer mecanismos adicionais de hardening do plano de gerenciamento, incluindo: controle de acesso baseado em papéis (RBAC) granular, suporte à autenticação multifator (MFA/2FA) para administradores, política de senhas com requisitos configuráveis e bloqueio após tentativas malsucedidas, bem como capacidade de restrição de acesso por origem (ACL) à interface de gerenciamento (GUI/API).

1.21. **Quantidades**

1.22. A solução deverá contemplar a proteção total de até 2.675 (duas mil seiscentos e setenta e cinco) caixas postais durante 36 (trinta e seis) meses ininterruptos.

1.23. **Serviço de Suporte Técnico**

1.24. As subscrições deverão contemplar, durante o período de validade (36 meses), o serviço de suporte técnico ofertado diretamente pelo fabricante da solução, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo feriados, para atendimento a incidentes, dúvidas e problemas relacionados à instalação, configuração, administração e operação da solução. O suporte deverá ser prestado, no mínimo, em língua inglesa, sendo desejável a disponibilidade de atendimento em português (Brasil) ou em espanhol durante o horário comercial. A CONTRATADA deverá assegurar o cumprimento de prazos de resposta e de resolução compatíveis com a criticidade dos chamados, bem como adotar procedimentos de escalonamento e de comunicação periódica do status até a completa resolução dos casos.

1.25. O suporte técnico deverá contemplar, no mínimo: esclarecimento de dúvidas não cobertas pela documentação; diagnóstico e resolução de falhas de funcionamento da solução; orientação quanto à detecção e ao tratamento de ameaças; apoio na utilização de funcionalidades de investigação e resposta (incluindo consultas e análise de telemetria); e assistência na configuração da solução para fins operacionais. O atendimento deverá ser realizado por meio de múltiplos canais, incluindo, no mínimo, portal web, e-mail, telefone e chat, devendo todos os chamados ser registrados e rastreáveis.

1.26. Os chamados de suporte técnico deverão ser classificados conforme os seguintes níveis de severidade: (a) crítica, quando houver indisponibilidade total da solução ou impacto severo em ambiente de produção, sem solução alternativa disponível; (b) alta, quando houver impacto significativo no funcionamento da solução, com degradação relevante, porém com possibilidade de operação parcial; (c) média, quando houver impacto moderado, sem comprometimento crítico das operações; e (d) baixa, para dúvidas, solicitações de configuração ou impactos mínimos sem prejuízo operacional. O atendimento deverá observar os seguintes prazos: até 4 (quatro) horas *corridas* para severidade crítica; até 8 (oito) horas *corridas* para severidade alta; e até 24 (vinte e quatro) horas *úteis* para severidades médias e baixas.

2. **REQUISITOS DE SEGURANÇA E FILTRAGEM DE CONTEÚDO**

2.1. A solução deverá operar como gateway de correio eletrônico em modo pre-delivery, com capacidade de inspecionar, filtrar e bloquear mensagens antes da sua entrega à caixa postal do usuário;

2.2. A solução deverá oferecer remediação pós-entrega por módulo do mesmo fabricante, com mecanismos de remediação pós-delivery para servidores de e-mail Microsoft Exchange, permitindo localizar, analisar, quarentenar ou remover mensagens entregues, inclusive cópias encaminhadas e mensagens distribuídas por listas, por meio de um fluxo centralizado de investigação. Todas as etapas de busca, seleção e exclusão das mensagens deverão ser realizadas exclusivamente através da interface gráfica administrativa (GUI) da solução, de forma centralizada e intuitiva, sendo expressamente vedada a necessidade de criação, edição ou execução manual de scripts (ex.: PowerShell, Python), comandos em terminal (CLI) ou códigos externos para a efetivação da remediação;

2.2.1. O módulo de remediação deverá consumir inteligência do próprio fabricante e permitir enriquecimento por fontes externas, padrões ou integrações suportadas, como STIX/TAXII, feeds de IOCs, SIEM/SOAR ou serviços de reputação, sem exigir contratação separada de ferramenta externa específica para atendimento do requisito

2.2.2. O módulo de remediação pós-delivery também deve ser capaz de remover mensagens da caixa postal dos usuários, sob demanda, independentemente de serem maliciosas ou não;

2.2.3. O módulo de remediação deverá ser capaz de se conectar a servidores de e-mail hospedados na nuvem, como Microsoft 365 ou Google Workspace, sem necessidade de licença adicional;

2.3. A solução deverá comprovar o uso de uma pilha multilayer com IA/ML, análise semântica, análise comportamental, reputação, relação remetente-destinatário, detecção visual (quando aplicável) e telemetria global de ameaças para phishing, BEC, malware, QR phishing e ameaças sem payload;

- 2.4. A solução deverá detectar e mitigar campanhas de engenharia social sem payload, incluindo call-back phishing e TOAD, avaliando linguagem, intenção, tema, urgência, padrões de fraude e contexto do remetente, com aplicação de quarentena, banner, bloqueio ou outra ação definida em política;
- 2.5. Deve ser capaz de identificar tentativas de engenharia social que não utilizem URLs ou anexos, mas induzam o usuário a realizar contato telefônico, com possibilidade de aplicação de ações automáticas de proteção;
- 2.6. A solução deverá disponibilizar um mecanismo de reporte de e-mails suspeitos pelo usuário final (por meio de um botão ou add-in no cliente de e-mail), com preservação integral de cabeçalhos, corpo e anexos, e encaminhamento automático das mensagens para uma caixa de abuso ou para um fluxo centralizado de análise.
- 2.6.1. Deve permitir a execução de ações de remediação automatizadas e/ou assistidas com base no resultado da análise, tais como a remoção pós-entrega, o bloqueio e a atualização de regras.
- 2.7. A remediação pós-entrega deverá suportar operação automatizada para campanhas e ameaças confirmadas, incluindo remoção em massa, acompanhamento do status de execução e capacidade de reversão controlada, quando necessário.
- 2.8. As políticas de antispam e segurança de correio eletrônico deverão ser aplicáveis de forma independente aos fluxos de entrada (inbound) e saída (outbound), permitindo configurações, níveis de inspeção e ações distintas para cada fluxo;
- 2.9. A solução deverá possuir um mecanismo próprio e centralizado de quarentena para mensagens retidas, independentemente das pastas de lixo eletrônico (spam/junk) ou de itens excluídos do sistema de correio eletrônico. Não serão aceitas soluções que utilizem exclusivamente as pastas nativas do servidor de e-mail como substituição ao mecanismo de quarentena da própria solução;
- 2.10. A solução deverá permitir a criação de pastas personalizadas de quarentenas, associando tais pastas a regras ou condições específicas de detecção;
- 2.11. A solução deverá possuir mecanismos de reputação e inteligência contra ameaças integrados nativamente ao produto, sendo o fabricante integralmente responsável pela manutenção, atualização e continuidade desses serviços durante a vigência contratual;
- 2.11.1. Os mecanismos de reputação de IP e de detecção de spam/phishing deverão estar incorporados à solução ofertada, com atualização automática e contínua, não sendo admitida a dependência exclusiva de listas públicas open source ou de serviços externos não garantidos contratualmente pelo fabricante.
- 2.12. A solução deverá possuir um mecanismo de análise da reputação de endereços IP de origem, com capacidade de bloquear automaticamente conexões provenientes de IPs classificados como maliciosos, de baixa reputação ou associados ao envio de spam. A base de reputação utilizada deverá ser mantida e atualizada continuamente pelo fabricante, que será integralmente responsável por sua disponibilidade e funcionamento durante a vigência contratual, não sendo admitida dependência exclusiva de listas públicas *open source*;
- 2.13. A solução deverá classificar e categorizar mensagens com base no tipo de ameaça identificada, permitindo a aplicação de ações distintas por categoria. Deverá, no mínimo, contemplar as seguintes categorias de classificação: (a) Phishing (b) Malware (c) Spam (d) Conteúdo adulto (d) Mensagens em massa ou indesejadas (Bulk/Greymlail);
- 2.14. A solução deverá permitir a criação e aplicação de políticas de filtragem e segurança com base em critérios granulares, incluindo, no mínimo: endereço IP, domínio, grupo de usuários e usuário individual;
- 2.15. A solução deverá possuir mecanismos de lista de remetentes permitidos (allow list) e bloqueados (block list), tanto em nível global (organizacional), definidos pelo administrador da solução, quanto em nível individual, definidos pelo usuário final. As listas globais deverão prevalecer sobre as listas individuais, de modo a garantir o cumprimento das políticas institucionais de segurança;

- 2.16. A CONTRATADA deverá comprovar que a implantação da solução seguirá orientações técnicas oficiais do fabricante, específicas para a versão ofertada, visando garantir baseline adequado de segurança;
- 2.17. A solução deverá permitir a criação, edição e customização de políticas de antispam e segurança de e-mail, conforme as necessidades específicas da CONTRATANTE;
- 2.18. A solução deverá permitir a criação de políticas de e-mail baseadas em múltiplas condições e critérios combináveis, possibilitando o uso de operadores lógicos (E/AND, OU/OR) na definição das regras;
- 2.19. A solução deverá permitir a configuração de critérios de filtragem com base em múltiplos atributos técnicos da mensagem, dos anexos e da conexão SMTP, possibilitando a criação de regras personalizadas, de acordo com as necessidades de segurança da organização. Deverá contemplar, no mínimo, a possibilidade de definição de critérios relacionados a:
- 2.19.1. Características dos anexos (tamanho, extensão, tipo MIME, nome do arquivo, quantidade de anexos, análise de arquivos compactados, profundidade de compactação e tamanho após descompactação);
- 2.19.2. Características do corpo da mensagem (tamanho, conteúdo, idioma e presença de código HTML);
- 2.19.3. Características da conexão SMTP (endereço IP do remetente, hostname, HELO/EHLO domain, envelope sender e envelope recipient, país de origem da conexão);
- 2.19.4. Controle do tamanho total da mensagem e identificação de mensagens criptografadas.
- 2.20. A solução deverá permitir a associação de políticas distintas de antispam a quarentenas específicas e segregadas, possibilitando a retenção das mensagens em pastas ou áreas de quarentena diferenciadas conforme a política aplicada;
- 2.21. As políticas de filtragem deverão permitir a definição das seguintes ações, independentemente da configuração de quarentena associada:
- 2.21.1. Entregar a mensagem ao destinatário final;
- 2.21.2. Bloquear a mensagem com possibilidade de customização da mensagem de retorno SMTP ao remetente;
- 2.21.3. Descartar a mensagem de forma silenciosa;
- 2.21.4. Permitir liberação controlada com exceção dos filtros aplicáveis, conforme política definida pela administração;
- 2.21.5. Enviar cópia da mensagem ao destinatário adicional definido na política;
- 2.21.6. Encaminhar automaticamente a mensagem para sistemas externos de análise, como um sandbox, ou para sistemas de armazenamento, mediante integração configurável.
- 2.22. Adicionalmente, ao executar qualquer ação definida na política de filtragem, a solução deverá permitir a aplicação de modificações controladas na mensagem, incluindo, no mínimo:
- 2.22.1. Alteração ou prefixação do assunto da mensagem;
- 2.22.2. Inserção de aviso ou banner de segurança no corpo da mensagem entregue;
- 2.22.3. Remoção de anexos específicos antes da entrega;
- 2.22.4. Inserção de campos ou marcações adicionais no cabeçalho da mensagem.
- 2.23. A solução deverá possuir mecanismos de prevenção contra backscatter e geração indevida de mensagens de não entrega (NDR), evitando respostas automáticas a remetentes com endereços falsificados ou inexistentes;
- 2.24. A solução deverá suportar validação e aplicação de políticas DMARC para mensagens entrantes, incluindo verificação integrada de SPF e DKIM, com possibilidade de aplicação de ações

conforme política publicada pelo domínio remetente;

2.25. A solução deverá possuir mecanismos de controle e limitação de tráfego SMTP de saída, permitindo identificar e bloquear envios massivos ou comportamentos anômalos por remetente, domínio ou conta de usuário, conforme parâmetros configuráveis pela administração;

2.26. A solução deverá possuir mecanismos de proteção contra ataques de enumeração de diretório (Directory Harvest Attack – DHA), realizando validação de destinatários e bloqueando mensagens direcionadas a endereços inexistentes ou inválidos;

2.27. A solução deverá permitir a criação de regras baseadas em dicionários personalizáveis de palavras-chave ou conteúdos considerados inapropriados, com suporte à inclusão de termos em português do Brasil;

2.28. A solução deverá permitir a inclusão futura de componente para prevenção de perda de dados nas mensagens de saída (outbound) no mesmo cluster e gerenciado no mesmo console;

2.29. A solução deverá possuir mecanismos para detecção e mitigação de tentativas de spoofing de domínio, incluindo verificação de inconsistências em SPF, DKIM e DMARC e identificação de uso indevido de domínios próprios ou semelhantes;

2.30. A solução deverá possuir tecnologia para detecção e mitigação de ataques de spoofing de domínio, incluindo tentativas de falsificação de domínios internos ou domínios confiáveis utilizados em campanhas de phishing e fraude;

2.31. A solução deverá ser capaz de bloquear ou aplicar política restritiva a e-mails contendo arquivos anexos protegidos por senha, criptografados ou que impeçam a inspeção de conteúdo, permitindo configuração de exceções conforme política da organização;

2.32. A solução deverá permitir a inserção automática de avisos visuais (tags ou banners) no corpo do e-mail, com base em critérios de classificação de risco configuráveis pela administração, incluindo, no mínimo:

2.32.1. Remetente externo à organização;

2.32.2. Remetente desconhecido ou não recorrente;

2.32.3. Domínio recentemente registrado;

2.32.4. Falha na autenticação DMARC;

2.32.5. Mensagem classificada como suspeita ou potencialmente insegura;

2.32.6. Uso de domínio com caracteres de script misto (homograph attack);

2.32.7. Indícios de remetente falsificado (impersonation).

2.33. A solução deverá permitir a implementação de mecanismo de proteção específico para usuários classificados como de alto risco, baseado em análise comportamental e histórico de relacionamento, capaz de identificar mensagens provenientes de remetentes sem comunicação prévia ou habitual com o destinatário, com possibilidade de retenção para revisão e mecanismo de aprendizado contínuo baseado em histórico de comunicação ou feedback administrativo;

2.34. A solução deverá fornecer um componente automático de browser isolation para quando usuários classificados como de alto risco cliquem em uma URL contida em qualquer mensagem, mesmo as classificadas como não maliciosas;

2.35. A solução deverá possuir mecanismo de detecção e mitigação de ataques caracterizados por envio massivo e anômalo de mensagens direcionadas a um mesmo destinatário (email bombing), permitindo retenção automática em quarentena para posterior análise;

2.36. A solução deverá detectar Business Email Compromise (BEC), sem anexo ou URL, por meio de análise comportamental, contextual e semântica, correlacionando remetente, destinatário, relacionamento, tema da fraude, intenção, urgência e histórico de ataques, além de identificar usuários mais visados e tendências de campanha;

2.37. Com relação à proteção contra malwares, a solução deverá atender aos seguintes requisitos mínimos:

2.37.1. Deve possuir mecanismo de proteção antimalware com análise dinâmica por sandbox integrada, sem limitação contratual de envio de arquivos para análise;

2.37.2. A funcionalidade de sandbox deverá ser nativa da solução ou fornecida pelo mesmo fabricante responsável pela plataforma principal, garantindo responsabilidade técnica unificada, integração plena e suporte centralizado;

2.37.3. Deve possuir proteção contra ameaças desconhecidas (zero-day/zero-hour), baseada em análise comportamental em sandbox;

2.37.4. Deve realizar proteção do fluxo de mensagens inbound e outbound;

2.37.5. Deve permitir a criação de políticas distintas de proteção para diferentes rotas de e-mail (ex.: inbound, outbound, interno);

2.37.6. As bases de detecção, reputação, modelos e inteligência de ameaças deverão ser atualizados continuamente ou em near real-time pelo fabricante, sem depender de janela manual de atualização e com evidência da propagação operacional de novos veredictos.

2.38. A solução deverá suportar criptografia TLS para o tráfego SMTP (entrada e saída) em integração com o Exchange on-premises, incluindo a capacidade de forçar o uso de TLS por domínio ou parceiro, bem como validar certificados de acordo com política definida, quando aplicável;

2.39. A solução deverá permitir a inspeção e o controle de anexos, com suporte à extração de conteúdo e à aplicação de políticas por tipo de arquivo (MIME/extensão), incluindo o bloqueio de arquivos com dupla extensão (double extension), de arquivos executáveis e de anexos potencialmente perigosos (por exemplo, macros), conforme a política.

Deverá, ainda, permitir a definição de políticas específicas por rota, por usuário, por grupo e por domínio;

2.40. A solução deverá permitir a inspeção de arquivos compactados (ZIP, RAR, 7z e similares), com limites configuráveis de profundidade e tamanho, bem como tratamento explícito de anexos criptografados ou protegidos por senha (por exemplo, quarentena, bloqueio ou encaminhamento para revisão);

2.41. A solução deverá suportar mecanismos de identificação e tratamento de mensagens do tipo bulk mail e newsletter (graymail), com categorização distinta de spam e malware, permitindo sua entrega em caixa de baixa prioridade ou em quarentena específica, conforme a política;

2.42. A solução deverá disponibilizar mecanismos adicionais para detecção de ataques de BEC (*Business Email Compromise*) e de impersonação, incluindo, no mínimo: (i) inconsistência entre os campos "From", "Reply-To" e *envelope sender*; (ii) detecção de *display name spoofing*; (iii) identificação de domínios semelhantes (*lookalike / typosquatting*); e (iv) detecção de remetentes recém-observados (*new sender*), com reforço de alerta;

2.43. A solução deverá permitir a criação de políticas de proteção baseadas em perfis de risco, com aplicação de controles mais restritivos (tais como quarentena preventiva, banners reforçados e exigência de sandbox), sem impacto indevido aos demais usuários;

2.44. A solução deverá suportar controles de integridade do fluxo SMTP e mecanismos antievasão, incluindo detecção de anomalias de sessão (por exemplo, padrões de conexão e tentativas de *bypass*), com aplicação de *throttling* e/ou *greylisting*, quando aplicável;

2.45. A solução deverá suportar a personalização de tags, banners e mensagens de aviso em HTML, incluindo, no mínimo, as seguintes categorias: "Externo", "Remetente desconhecido", "DMARC falhou", "Potencialmente suplantado" e "Domínio recentemente registrado", quando suportado;

2.46. A solução deverá prover mecanismos de aprendizagem e adaptação de higiene de e-mail (*adaptive hygiene*), baseados no comportamento do usuário (por exemplo, ações de liberar, quarentenar ou reportar mensagens suspeitas), com o objetivo de reduzir falsos positivos ao longo do tempo.

3. REQUISITOS DE ANÁLISE DINÂMICA E PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

3.1. A solução deverá prover mecanismo de análise dinâmica em ambiente controlado (sandbox), integrado nativamente à plataforma, destinado à detecção e ao bloqueio de ameaças conhecidas e desconhecidas, incluindo, no mínimo: ataques do tipo zero-hour, variantes de malware, phishing com roubo de credenciais e documentos contendo códigos maliciosos ocultos;

3.2. O mecanismo de sandbox deverá permitir a análise comportamental de arquivos e objetos suspeitos, com capacidade de identificar ações maliciosas durante sua execução em ambiente isolado;

3.3. A solução deverá realizar análise e bloqueio, em tempo real ou próximo ao tempo real, de ameaças veiculadas por URLs e arquivos anexos, tanto no fluxo de mensagens inbound quanto no outbound;

3.4. A solução deverá permitir a criação de políticas e regras administrativas que definam, de forma granular, quando objetos (arquivos, URLs ou mensagens) serão submetidos à análise em sandbox, bem como as ações a serem aplicadas com base no resultado da análise;

3.5. O mecanismo de sandbox deverá ser fornecido como parte integrante da solução ofertada, sob responsabilidade técnica do mesmo fabricante da plataforma principal, não sendo admitida simples intermediação de serviços genéricos de terceiros sem integração nativa e suporte unificado;

3.6. A solução deverá permitir a personalização do período máximo de análise de URLs e anexos pelo Sandbox, e das ações quando a análise exceder o período máximo configurado. As ações possíveis devem conter as seguintes opções, no mínimo: entregar a mensagem, enviar à quarentena, descartar a mensagem, alterar o cabeçalho e reenviar a mensagem para outro destinatário;

3.6.1. A solução deve permitir que a configuração acima seja restrita a um domínio ou a um grupo de usuários

3.7. A console de sandbox deverá ser acessível a partir do console central de administração da solução, permitindo visualização de eventos, relatórios, status de análise, configuração de políticas e auditoria;

3.8. Quando um arquivo ou objeto for encaminhado para análise dinâmica, a solução deverá permitir a retenção temporária da mensagem até a conclusão do processo de análise e classificação, aplicando automaticamente a ação configurada conforme o resultado obtido;

3.9. A solução deverá permitir o bloqueio de arquivos anexos com base em listas de *hashes* (ex.: SHA-256 ou algoritmo equivalente), possibilitando a criação e gestão de listas personalizadas de bloqueio;

3.10. A solução deverá suportar mecanismo de reescrita de URLs contidas em mensagens de email, independentemente da classificação de risco, mesmo para mensagens consideradas não maliciosas, permitindo sua aplicação de forma global ou com base em categorias de classificação definidas pela solução (por exemplo, phishing, spam, conteúdo adulto, envio em massa ou equivalentes técnicos);

3.10.1. A proteção de URLs deverá reavaliar o destino no momento do clique, em qualquer dispositivo ou rede, mesmo quando a URL tenha sido considerada benigna na entrega, bloqueando ou advertindo quando houver mudança de veredito;

3.10.2. O mecanismo de reescrita de URL deverá permitir a configuração de políticas por domínio, grupo ou usuário, abrangendo a parte da mensagem onde a URL será reescrita (corpo, anexo), reenvio da mensagem a outro destinatário e exclusões;

3.10.3. A solução deverá registrar telemetria de cliques em URLs reescritas e permitir a execução de ações automáticas de bloqueio e de remediação pós-entrega quando uma URL for posteriormente classificada como maliciosa.

3.11. A solução deverá oferecer isolamento de navegação para URLs suspeitas ou desconhecidas, aplicável, por política, a usuários de alto risco ou perfis definidos, sem instalação de agente no endpoint e com evidência de que o conteúdo ativo não é entregue ao dispositivo.

- 3.12. As mensagens que contenham arquivos ou objetos previamente identificados e classificados como maliciosos pela solução deverão estar sujeitas à aplicação automática das ações definidas pela administração, incluindo, no mínimo, bloqueio e encaminhamento para quarentena;
- 3.13. A solução deverá permitir a definição de domínios ou remetentes confiáveis (*allowlist*), para os quais poderá ser dispensada a aplicação de reescrita de URLs, conforme política administrativa;
- 3.14. Caso arquivos anexos ou URLs sejam classificados como maliciosos pelos mecanismos de análise da solução, deverá ser possível aplicar automaticamente ações de bloqueio, quarentena ou outra medida de contenção previamente definida na política de segurança;
- 3.15. A solução deverá possuir mecanismos de verificação e reputação de URLs capazes de identificar indícios de comprometimento em websites acessíveis por meio de links contidos nas mensagens, ainda que o domínio de origem seja legítimo, permitindo a aplicação automática de ações de bloqueio, neutralização do link ou advertência ao usuário, conforme política definida;
- 3.16. A solução deverá ser capaz de realizar a extração e análise de códigos QR (QR Code) presentes nas mensagens de e-mail, incluindo a submissão das URLs extraídas para mecanismos de análise dinâmica (sandbox ou tecnologia equivalente) antes da entrega da mensagem ao usuário final, conforme política configurada;
- 3.17. A solução deverá permitir a análise de códigos QR (QR Code) presentes em mensagens reportadas pelos usuários como suspeitas, submetendo as URLs extraídas aos mecanismos de inspeção e aplicando automaticamente as ações definidas pela administração;
- 3.18. A solução deverá disponibilizar um painel analítico orientado ao usuário, correlacionando ameaças recebidas, cliques, mensagens reportadas, comportamento, exposição, severidade, campanhas e usuários críticos ou mais atacados. Deverá contemplar, no mínimo:
- 3.18.1. Classificação das ameaças por tipo (URL maliciosa, anexo malicioso ou ambos), vetor de ataque e nível de severidade;
- 3.18.2. Identificação de indícios de ataques direcionados (*targeted attacks*) e campanhas coordenadas, conforme mecanismos analíticos da solução;
- 3.18.3. Métricas consolidadas e históricas de URLs maliciosas recebidas, bloqueadas e efetivamente acessadas;
- 3.18.4. Identificação automática dos usuários mais visados por ameaças e daqueles que interagiram com conteúdos maliciosos;
- 3.18.5. Geração automática de indicador de risco ou exposição por usuário, baseado na correlação entre volume de ameaças recebidas, interações realizadas e criticidade do perfil;
- 3.18.6. Possibilidade de detalhamento individual por usuário, incluindo histórico de eventos e interações;
- 3.18.7. Visão específica dos usuários cadastrados e classificados pela CONTRATANTE como críticos, estratégicos ou de alta sensibilidade operacional, bem como das ameaças direcionadas a esses perfis;
- 3.19. A solução deverá identificar automaticamente os usuários mais atacados e disponibilizar insights de ameaça (ex.: tendências por ator/campanha, temas recorrentes e evolução temporal), permitindo aplicação de controles reforçados para esses perfis;
- 3.20. A solução de sandbox deverá correlacionar os resultados das análises dinâmicas e estáticas de arquivos, URLs e artefatos comportamentais com múltiplas fontes de inteligência de ameaças (*threat intelligence*), próprias e/ou de terceiros, com atualização automática. Deverá também:
- 3.20.1. Fornecer também relatório forense detalhado por amostra (arquivo/URL), contendo, pelo menos: veredito, comportamento observado, artefatos gerados, indicadores (IOCs), linhas do tempo e evidências de rede/processo;
- 3.20.2. O painel de informações sobre as ameaças avançadas detectadas deverá conter a classificação conforme o padrão MITRE ATT&CK;

- 3.20.3. O administrador deverá ser capaz de acessar qualquer URL detectada como maliciosa em ambiente isolado (browser isolation) a partir do console do Sandbox;
- 3.20.4. O sandbox deverá fornecer informações detalhadas de forensics, especificando as razões pelas quais uma URL ou arquivo foi bloqueado, e exemplos contidos nas mensagens;
- 3.20.5. Permitir exportação de eventos para SIEM/SOAR.
- 3.20.6. Suportar mecanismos de análise capazes de identificar e mitigar técnicas comuns de evasão (por exemplo, detecção de máquina virtual, *time delay* e *geofencing*), bem como demonstrar capacidade de detonação em múltiplos perfis de ambiente (por exemplo, diferentes sistemas operacionais e aplicações amplamente utilizadas).
- 3.21. A proteção de URLs em tempo de clique (click-time protection) deverá suportar a análise de cadeias de redirecionamento e de serviços de encurtamento de URLs, bem como a detecção de páginas de phishing de credenciais, ainda que não envolvam o download de payload, com aplicação de bloqueio por meio de uma página de aviso configurável.
- 3.21.1. A solução deverá permitir a definição de exceções controladas (*allowlist*) para mecanismos de reescrita e análise de URLs, bem como para *sandbox*, de forma a evitar impacto indevido em aplicações corporativas, com registro de auditoria das exceções e respectivas justificativas;
- 3.21.2. A solução deverá suportar a identificação de campanhas e ataques correlacionados, permitindo operações de busca e pivoteamento (*search/pivot*) por indicadores de comprometimento (IOCs) — tais como hash, URL, domínio e endereço IP — bem como por usuário-alvo, com indicação da abrangência do incidente (por exemplo, número de destinatários afetados);
- 3.21.3. A solução deverá suportar remediação pós-entrega quando uma URL, anexo ou mensagem tiver o veredito alterado para malicioso, localizando mensagens correlatas, removendo-as ou colocando-as em quarentena e registrando uma auditoria completa.
- 3.21.4. A solução deverá suportar o isolamento de navegação para links suspeitos, aplicável ao público definido na licença (por exemplo, usuários de alto risco), com definição de políticas sobre quando aplicar o isolamento e com evidência de que o endpoint não receba conteúdo malicioso.

4. REQUISITOS E GESTÃO E ADMINISTRAÇÃO DE QUARENTENA

- 4.1. A solução deverá possuir mecanismo completo de gestão de quarentena para mensagens retidas nos fluxos de entrada e saída, atendendo aos seguintes requisitos:
- 4.1.1. Deve suportar a segregação lógica de quarentenas por política de segurança, permitindo a existência de quarentenas distintas associadas a diferentes regras ou políticas configuradas na solução;
- 4.1.2. Deve suportar quarentenas individualizadas por usuário, permitindo que cada usuário final realize a gestão das mensagens retidas associadas à sua conta;
- 4.1.3. Deve permitir ao administrador a pesquisa e consulta centralizadas de mensagens retidas nas quarentenas individuais dos usuários, com possibilidade de filtragem por fluxo de mensagens (entrada e saída), remetente, destinatário, assunto, período (data e hora), status da mensagem (ex.: retida, liberada, bloqueada) e outros metadados disponíveis na solução, permitindo a aplicação simultânea de múltiplos filtros;
- 4.1.4. Os resultados da pesquisa deverão ser apresentados em formato estruturado (ex.: tabela ou visualização equivalente), contendo informações essenciais da mensagem, como remetente, destinatário, assunto, data e hora, classificação ou categorização de segurança, status de tratamento e demais metadados relevantes disponíveis na solução.
- 4.1.5. O armazenamento e a gestão da quarentena deverão ser centralizados para os fluxos de entrada e saída, sem a necessidade de infraestrutura adicional além dos componentes nativos da própria solução ofertada;
- 4.1.6. O tempo de retenção das mensagens em quarentena deverá ser configurável pelo administrador, para período mínimo de 30 (trinta) dias ou superior, conforme capacidade da solução;

4.1.7. A solução deverá prover acesso à quarentena por meio de portal web seguro utilizando protocolo HTTPS, bem como por comunicação via e-mail aos usuários finais para gestão das mensagens retidas;

4.1.8. Deve permitir ao administrador a execução de ações centralizadas sobre mensagens retidas, inclusive em lote, tais como liberação, bloqueio, reporte de falso positivo e outras ações equivalentes disponíveis na solução.

4.1.9. O portal de quarentena do usuário final e a comunicação via e-mail a esses usuários deverão suportar múltiplos idiomas, sendo disponibilizados, no mínimo, nos idiomas português (Brasil) e inglês (Estados Unidos);

4.1.10. A comunicação via e-mail e o portal de quarentena do usuário final deverão permitir personalização visual institucional, incluindo a inserção do logotipo da CONTRATANTE e customização de elementos visuais compatíveis com sua identidade institucional;

4.1.11. A solução deverá permitir que o usuário final administre sua própria lista de remetentes permitidos (allow list) e bloqueados (block list) , com aplicação automática às mensagens recebidas, respeitadas as políticas globais definidas pelo administrador;

4.1.12. A solução deverá disponibilizar acesso a informações detalhadas das mensagens retidas, incluindo, no mínimo, remetente, destinatário, assunto, data e hora (timestamp), status de tratamento e classificação de segurança atribuída pela ferramenta, de forma a permitir a investigação, a auditoria e o tratamento de incidentes. Quando aplicável, deverão ser apresentadas informações técnicas adicionais, como registros de cabeçalho (headers), endereço IP de origem e demais metadados relevantes à análise de segurança;

4.1.13. A solução deverá manter trilha de auditoria detalhada das ações realizadas sobre mensagens em quarentena, incluindo identificação do usuário ou administrador responsável, data e hora da ação, tipo de ação executada e resultado obtido, para fins de auditoria e rastreabilidade;

4.1.14. A solução deverá permitir controle de acesso baseado em perfis (RBAC), possibilitando a delegação de permissões específicas para consulta, liberação ou bloqueio de mensagens em quarentena, conforme política definida pela CONTRATANTE;

4.1.15. A solução deverá enviar, por e-mail, um relatório de quarentena aos usuários finais (e-mail digest), contendo a listagem das mensagens retidas e permitindo a execução de ações diretamente a partir do próprio e-mail, sem necessidade de acesso ao portal web. Deverá permitir a configuração da periodicidade de envio automático do relatório de quarentena, com frequência mínima configurável de até 12 (doze) horas. O relatório deverá, no mínimo, permitir as seguintes ações sobre as mensagens diretamente pela caixa postal sem a necessidade de uso do portal de quarentena do usuário:

4.1.15.1. Visualização prévia segura do conteúdo da mensagem retida, incluindo remetente, destinatário, assunto e corpo da mensagem, com remoção ou neutralização de conteúdo ativo e bloqueio padrão de imagens ou elementos potencialmente executáveis;

4.1.15.2. Liberação da mensagem sem aprovação permanente do remetente;

4.1.15.3. Permitir o reporte de mensagens classificadas pela solução como indevidas (falso positivo) ou como não detectadas (falso negativo), incluindo categorias como spam ou phishing, diretamente a partir do relatório de quarentena ou do portal web;

4.1.15.4. Liberação da mensagem com aprovação permanente do remetente, quando aplicável e respeitadas as políticas globais definidas pelo administrador;

4.1.15.5. Bloqueio do remetente, com inclusão automática na lista de remetentes bloqueados do usuário, aplicável a mensagens futuras, respeitando as políticas globais definidas pelo administrador.

4.2. Adicionalmente, deverá permitir:

4.2.1. Solicitação de atualização e reenvio do relatório de quarentena sob demanda, sem necessidade de autenticação e independentemente da periodicidade automática configurada na solução;

- 4.3. A quarentena deverá permitir a visualização segura do conteúdo das mensagens (por exemplo, renderização em texto plano ou *preview* seguro), evitando a execução de conteúdo ativo durante a análise;
- 4.4. A solução deverá permitir a definição de diferentes períodos de retenção por tipo de quarentena (spam, *bulk*, suspeito e malware) e por política, com possibilidade de ajuste sem necessidade de reinício do serviço;
- 4.5. A solução deverá permitir a liberação de mensagens com reprocessamento opcional, forçando a reaplicação de políticas e motores atualizados antes da entrega ao destinatário;
- 4.6. A solução deverá suportar a delegação de acesso à quarentena a diferentes equipes (por exemplo, SOC e mensageria), por meio de controle de acesso baseado em papéis (RBAC), com perfis de somente leitura, revisão/aprovação e administração completa.

5. REQUISITOS DE MONITORAMENTO E RASTREAMENTO

- 5.1. A solução deverá disponibilizar visualização em tempo real ou quase em tempo real (near real-time), por meio da interface gráfica de gerenciamento (GUI):
 - 5.1.1. Visualização atualizada do processamento das filas de e-mail;
 - 5.1.2. Visualização das conexões SMTP externas ativas e recentes;
 - 5.1.3. Acesso a relatórios operacionais e gerenciais diretamente no próprio console de gerenciamento, sem necessidade de integração obrigatória com produtos de terceiros, soluções “open source” ou servidores adicionais para visualização básica das informações;
 - 5.1.4. Recurso nativo de rastreamento de mensagens (message tracking), sem necessidade de integração obrigatória com ferramentas de terceiros, open source ou infraestrutura adicional para fins exclusivos de consulta. A funcionalidade deverá permitir o rastreamento utilizando, no mínimo, os seguintes parâmetros:
 - 5.1.4.1. Endereço IP do remetente e do destinatário;
 - 5.1.4.2. Endereço de e-mail do remetente e do destinatário;
 - 5.1.4.3. Assunto da mensagem;
 - 5.1.4.4. Hostname ou endereço IP do servidor de e-mail remetente;
 - 5.1.4.5. Nome do anexo;
 - 5.1.4.6. Ação final aplicada pelo sistema (ex.: entregue, bloqueada, quarentenada, diferida, rejeitada);
 - 5.1.4.7. Regra ou política responsável pelo tratamento da mensagem.
- 5.2. Adicionalmente, a solução deverá suportar a integração com sistemas externos de coleta de logs via protocolo Syslog, tanto em ambientes on-premises quanto na cloud, permitindo o envio de eventos e registros para soluções de monitoramento, auditoria ou SIEM.
- 5.3. A solução deverá disponibilizar mecanismos de alerta configuráveis para eventos operacionais e de segurança (por exemplo, indisponibilidade de nó, filas acima de limiar, falha de atualização, surtos de spam e detecção de campanhas), com envio por e-mail e/ou integração via Syslog;
- 5.4. A solução deverá disponibilizar relatórios e *dashboards* de eficácia, incluindo, no mínimo: volume por categoria (spam, *graymail*, phishing, malware e BEC), principais remetentes e destinatários, tendências de detecção e identificação dos usuários mais visados;
- 5.5. A solução deverá manter retenção mínima local de logs e trilhas de auditoria para consulta operacional (no mínimo, 30 dias de logs de processamento e 12 meses de auditoria administrativa), ou disponibilizar um mecanismo de exportação contínua para retenção estendida em solução externa, como SIEM;

- 5.6. A solução deverá disponibilizar integração via API para consulta e automação de mensagens, vereditos, quarentena, eventos, IOCs e ações de remediação, com credenciais controladas, revogação e auditoria de uso;
- 5.7. A solução deverá permitir a exportação de relatórios em formatos abertos (CSV, PDF e HTML) e, quando aplicável, o agendamento de relatórios periódicos para envio automático a grupos definidos;
- 5.8. A solução deverá disponibilizar mecanismos de pesquisa avançada e pivoteamento, com suporte a múltiplos critérios (por exemplo, hash, URL, endereço IP, assunto, *message-id* e regra aplicada), permitindo uma investigação ágil e repetível de incidentes.

6. SERVIÇOS DE IMPLANTAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRATADA

- 6.1. A CONTRATADA deverá conduzir a implantação da solução de forma planejada, controlada e validada, sendo responsável pela entrega da solução em pleno funcionamento, conforme os requisitos deste Termo de Referência.
- 6.2. Previamente à implantação, a CONTRATADA deverá apresentar um Plano de Implantação, contendo, no mínimo: a arquitetura da solução (incluindo a distribuição entre os sites e a operação em modo ativo-ativo), fluxos de e-mail, integrações, políticas iniciais, cronograma de execução, riscos identificados e respectivas estratégias de mitigação. O plano deverá ser submetido à aprovação da CONTRATANTE.
- 6.3. A implantação deverá contemplar a configuração completa da solução, incluindo a integração com a infraestrutura existente, configuração de domínios, conectores, certificados digitais, políticas de segurança e mecanismos de alta disponibilidade, garantindo o correto funcionamento do fluxo de envio e recebimento de e-mails.
- 6.4. A CONTRATADA deverá disponibilizar um ambiente de testes e realizar validação prévia à entrada em produção, contemplando, no mínimo: verificação do fluxo de mensagens, aplicação de políticas de segurança, detecção de ameaças simuladas e validação de mecanismos de alta disponibilidade. Os resultados dos testes deverão ser registrados e apresentados à CONTRATANTE.
- 6.5. A entrada em produção deverá ser realizada de forma controlada, com definição de janela de mudança, validação assistida do funcionamento e previsão de procedimentos de rollback em caso de falhas.
- 6.6. A solução somente será considerada implantada após a comprovação do funcionamento adequado em produção, incluindo o fluxo correto de mensagens, a aplicação efetiva das políticas de segurança e a disponibilidade dos serviços.
- 6.7. A CONTRATADA deverá entregar documentação técnica completa e atualizada, contendo a arquitetura implementada, as configurações realizadas, as políticas aplicadas, as integrações e os procedimentos operacionais (runbooks), de modo a permitir a administração e a operação da solução pela equipe da CONTRATANTE.
- 6.8. Após a entrada em produção, a CONTRATADA deverá prestar suporte assistido durante o período de estabilização, incluindo ajustes de políticas, redução de falsos positivos e negativos e acompanhamento do desempenho da solução, até sua plena operação.

7. TRANSFERÊNCIA DE CONHECIMENTO

- 7.1. A CONTRATADA deverá transferir à equipe técnica da CONTRATANTE o conhecimento sobre a solução implantada.
- 7.2. A CONTRATADA deverá apresentar um Plano de Transferência de Conhecimento, a ser aprovado pela CONTRATANTE, que contemple o conteúdo programático, a carga horária e a abordagem prática.

- 7.3. A transferência de conhecimento deverá ser realizada no ambiente já implantado na CONTRATANTE, contemplando atividades práticas (hands-on), de modo a capacitar a equipe para operação autônoma da solução.
- 7.4. O conteúdo mínimo deverá abranger:
- 7.5. Administração e operação da solução (console).
- 7.6. Criação e ajuste de políticas de segurança.
- 7.7. Monitoramento de alertas e eventos.
- 7.8. Geração de relatórios.
- 7.9. Boas práticas de operação e manutenção.
- 7.10. A transferência de conhecimento deverá ser realizada na modalidade remota (EAD) em horários acordados com a CONTRATANTE.
- 7.11. Todo o material didático deverá ser fornecido pela CONTRATADA, incluindo guias operacionais, manuais e documentação da solução.
- 7.12. Ao final da transferência de conhecimento, a CONTRATADA deverá disponibilizar documentação complementar, incluindo procedimentos operacionais (playbooks), relativos às principais atividades da solução.
- 7.13. A transferência de conhecimento será considerada concluída após a validação da CONTRATANTE quanto à capacidade da equipe de operar a solução de forma autônoma.
- 7.14. Caso a CONTRATANTE identifique insuficiência de capacitação, a CONTRATADA deverá realizar sessões complementares, sem ônus adicional.

8. TESTE DE BANCADA (PROVA DE CONCEITO – POC) DA SOLUÇÃO DE SEG

- 8.1. A licitante provisoriamente classificada em primeiro lugar deverá submeter a solução ofertada ao Teste de Bancada (PoC), com o objetivo de comprovar, de forma prática, o atendimento aos requisitos técnicos estabelecidos neste Termo de Referência.
- 8.2. A PoC terá duração de até 6 (seis) horas e deverá ser realizada em ambiente controlado, disponibilizado pela licitante, no prazo máximo de 5 (cinco) dias úteis após a convocação formal, podendo utilizar ambiente SaaS, cloud-delivered ou híbrido do fabricante, desde que equivalente aos módulos ofertados. A PoC deverá permitir a validação pela CONTRATANTE, inclusive por meio da execução de testes independentes com amostras seguras, controladas e previamente acordadas.
- 8.3. A licitante deverá preparar previamente o ambiente, incluindo consoles, integrações, contas de teste, políticas, módulos licenciados e amostras controladas, garantindo que todos os cenários de teste estejam aptos à execução no momento da avaliação.
- 8.4. Durante a PoC, os licitantes deverão demonstrar, de forma prática, nos consoles, módulos e integrações do mesmo fabricante ofertados para a solução, no mínimo, os seguintes cenários:
- a) Bloqueio, quarentena, tag ou ação preventiva para amostras controladas de phishing, BEC e malware, incluindo casos de BEC ou engenharia social sem URL e sem anexo, com evidência do veredito, categoria da ameaça, política aplicada e ação executada;
 - b) Reescrita de URLs e proteção em tempo de clique, incluindo caso de URL que seja reclassificada após a entrega ou cenário equivalente demonstrado por URL controlada/homologada pelo fabricante, com evidência do clique, veredito no momento da interação e ação aplicada;
 - c) Submissão de anexos suspeitos para análise avançada/sandbox, com retenção até o veredito, quando aplicável, e ação automática conforme a política e o relatório técnico sobre o comportamento observado. Para URLs, será aceita arquitetura de reescrita,

análise em tempo de clique, reputação, sandbox ou tecnologia equivalente, com reclassificação posterior e evidência de bloqueio, aviso ou contenção;

d) Isolamento de navegação para links suspeitos, desconhecidos ou de risco, quando aplicável e licenciado, demonstrando as políticas de restrição, o usuário ou grupo protegido e a evidência de que o acesso foi realizado em ambiente isolado;

e) Gestão de quarentena por portal, console administrativo e/ou e-mail digest, com demonstração de ações do usuário ou administrador, visualização segura quando aplicável e auditoria das ações executadas;

f) Rastreamento de mensagens com filtros por remetente, destinatário, assunto, IP ou relay quando disponível, message-id, veredito, política/regra e ação aplicada, incluindo correlação com URL, anexo ou campanha quando tais metadados existirem;

g) Remediação pós-entrega por módulo cloud do mesmo fabricante, com capacidade de localizar e remover, quarentenar ou aplicar ação equivalente sobre a mesma mensagem em múltiplas caixas postais nas plataformas suportadas, apresentando evidência do escopo, status por destinatário e auditoria da ação;

h) Workflow de reporte pelo usuário por botão, add-in ou mecanismo equivalente, com preservação de cabeçalhos, corpo e anexos, análise automática ou assistida do e-mail reportado, classificação da ameaça, busca de mensagens similares quando aplicável e feedback ao usuário ou ao time de segurança;

i) Validação de DMARC, SPF e DKIM no fluxo de e-mail, com evidência do veredito e da ação aplicada, como bloqueio, quarentena, tag, banner ou entrega controlada, incluindo caso controlado de spoofing em domínio de teste ou domínio previamente preparado para a PoC;

j) Teste de detecção de QR code malicioso ou suspeito em corpo de e-mail ou anexo suportado, imagem ou PDF, com evidência de extração da URL ou tratamento equivalente do destino identificado, veredito e ação aplicada pela política;

k) Teste de TOAD/call-back phishing: e-mail sem URL e sem anexo induzindo ligação telefônica ou ação de risco, com evidência de detecção semântica ou contextual, classificação da ameaça e ação aplicada, como bloqueio, quarentena, tag ou banner;

l) Teste de disponibilidade/failover: simulação de indisponibilidade de componente, rota ou destino de entrega durante o processamento, com evidência de continuidade do serviço, enfileiramento, retry, ausência de perda de mensagens e de rastreabilidade. Para soluções SaaS ou cloud-delivered, será aceita evidência de arquitetura resiliente do fabricante e demonstração prática de continuidade operacional, sem exigência de sincronização de cluster local entre appliances;

m) Teste de exportação de logs, eventos ou vereditos via Syslog, API, conector, webhook ou mecanismo equivalente oficialmente suportado, com evidência de campos mínimos ou equivalentes, como message-id, veredito, ação, regra/política, timestamp, remetente e destinatário, quando disponíveis.

8.5. A CONTRATANTE poderá, durante a execução, conduzir ou solicitar a execução direta de testes adicionais ou variações nos cenários, com o objetivo de verificar a usabilidade, a operação e o atendimento aos requisitos da solução, desde que tais testes estejam relacionados ao escopo ofertado, utilizem amostras seguras e controladas, e sejam compatíveis com os módulos, integrações e o ambiente disponibilizados para a PoC.

8.6. A solução será considerada aprovada caso demonstre, de forma satisfatória, o atendimento aos cenários de teste definidos neste Termo de Referência e aos requisitos essenciais estabelecidos, por meio de funcionalidades nativas, módulos integrados do mesmo fabricante ou de arquitetura equivalente suportada, desde que comprovado o resultado técnico esperado.

8.7. O descumprimento dos requisitos essenciais implicará a desclassificação da licitante quando não houver atendimento por funcionalidade nativa, por módulo ofertado do mesmo fabricante, por integração suportada ou por mecanismo equivalente que comprove o resultado técnico exigido.

8.8. Todos os custos relacionados ao Teste de Bancada serão de responsabilidade da licitante.

8.9. A CONTRATANTE poderá registrar as evidências e elaborar um relatório técnico com os resultados obtidos na PoC, incluindo telas, logs, relatórios, trilhas de auditoria, eventos exportados e evidências obtidas nos consoles e módulos da solução ofertada.

Duque de Caxias, na data da assinatura.



DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO
ART. 6º, § 1º, DO [DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015](#) EM
17/07/2026, ÀS 14:52, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

ANDRE GHEVENTER

Integrante Técnico da Equipe de Planejamento da Contratação



DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO
ART. 6º, § 1º, DO [DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015](#) EM
17/07/2026, ÀS 15:01, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

PAULO GUSTAVO DE OLIVEIRA DEL PELOSO

Integrante Requisitante da Equipe de Planejamento da Contratação

A autenticidade deste documento pode ser conferida no site

https://sei.inmetro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0,
informando o código verificador **2527143** e o código CRC
F5B779D8.

