Política Corporativa de Segurança da Informação e Proteção de Dados Pessoais - POSIC

Sumário

IDENTIFICAÇÃO GERAL

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

CNPJ: 34.028.316/0001-03 - NIRE: 5350000030-5

Empresa Pública de Capital Fechado

Elaboração: Gerência de Normas e Processos de Informação - GNPI/DESID

Aprovação:

Conforme Ata da 3ª Reunião Ordinária Conselho de Administração, 30/03/2026.

Em conformidade com o art. 10, inciso IV, do Decreto 12.572/2025, Decreto 11.856/2023, art. 50, § 2º, inciso I, alínea "a" da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), art. 2º, inciso X, da Resolução CGPar n.º 41/2022, bem como as Instruções Normativas - IN nº 1, de 27 de maio de 2020 e a GSI/PR nº 3, de 28 de maio de 2021, o Conselho de Administração da Empresa Brasileira de Correios e Telégrafos subscreve a presente Política Corporativa de Segurança da Informação e Proteção de Dados Pessoais.

1 OBJETIVO

1.1 Estabelecer os princípios, as reponsabilidades e as diretrizes que promovam a segurança da informação e comunicação, por meio da governança e gestão dos ativos de informação, da proteção e privacidade dos dados pessoais (em conformidade com a legislação vigente, diretrizes e normas técnicas pertinentes) e dos valores corporativos, corroborando com a confidencialidade, integridade, disponibilidade, autenticidade da informação e a gestão da continuidade dos serviços de TIC estabelecendo controles internos para minimização de riscos e dos possíveis danos causados pelo impacto de incidentes de segurança.

2 ABRANGÊNCIA

2.1 Esta política e as eventuais normas, metodologias, manuais, processos e procedimentos dela decorrentes aplicam-se, direta ou indiretamente, às instâncias de governança, empregados, visitantes, controladas, coligadas, patrocinadas, suas subsidiárias e os seus parceiros que tenham acesso aos ativos de informação dos Correios.

3 DEFINIÇÕES

3.1 As definições utilizadas nesta política são:

a) ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

b) ativo de informação: patrimônio composto por todos os dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos processos de trabalho dos Correios;

c) autenticidade: propriedade de que a informação foi produzida, expedida, modifica ou destruída por uma determinada pessoa física, ou por um determinado, sistema, órgão ou entidade;

d) confidencialidade: propriedade de que a informação não esteja disponível nem seja revelada a pessoa física, sistema, órgão nem entidade não autorizados nem credenciados;

e) controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear acesso;

f) custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, pela operação, administração e preservação de ativos de informação que não lhe pertencem, mas estão sob sua custódia;

g) *Computer Security Incident Response Time* – CSIRTs: Grupo de Resposta a Incidentes de Segurança, é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. Um CSIRT normalmente presta serviços para uma co-

munidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços para uma comunidade maior, como um país, uma rede de pesquisa ou clientes que pagam por seus serviços;

h) dados pessoais: informação relacionada à pessoa natural identificada ou identificável;

i) disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

j) gestor de segurança da informação: responsável pelas ações de segurança da informação e comunicações no âmbito dos Correios, indicado pela alta administração, na forma definida pela Instrução Normativa nº 3, de 28 de maio de 2021, do Gabinete de Segurança Institucional da Presidência da República;

k) integridade: propriedade de que a informação não foi modificada, suprimida nem destruída de maneira não autorizada;

l) Programa de Privacidade e Segurança da Informação - PPSI: caracteriza-se como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação e tem como valores: a maturidade; a resiliência; a efetividade; a colaboração e a inteligência, instituído por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023, do Ministério da Gestão e da Inovação em Serviços Públicos/Secretaria de Governo Digital;

m) privacidade de dados: entende-se pela possibilidade de cada cidadão determinar de forma autônoma a utilização que é feita de seus próprios dados pessoais, em conjunto com o estabelecimento de uma série de garantias para evitar que esses dados pessoais sejam utilizados de forma a causar discriminação, ou danos de qualquer espécie, ao cidadão ou à coletividade;

n) proprietário do ativo de informação: indivíduo legalmente instituído por sua posição ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

o) risco: efeito da incerteza sobre os objetivos (ISO/IEC 27000); e

p) vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4 PRINCÍPIOS

4.1 Constituem princípios norteadores das atividades tratadas nesta política:

a) proteção da imagem dos Correios;

b) respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a proteção de dados pessoais e a do sigilo postal;

c) manutenção da conformidade legal dos procedimentos relacionados à segurança da informação e privacidade dos dados;

d) observância aos fundamentos de acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade e do não repúdio da informação corporativa;

e) orientação à tomada de decisões institucionais que visem à efetividade das ações de segurança da informação;

f) visão abrangente e sistêmica, proporcionando a articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos de informação;

g) capacitação como alicerce fundamental para o fomento da cultura em segurança da informação e privacidade dos dados pessoais;

h) alinhamento à governança, aos processos e à sustentabilidade do negócio dos Correios;

i) orientação à gestão de riscos e à gestão da segurança da informação;

j) prevenção e tratamento de incidentes cibernéticos;

k) promoção de ampla comunicação envolvendo público interno e partes externas relevantes; e

l) comprometimento da alta administração com a segurança da informação.

5 DIRETRIZES

5.1 Relacionadas com tratamento e classificação da informação, constituem diretrizes desta política:

a) as informações geradas, adquiridas ou custodiadas sob responsabilidade dos Correios são ativos corporativos, protegidos pelos princípios de segurança da informação corporativa, sendo vedado o seu uso não autorizado;

b) o tratamento da informação corporativa e dos dados, físicos ou digitais, deve ser realizado de modo ético e responsável, para propósitos legítimos, específicos, explícitos e informados ao titular, considerando as restrições de acesso e sigilo, observando os normativos legais vigentes, em todo seu ciclo de vida: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

c) realização pelos seus proprietários da classificação da informação corporativa com os respectivos controles, consoante a legislação e normativo corporativo vigentes para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento e a disponibilização pela área de tecnologia da informação de ambientes com o nível de segurança necessário ao seu armazenamento;
d) a proteção das informações deve ser compatível com a sua criticidade nos processos, informatizados ou não;

e) o uso da informação deve ser passível de monitoramento e auditoria, devendo ser implementados e mantidos mecanismos que permitam sua rastreabilidade, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna, bem como a existência de rastro de auditoria (*log*) em sistemas críticos;

f) estabelecimento de processo de gestão de incidentes de segurança da informação e realização de monitoramento contínuo de informação por meio de processos, controles e tecnologias de prevenção e resposta a incidentes de segurança da informação e dados pessoais, com vistas a mitigar a ocorrência do perigo e os impactos decorrentes;

g) análise das ocorrências de tratamento indevido de informações corporativas sob os aspectos legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades;

h) preservação do acervo histórico e documental corporativo dos Correios em concordância com a tabela de temporalidade e legislação vigentes;

i) avaliação periódica do grau de cumprimento da política de segurança da informação pelos atores envolvidos com sua execução, bem como avaliar criticamente a própria política (eficiência, eficácia e efetividade), e devem ser realizados os ajustes que se revelarem necessários; e

j) as informações críticas para a organização (produzidas ou custodiadas) devem ter os riscos de segurança da informação identificados, analisados e avaliados, considerando-se os seguintes aspectos: confidencialidade, integridade e disponibilidade. Outros atributos da informação como autenticidade e confiabilidade também podem ser considerados.

5.2 Relacionadas com segurança física e dos ambientes de TI, constituem diretrizes desta política:

a) restrição de acesso a áreas críticas de TI e garantia de níveis adequados de proteção para cada espaço;

b) identificação e classificação das áreas críticas, como *data centers*, salas de servidores, áreas de *backup* e estações de trabalho sensíveis, com estabelecimento de níveis diferentes de acesso (ex.: público, restrito, altamente restrito);

c) utilização de controle de acesso físico por meio de credenciais (crachás, biometria, cartões magnéticos) e manutenção dos registros de acessos em áreas críticas;

d) adoção de monitoramento e vigilância;

e) proteção contra incêndios, perda de energia e controle de temperatura e humidade;

f) política de descarte seguro de equipamentos e mídias;

g) proteção e fixação de equipamentos críticos;

h) iniciativas de experimentação e validação de solução deverão ser realizadas em ambiente controlado e com a autorização do órgão de TIC;

i) a implementação de ações de segurança da informação corporativa e dos dados deve considerar os objetivos estratégicos, os processos, incluindo os de gestão de riscos de segurança da informação e os controles dele derivados, os requisitos legais e a estrutura dos Correios;

j) observância aos requisitos de segurança da informação corporativa, cibernética e proteção de dados na contratação de serviços ou de pessoas e no relacionamento com empregados, fornecedores, terceiros, parceiros, contratados e estagiários;

k) promoção da cultura de segurança da informação corporativa e privacidade dos dados pessoais, com atenção especial à cibernética, por meio de programa permanente de sensibilização, conscientização e capacitação; e

l) implemento da segurança da informação desde a concepção de projetos de negócio até sistemas informáticos.

5.3 Relacionadas com gestão de incidentes em segurança da informação, constituem diretrizes desta política:

a) emprego de mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens, roubo e ataques cibernéticos, em todo o ciclo de vida das informações e dados;

b) gestão dos incidentes de segurança definindo, estabelecendo e comunicando processos, papéis e responsabilidades;

c) resposta aos incidentes em conformidade aos procedimentos internos documentados;

d) aquisição, identificação e preservação das evidências relacionadas a eventos da segurança da informação, de forma a fortalecer os controles de segurança da informação e buscar a melhoria contínua do processo; e

e) manutenção da segurança da informação em um nível apropriado durante a disrupção.

5.4 Relacionadas com gestão dos ativos de informação, constituem diretrizes desta política:

a) asseguração, por parte da gestão, de que os ativos de informação, tecnológico, físico ou lógico, sejam inventariados e protegidos em todos os ambientes computacionais dos Correios;

b) controle da entrada e da saída dos ativos tecnológicos, de forma que eles só ocorram mediante autorização registrada pelo gestor da unidade competente;

c) disponibilização, sempre que necessária, das informações sobre monitoramento e rastreabilidade do uso do ativo, bem como o custodiante responsável;

d) conscientização de todas as pessoas indicadas a seguirem esta Política de que:

I - os ativos de informação não podem ser utilizados para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins, observando a legislação em vigor; e

II - é vedada aos empregados e colaboradores a instalação de *softwares* ou sistemas não homologados pelo órgão responsável;

e) estabelecimento e implementação de procedimentos de codificação segura;

f) separação e proteção dos ambientes de homologação e produção; e

g) promoção do descarte seguro de equipamentos e mídias e/ou garantia da reutilização de forma a evitar ocorrências de violação de dados com restrição de acesso.

5.5 Relacionadas com gestão do uso dos recursos operacionais e de comunicações (*e-mail*; acesso à *internet*, mídias sociais, computação em nuvem, dentre outros), constituem diretrizes desta política:

a) garantia da configuração de segurança de *hardware*, *software* e redes de forma adequada dentro dos normativos manualizados;

b) controle do acesso de leitura e escrita do código-fonte, ferramentas de desenvolvimento e bibliotecas de *software*;

c) monitoramento e ajuste de acordo com os requisitos de capacidade atual e esperado, o uso dos recursos;

d) definição, manutenção e teste de acordo com normativos, as cópias de *backup* de informações, *software* e sistemas;

e) registro de *logs* das atividades, exceções, falhas e outros que se fizerem necessários, sobretudo em sistemas críticos;

f) monitoramento das atividades de alta criticidade (redes, aplicações e sistemas) quanto a comportamentos anômalos, garantindo a realizações de ações apropriadas para avaliar possíveis incidentes de segurança da informação;

g) restrição e controle rigoroso do uso de programas utilitários que possam ser capazes de se sobrepor a controles de sistemas e aplicações;

h) adoção de procedimentos e medidas para gerenciar a instalação segura de *software* em sistemas operacionais; e

i) aplicação das melhores práticas de privacidade e segurança durante o processo de desenvolvimento de sistemas, bem como atuar na manutenção dos legados de forma que atendam a essa abordagem.

5.6 Relacionadas com controle de acesso, credenciais e perfis dos usuários, constituem diretrizes desta política:

a) garantia de que o controle de acesso, credenciais e perfis dos usuários estejam adequados às atividades desempenhadas e cumpram com os requisitos de segurança e privilégios definidos nos manuais organizacionais, considerando o acesso local e remoto às redes de dados, o acesso aos sistemas, o acesso físico aos equipamentos de TIC, assim como o uso de unidades portáteis de armazenamento de dados e de computadores portáteis;

b) garantia em caso de desligamento ou movimentação dos empregados, que as unidades atendam aos ritos relativos à este processo cumprindo o disposto nos manuais;

c) o acesso remoto aos recursos computacionais deve ser realizado mediante adoção dos mecanismos de segurança definidos pelo órgão responsável a fim de evitar ameaças à integridade e ao sigilo do serviço; e

d) segregação das funções de desenvolvimento e uso dos ativos de informação, na gestão de segurança da informação corporativa e demais áreas gestoras de informação.

5.7 Relacionadas com gestão de riscos de segurança da informação, constituem diretrizes desta política:

a) colaboração com a gestão de riscos de segurança da informação de forma sistemática e contínua, contemplando todos os ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da empresa, a fim de tratar riscos relacionados à disponibilidade, integridade, confidencialidade e autenticidade;

b) avaliação do impacto à proteção dos dados pessoais nos ambientes computacionais e processos de negócio, principalmente quando o tratamento envolver a hipótese legal do legítimo interesse ou envolver dados sensíveis e/ou dados de crianças e adolescente;

c) identificação, análise, avaliação e tratamento dos perigos que envolvem os ativos de informação corporativa, por meio de avaliação periódica e processo estabelecido, documentado e alinhado ao negócio dos Correios;

d) promoção da gestão de riscos como parte integrante da tomada de decisão, integrado a estrutura, operações e processo da organização, que envolva as etapas de escopo, contexto e critérios, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, comunicação e consulta, monitoramento e análise crítica;

e) observação dos princípios da segurança da informação aplicados à cadeia de suprimento;

f) execução, colaboração e manutenção do monitoramento do plano de ação com as estratégias pertinente ao tratamento dos riscos identificados na análise de impacto à proteção dos dados pessoais.

5.8 Relacionadas com gestão da continuidade dos serviços de TIC, constituem diretrizes desta política:

a) direcionamento de esforços, por parte das áreas de segurança da informação e comunicações, infraestrutura e desenvolvimento, na proteção contínua do ambiente computacional e dos dados, garantindo a continuidade do negócio, identificando os riscos relacionados e atuando neles, maximizando o retorno sobre os investimentos e as oportunidades pertinentes;

b) determinação das estratégias e planos de ação que garantam o funcionamento e a disponibilidade mínimos dos serviços críticos da organização;

c) definição de medidas de controle e de recuperação dos ativos de informação e de processos críticos frente a situações de desastres; e

d) garantia a prontidão de TIC de forma planejada, implementada, mantida e testada com base nos objetivos de serviços de TIC e nos requisitos de continuidade de TIC.

5.9 Relacionadas com auditoria e conformidade, constituem diretrizes desta política:

a) planejamento, estabelecimento, implementação e manutenção de programa de auditoria dos serviços de TIC, com existência de rastro de auditoria (*log*) em sistemas críticos, frequência, métodos, responsabilidade, requisitos de planejamento e relato;

b) proteção dos sistemas de informação por meio de testes de auditoria planejados; e

c) asseguramento de que o sistema de gestão da segurança da informação esteja em conformidade como os requisitos legais e institucionais.

5.10 Relacionadas ao atendimento de clientes e cidadãos, de forma presencial, digital ou por meio de ligações telefônicas, constituem diretrizes desta política:

a) alinhamento com as melhores práticas definidas nos normativos internos quanto à privacidade de dados pessoais e tratamento de informações com restrição de acesso por sigilos determinados em conformidade com a legislação vigente; e

b) aplicação e colaboração com as estratégias de segurança de dados dos clientes, atuando com base nos processos internos de forma a prevenir qualquer tipo de violação de dados.

5.11 Relacionadas com a aquisição de novo produtos e serviços ou parcerias efetivadas, constituem diretrizes desta política:

a) comprovação, por parte dos prestadores de serviços e parceiros dos Correios, da conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD, evidenciando, no mínimo a aplicação dos requisitos de segurança e privacidade já implementados nos Correios;

b) inclusão, em contratos, convênios e instrumentos congêneres, de cláusulas referentes à segurança da informação e privacidade, essa última, caso haja tratamento de dados pessoais; e

c) inclusão nos projetos básicos, de requisitos de segurança da informação e privacidade aderentes ao ambiente computacional dos Correios e normativos internos.

5.12 Relacionadas ao Compliance, constituem diretrizes desta política:

a) atenção aos requisitos e dispositivos afetos à segurança da informação dispostos na legislação e normativos aplicáveis, tais como: Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei nº 12.527/2011 (Lei de Acesso à Informação), Decreto nº 12.572/2025 (Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal), Decreto nº 11.856/2023 (Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança) e Resolução CGPar/ME nº 41/2022;

b) atenção as orientações contidas nas Instruções Normativas do Governo Federal, envidando os melhores esforços para emprega-las; e

c) envidamento dos melhores esforços para garantir a conformidade aos padrões éticos e regulamentos internos e externos.

5.13 Relacionadas ao Programa de Privacidade e Segurança da Informação – PPSI, constituem diretrizes desta política:

a) atuação na segurança dos ativos de informação corporativa tendo como base o Programa de Privacidade e Segurança da Informação - PPSI;

b) observação para cada um dos processos que compõem o PPSI, a pertinência de elaboração de normas e procedimentos de forma a disciplinar seu entendimento;

c) planejamento da proteção de ativos de informação e prevenção de incidentes e crimes: realizar o mapeamento de ativos de informação, considerando preliminarmente os objetivos estratégicos da organização, seus processos internos, requisitos legais e estrutura do órgão ou entidade, bem como as interfaces e interdependências entre eles. Deve-se também identificar e avaliar suas ameaças, vulnerabilidades e proprietário, bem como classificar ativos de informação, e modelar os critérios e métodos de prevenção e proteção desses;

d) mitigação das vulnerabilidades dos ativos de informação: promover a gestão de riscos de segurança da informação, por meio de um plano de gestão de riscos, de forma a conceber produtos, serviços e *softwares* considerando a proteção dos ativos de informação e, em especial, dos dados pessoais, prevenir incidentes e crimes contra os ativos de informação e proteger os dados pessoais;

e) redução dos impactos: promover a gestão de continuidade, por meio da definição de planos de contingência e de continuidade para incidentes e crimes contra os ativos de informação, utilizar canal único para registro de denúncias de incidentes e de crimes relacionados à segurança da informação e apurar incidentes e crimes relacionados à segurança da informação;

f) implementação do processo de gestão de mudanças: preparar e adaptar os órgãos para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências; e

g) avaliação da conformidade nos aspectos de segurança da informação e proteção de dados: proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento aos princípios legais e de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

6 RESPONSABILIDADES

6.1 Constitui responsabilidade do Conselho de Administração – CA: aprovar a política de segurança de informação e proteção de dados.

6.2 Constituem responsabilidades do gestor de segurança da informação:

a) coordenar o Comitê de Gestão de Segurança da Informação e Comunicação – COGSI ou estrutura equivalente;

b) coordenar a elaboração da Política Corporativa de Segurança da Informação e Proteção de Dados dos Correios - POSIC e das normas internas de segurança da informação, observadas as normas afins aplicáveis aos Correios;

c) assessorar a alta administração na implementação da Política Corporativa de Segurança da Informação e Proteção de Dados Pessoais;

d) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

e) promover a divulgação da política e das normas internas de segurança da informação a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

f) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

g) propor recursos necessários às ações de segurança da informação;

h) acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

i) verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

j) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

k) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

6.3 Constituem responsabilidades do Comitê de Gestão de Segurança da Informação e Comunicação – COGSI Correios:

a) propor a definição de políticas, diretrizes, normas e procedimentos gerais relacionados à segurança da informação e comunicação;

b) apoiar na implantação de soluções de tecnologia de informação e comunicação para eliminação ou minimização dos riscos empresariais;

c) propor a instituição de grupos de trabalho para tratar de temas específicos relacionados à segurança da informação e comunicações;

d) promover, por meio das áreas competentes, a cultura de segurança da informação e comunicação;

e) propor programa orçamentário específico para as ações de segurança da informação e comunicação, anualmente, se necessário;

f) propor e emitir parecer quanto aos recursos necessários às ações de segurança da informação e comunicação;

g) conhecer o resultado dos processos de auditoria de gestão da segurança da informação e comunicações e acompanhar o desenvolvimento de suas recomendações;

h) conhecer os resultados das investigações e das avaliações dos danos decorrentes de quebras de segurança da informação e comunicação e acompanhar o desenvolvimento das suas recomendações;

i) propor o aprimoramento das normas da Empresa visando a sua atualização quanto às responsabilidades individuais, no que tange a segurança da informação e comunicação;

j) assessorar na implementação das ações de segurança da informação e comunicações; e

k) acompanhar a implementação de medidas relacionadas à prevenção de fraudes e à gestão da segurança da informação e comunicação; e

l) assessorar e propor ao Conselho de Administração sugestões afetas aos temas e recomendações do Comitê Permanente de Avaliação de Documentos - COPAD e do gestor corporativo de segurança da informação (segurança empresarial) referentes à avaliação de documentos sigilosos, e principalmente sobre a política de segurança e confidencialidade da informação corporativa nos Correios.

6.4 Constituem responsabilidades da Equipe de Tratamento, Prevenção e Resposta a Incidentes de Rede dos Correios – ETIR Correios:

a) criar e manter canais específicos de comunicação com as demais CSIRTs e com os órgãos internos dos Correios;

b) receber, classificar, orientar aos envolvidos e responder às solicitações e alertas, provenientes de canais específicos;

c) receber informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, seu mecanismo e suas consequências e desenvolver estratégias para detecção e mitigação;

d) receber informações ou cópia de artefato malicioso, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, caso necessário, o artefato poderá ser encaminhado para os órgãos responsáveis para providências cabíveis;

e) coordenar a execução de ações visando mitigar e prevenir incidentes de cibersegurança e de privacidade de dados;

f) deliberar sobre ações a serem tomadas pela área de tecnologia com intuito de mitigar, remediar, prevenir e tratar incidentes relacionados à cibersegurança; e

g) atuar, nas atividades de tratamento de dados pessoais, observando a boa fé e os princípios prescritos na Lei Geral de Proteção de Dados Pessoais - LGPD.

6.5 Constituem responsabilidades dos dirigentes, empregados, usuários, prestadores de serviço, contratados e terceirizados:

a) zelar pela observância e cumprimento da POSIC e dos atos e ações decorrentes da sua implementação;

b) atuar como agentes ativos, comprometidos com a segurança das informações corporativas;

c) em caso de dúvidas relacionadas à segurança das informações corporativas e/ou privacidade dos dados pessoais, buscar orientação do superior hierárquico imediato, acessar os manuais e políticas ou entrar em contato diretamente com a área responsável pelo tema;

d) dar o tratamento adequado ao ativo de informação, de acordo com a sensibilidade dos dados, aplicando a classificação (pública, restrita ou sigilosa) sempre que a ferramenta, aplicação ou sistema oferecer tal funcionalidade;

e) participar de ações de capacitação e iniciativas relacionadas à segurança de informação promovidas ou divulgadas;

f) comunicar formalmente e tempestivamente à Equipe de Tratamento, Prevenção e Resposta a Incidentes de Rede dos Correios – ETIR Correios qualquer incidente ou ameaça à segurança da informação e proteção de dados de que tiver ciência;

g) comunicar ao Comitê de Gestão de Segurança da Informação e Comunicação - COGSI qualquer descumprimento ou violação desta Política ou demais normativos correlatos;

h) promover adequadamente o tratamento de dados pessoais em conformidade com a LGPD;

i) primar pelo correto uso e confidencialidade de suas senhas; e

j) participar de cursos sobre segurança da informação.

7 DISPOSIÇÕES GERAIS

7.1 A POSIC, quando necessário, deve ser complementada por manuais, metodologias e procedimentos.

7.2 Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelos Correios devem observar o contido na POSIC e nos atos decorrentes da sua implementação.

7.3 Os casos e as ações que violem a POSIC ou quebra de segurança das normas, procedimento e/ou processos, poderão acarretar, isoladamente ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais.

7.4 A periodicidade para a revisão desta POSIC é de no máximo 4 (quatro) anos.

7.5 As diretrizes da POSIC não são excludentes e podem ser complementadas por outras políticas institucionais, como: Política de Segurança Corporativa, Política de Governança e Gestão de Dados, Política de Auditoria Interna dos Correios, Política de Gestão de Riscos, Política de Governança Corporativa, entre outras.

8 REFERÊNCIAS

8.1 Fundamentação legal e normativa que orienta esta política:

a) Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI);

b) Lei nº 13.303, de 30 de junho de 2016;

c) Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

d) Decreto nº 8.945, de 27 de dezembro de 2016;

e) Decreto nº 12.572, de 4 de agosto de 2025;

f) Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

g) Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021;

h) Resolução CGPar nº 41, de 4 de agosto de 2022;

i) Portaria MCTIC nº 4.711, de 18 de agosto de 2017;

j) Estatuto Social dos Correios;

k) ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos;

l) ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação;

m) ABNT NBR ISO/IEC 27003:2020: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações; e

n) ABNT NBR ISO/IEC 27701:2020: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.