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

Aprovações:

1. Ata da 5ª Reunião Ordinária COGSI, 30/06/2022, versão 2.
2. Ata da 2ª Reunião Ordinária do COETI 2022, 11/10/2022, versão 2.
3. Ata da 38ª Reunião Ordinária de Diretoria, 01/12/2022, versão 2.
4. Ata da 23ª Reunião Ordinária do Comitê de Auditoria, 09/12/2022, versão 2.
5. Ata da 12ª Reunião Ordinária Conselho de Administração, 13/12/2022, versão 2.

Em conformidade com os artigos art. 15, inciso II, do Decreto 9.637/2018, 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 A presente Política Corporativa de Segurança da Informação e Proteção dos Dados Pessoais – POSIC tem como objetivo definir os princípios, diretrizes e responsabilidades relativas à governança e gestão da segurança da informação corporativa, proteção e privacidade dos dados pessoais em conformidade com a legislação vigente, as normas técnicas pertinentes, os valores corporativos e as melhores práticas, visando manter a disponibilidade, a integridade, a confidencialidade, a autenticidade, a legalidade, a privacidade, a auditabilidade e o não repúdio da informação corporativa.

2 ABRANGÊNCIA

2.1 Esta política e as eventuais normas, metodologias, manuais e procedimentos dela decorrentes aplicam-se, direta ou indiretamente, aos 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: qualquer elemento (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

c) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

d) curador de dados: os curadores (data stewards, em inglês) são as pessoas ou grupos de pessoas que têm responsabilidades de cuidar dos dados sob sua alçada de negócio. Ele compartilha com a TIC a missão de cuidar dos dados corporativos;

e) curadoria da informação: estrutura responsável por definir e manter as informações sobre dados (metadados) e manter a conformidade com a legislação e normativo vigentes e primar pela qualidade dos dados. A curadoria é composta por curadores estratégicos e curadores de negócio;

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

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

h) gestor de segurança da informação: responsável pelas ações de segurança da informação e comunicações no âmbito dos Correios na forma definhada pela Instrução Normativa nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República. Coordena o COGSI e a equipe de tratamento e resposta a incidentes em redes computacionais. Promove as ações de segurança da informação e proteção de dados pessoais na forma definida pela LGPD. Mantém contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC) para o trato de assuntos relativos à segurança da informação e comunicações;

i) metadados: são dados sobre outros dados. Um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador;

j) 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 estes dados pessoais sejam utilizados de forma a causar discriminação, ou danos de qualquer espécie, ao cidadão ou à coletividade;

k) 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;

l) titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

m) 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.

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, 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) identificação e definição dos responsáveis pelas curadoria da informação e dos dados, em nível estratégico e de negócio, de acordo com normativo corporativo vigente;

d) realização da classificação da informação corporativa pelos seus proprietários 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 proteção das informações deve ser compatível com a sua criticidade nos processos, informatizados ou não;

f) 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;

g) 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;

h) 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;

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

5.2 Relacionadas com gestão da segurança da informação e proteção dos dados pessoais, constituem diretrizes desta política:

a) a segurança da informação e comunicações tem como principal orientação a proteção da informação e dados, garantindo a continuidade do negócio, direcionando e controlando os riscos relacionados, de forma a minimiza-los, maximizando o retorno sobre os investimentos e as oportunidades pertinentes;

b) é vedado aos empregados e colaboradores a instalação de *software*s ou sistemas não homologados pelo órgão responsável;

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

d) 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) a implementação de ações de segurança da informação corporativa e dos dados deve considerar os objetivos estratégicos, processos, requisitos legais e a estrutura dos Correios;

f) 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;

g) 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;

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

i) promoção de 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.

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

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

b) a entrada e saída dos ativos tecnológicos devem ocorrer mediante a 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) 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.

5.4 Relacionadas com gestão de continuidade de negócios, constituem diretrizes desta política:

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

b) definir medidas de controle e de recuperação dos ativos de informação e de processos críticos frente a situações de desastres.

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

a) corroborar com a gestão de riscos de segurança da informação de forma sistemática e contínua, contemplando todos os ativos de informação a fim de tratar riscos relacionados à disponibilidade, integridade, confidencialidade e autenticidade;

b) avaliar o impacto à proteção dos dados pessoais nos ambientes computacionais;

c) identificar, analisar, avaliar e tratar os perigos que envolvem os ativos de informação corporativa, por meio de avaliação periódica e processo estabelecido, documentado e alinhado ao negócio dos Correios.

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

a) garantir 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;

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

6 RESPONSABILIDADES

6.1 Constituem responsabilidades do Conselho de Administração – CA:

a) aprovar a POSIC, assim como suas revisões (Estatuto Social dos Correios aprovado na 19a Assembleia Geral Extraordinária, de 24/11/2020, Art. 50, inciso XII);

b) validar programa orçamentário específico para as ações de segurança da informação e comunicações e para proteção de dados (Estatuto Social dos Correios aprovado na 19ª Assembleia Geral Extraordinária, de 24/11/2020, Art. 50, inciso XIII).

6.2 Constituem responsabilidades da Diretoria Executiva dos Correios – DIREX:

a) aprovar as políticas e diretrizes de segurança de informação e proteção de dados e garantir seu cumprimento (Estatuto Social dos Correios aprovado na 19a Assembleia Geral Extraordinária, de 24/11/2020, Art. 67, inciso XVIII);

b) acompanhar o gerenciamento da segurança da informação corporativa e de proteção de dados (Estatuto Social dos Correios aprovado na 19ª Assembleia Geral Extraordinária, de 24/11/2020, Art. 67, inciso I);

c) designar o Gestor de Segurança da Informação e Comunicações (Decreto 9.637/2018, Art. 15, inciso III).

6.3 Constituem responsabilidades do gestor de segurança da informação:

a) coordenar a gestão de riscos de segurança da informação;

b) designar o agente responsável pela gestão de riscos de segurança da informação, dentre os empregados efetivos do órgão;

c) aprovar o plano de gestão de riscos de segurança da informação;

d) aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;

e) aprovar o relatório de tratamento de riscos de segurança da informação;

f) propor medidas preventivas à alta administração;

g) o gestor de segurança da informação coordenará o processo de gestão de continuidade de negócios em segurança da informação nos seus respectivos órgãos ou entidades, bem como designará um agente responsável pela referida gestão, dentre os servidores efetivos do órgão;

h) cabe ao gestor de segurança da informação, com relação ao processo de gestão de mudanças nos aspectos de segurança da informação: (i) coordenar a gestão de mudanças; (ii) designar o agente responsável pela gestão de mudança, dentre os servidores efetivos do órgão; (iii) analisar e encaminhar o documento de avaliação e aprovação de mudança para apreciação da alta administração do órgão, à qual cabe a decisão de aprovar ou indeferir a mudança; e (iv) proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação;

i) cabe ao gestor de segurança da informação, com relação à avaliação de conformidade nos aspectos de segurança da informação: (i) coordenar a avaliação de conformidade nos aspectos relativos à segurança da informação; (ii) designar, dentre os servidores efetivos do órgão, um ou mais agentes responsáveis pela avaliação de conformidade, de acordo com os aspectos relativos à segurança da informação, não podendo ser nenhum dos membros da equipe de gestão de segurança da informação do órgão ou da entidade; (iii) fornecer, ao(s) agente(s) responsável(is) pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação; (iv) analisar o relatório de avaliação de conformidade e encaminhá-lo para apreciação e aprovação da alta administração; e (v) adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração.

6.4 Constituem responsabilidades do agente responsável pela gestão de riscos de segurança da informação:

a) elaborar o plano de gestão de riscos de segurança da informação;

b) elaborar o relatório de identificação, análise e avaliação dos riscos de segurança da informação;

c) elaborar o relatório de tratamento de riscos de segurança da informação.

6.5 Constituem responsabilidades do agente responsável pela gestão de continuidade de negócios em segurança da informação:

a) assessorar os responsáveis pelo processo ou os titulares das unidades em que forem identificadas atividades críticas;

b) avaliar o plano de continuidade de negócios em segurança da informação e propor mudanças, quando aplicável;

c) supervisionar a implementação, os testes de funcionamento e a atualização desse plano;

d) propor melhorias na implementação de novos controles relativos ao plano de continuidade de negócios em segurança da informação;

e) participar da elaboração da análise de impacto nos negócios;

f) propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação.

6.6 Constituem responsabilidades do Agente responsável pela gestão de mudança nos aspectos de segurança da informação:

a) recomendar à alta administração a instituição de um grupo técnico de mudança, composto por empregados das áreas afetadas e da área de segurança da informação para a elaboração do documento de avaliação e aprovação de mudança;

b) elaborar, juntamente com o grupo técnico de mudança, o documento de avaliação e aprovação de mudança e submetê-lo à análise do gestor de segurança da informação;

c) acompanhar, juntamente com o grupo técnico de mudança, os testes da mudança aprovada pelo documento de avaliação e aprovação de mudança;

d) acompanhar, juntamente com o grupo técnico de mudança, a implementação da solução aprovada no documento de avaliação e aprovação de mudança;

e) assegurar, juntamente com o grupo técnico de mudança, registro de auditoria contendo todas as informações relevantes relacionadas com a mudança;

f) informar ao gestor de segurança da informação sobre o andamento e a conclusão do processo.

6.7 Constituem responsabilidades do agente responsável pela avaliação de conformidade:

a) elaborar o plano de verificação de conformidade.

b) elaborar o relatório de avaliação de conformidade e remetê-lo à alta administração do órgão.

c) verificar a adequação dos procedimentos de segurança da informação de acordo com as recomendações descritas no relatório de avaliação de conformidade.

6.8 Constituem responsabilidades do Encarregado de Dados:

a) tratar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) promover a cultura de proteção e privacidade de dados pessoais;

d) fornecer orientação, liderar e gerenciar, conforme necessário, os aspectos de design, desenvolvimento, implementação, documentação e manutenção de políticas, procedimentos e padrões de segurança da informação em todos os departamentos e funções da empresa;

e) analisar os relatórios sobre incidentes de segurança e violações de dados;

f) fomentar as ações de proteção de dados;

g) monitorar a conformidade dos procedimentos de proteção de dados;

h) definir o programa e padrões de proteção de dados;

i) executar as demais atribuições determinadas pelo COGSI ou estabelecidas em normas complementares;

j) comunicar ao COGSI as violações de proteção e privacidade de dados existentes ou potenciais.

6.9 Constituem responsabilidades do proprietário do ativo de informação:

a) assegurar que os ativos de informação sob sua propriedade, ao longo do seu ciclo de vida, sejam tratados consoante os princípios e as diretrizes de segurança da informação corporativa previstos nesta política e na legislação vigente;

b) definir o gestor e custodiante do ativo de informação;

c) definir o curador de dados de sua área de atuação;

d) patrocinar as iniciativas de segurança da informação corporativa de forma a disponibilizar os recursos necessários;

e) atuar como instância superior, no âmbito de segurança da informação corporativa, na tomada de decisões que extrapolem a autoridade do gestor da informação;

f) aprovar a classificação dos ativos de informação sob sua propriedade;

g) aprovar as regras específicas e procedimentos operacionais de segurança da informação no seu âmbito de atuação;

h) comunicar a ocorrência ou evidência de incidentes de segurança da informação corporativa que possam afetar criticamente os Correios.

6.10 Constituem responsabilidades do curador estratégico:

a) indicar curadores de negócio para atuarem na gestão dos ativos de informação de sua área de atuação;

b) fazer a gestão da curadoria da sua área de atuação;

c) realizar a identificação dos ativos de informação conforme diretrizes estabelecidas;

d) classificar os ativos de informação, observados os dispositivos legais e regimentais relativos à confidencialidade e a outros critérios de classificação pertinentes;

e) propor normativo e procedimentos operacionais de segurança da informação no seu âmbito de atuação;

f) propor regras específicas para o uso dos ativos de informação corporativas;

g) definir os requisitos de segurança da informação necessários ao negócio, com base em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho;

h) realizar análise de impacto de privacidade nos ativos de informações de sua área de atuação;

i) gerenciar os metadados dos ativos de informação (pessoais, não pessoais, digitais e não digitais de sua área de atuação.

6.11 Constituem responsabilidades do curador de dados:

a) realizar e manter os metadados dos ativos de informação (pessoais, não pessoais, digitais e não digitais) da sua área de atuação, consoante legislação e normativo corporativo vigentes;

b) administrar o fluxo dos dados com foco, também, na privacidade e proteção dos dados;

c) documentar regras e padrões de dados a serem disponibilizados;

d) gerenciar a qualidade de dados;

e) definir processos em torno dos dados;

f) manter a documentação dos dados;

g) executar atividades operacionais de governança de dados estabelecidas corporativamente.

6.12 Constituem responsabilidades do custodiante do ativo de informação:

a) garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo proprietário ou curador do ativo de informação;

b) Comunicar tempestivamente ao proprietário e curador da informação sobre situações que comprometam a segurança das informações sob custódia;

c) Comunicar ao proprietário e curador da informação eventuais limitações para o cumprimento dos critérios por ele definidos com vistas à proteção da informação.

6.12 Constituem responsabilidades de 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) buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das informações corporativas.

d) dar o tratamento adequado ao ativo de informação consoante classificação recebida.

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

f) comunicar formalmente à Equipe de Tratamento de Incidentes de Rede – 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 - COGSI qualquer descumprimento ou violação desta Política ou demais normativos correlatos.

7 DISPOSIÇÕES GERAIS

7.1 O Sistema de Gestão de Segurança da Informação Corporativa e de Proteção de Dados - SGSI é a parte do sistema de Governança dos Correios, baseado na abordagem de segurança e proteção do negócio no tratamento dos ativos de informação. Assegura que os ativos de informação corporativa são adequadamente protegidos.

7.2 O SGSI adotado pelos Correios é composto pelos seguintes processos:

a) planejar a proteção de ativos de informação e prevenir 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;

b) mitigar 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;

c) reduzir 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;

d) implementar 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

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

7.2.1 Para cada um dos processos que compõem o SGSI/Correios deve ser observada a pertinência de elaboração de normas e procedimentos de forma a disciplinar seu entendimento.

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

7.4 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.

7.5 Os casos de violação da Política Corporativa de Segurança da Informação e Proteção dos Dados Pessoais ou da quebra de segurança e proteção de dados, ocorrerão de acordo com as normas existentes no ordenamento jurídico vigente sobre penalidades ao agente público federal relativas ao assunto.

7.6 A periodicidade para a revisão desta Política Corporativa de Segurança da Informação e Proteção dos Dados Pessoais é de no máximo 4 (quatro) anos.

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 9.637, de 26 de dezembro de 2018 - Política Nacional de Segurança Nacional.

f) Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

g) Resolução CGPAR nº 41, de 04 de agosto de 2022.

h) Portaria MCTIC nº 4.711, de 18.08.2017.

i) Estatuto Social dos Correios aprovado na 19ª Assembleia Geral Extraordinária, de 24/11/2020.

j) NBR ISO/IEC 27001:2013: sistemas de gestão de segurança da informação.

k) NBR ISO/IEC 27002:2007: código de prática para a gestão da segurança da informação.