Política Corporativa de Segurança da Informação e de Proteção de Dados Pessoais (POSIC)

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 Organização da Informação de Negócio (GOIN/DEARP)		
Aprovações:	Documento de Aprovação	Data de Aprovação	Versão
	2ª Reunião Ordinária do COETI 2021	14/06/2021	
	3ª Reunião Ordinária COGSI	30/06/2020	
	13ª Reunião Ordinária de Diretoria	30/06/2021	
	17ª Reunião Ordinária do Comitê de Auditoria	02/07/2021	
	7ª Reunião Ordinária Conselho de Administração	29/07/2021	

Em conformidade com o art. 2º, inciso X, da Resolução GCPAR n.º 11/2016, bem como do art. 15, inciso II, do Decreto 9.637/2018 e com o art. 50, § 2º, inciso I, alínea "a" da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), o Conselho de Administração da Empresa Brasileira de Correios e Telégrafos subscreve a presente Política Corporativa de Segurança da Informação e de Proteção de Dados Pessoais.

1. Objetivo

1.1.A presente Política Corporativa de Segurança da Informação e de Proteção de Dados Pessoais – POSIC tem como objetivo definir os princípios, diretrizes e responsabilidades relativas ao uso e compartilhamento de informação corporativa em conformidade com a legislação vigente, as normas técnicas pertinentes, os valores corporativos e as melhores práticas de segurança da informação e comunicações, bem como de proteção de dados, com vistas a:

a) assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações corporativas;

b) minimizar riscos inerentes ao ciclo de vida da informação;

c) garantir a eficácia dos processos da cadeia de valor;

d) preservar a imagem dos Correios; e

e) controlar e proteger os dados pessoais, produzidos, adquiridos, custodiados e processados pelos Correios, observando as responsabilidades do controlador e do operador de dados previstos na Lei 13.709/2018.

2. Abrangência

2.1. Esta política e as eventuais normas, metodologias, manuais e procedimentos decorrentes aplicam-se aos que, direta ou indiretamente, realizam tratamento de informação nos Correios, incluindo as suas controladas, coligadas, patrocinadas, suas subsidiárias, os seus parceiros e, quando pertinente, os contratados.

3. Definições

3.1. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

3.2. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

3.3. 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.

3.4. 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.

3.5. Dados pessoais: informação relacionada à pessoa natural identificada ou identificável.

3.6. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

3.7. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

3.8. 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.

3.9. Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação da informação, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

3.10. Gestor de Segurança da Informação e Comunicações: 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.

3.11. Gestor de Governança e Segurança da Informação: responsável pelas ações de segurança da informação e comunicações em segundo nível no âmbito dos Correios.

3.12. 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.

3.13. 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.

3.14. 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.

3.15. Segurança da Informação Corporativa: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações corporativas.

3.16. Tratamento da informação: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3.17. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

3.18. 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. Respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a proteção de dados pessoais e a do sigilo postal.

4.2. 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.

4.3. Alinhamento à Governança, aos processos e à sustentabilidade do negócio dos Correios.

5. Diretrizes

5.1. A segurança da informação e comunicações tem como principal orientação a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

5.2. Considerar os objetivos estratégicos, processos, requisitos legais e a estrutura dos Correios para implementação de ações de segurança da informação corporativa.

5.3. As informações geradas, adquiridas ou custodiadas sob responsabilidade dos Correios são ativos corporativos, protegidos pelos princípios de Segurança da Informação Corporativa, sendo vedado seu uso não autorizado.

5.4. Tratamento da informação corporativa de modo ético e responsável em todo seu ciclo de vida: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.

5.5. Classificação da informação corporativa, consoante legislação e normativo corporativo vigentes para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento.

5.6. Proteção aos ativos de informação de forma compatível com sua criticidade nos processos, informatizados ou não, inclusive quando do uso de computação em nuvem.

5.7. 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.

5.8. 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.

5.9. Monitoramento contínuo dos ativos de informação por meio de processos, controles e tecnologias de prevenção e resposta a incidentes de segurança da informação, com vistas a mitigar a ocorrência do perigo e os impactos decorrentes.

5.10. Segregação das funções de desenvolvimento e uso dos ativos de informação, na gestão de segurança da informação corporativa e demais áreas gestoras de informação.

5.11. Definição do gestor de segurança da informação e comunicação dos Correios.

5.12. Identificação e definição do proprietário da informação com responsabilidades sobre a informação em todo o seu ciclo de vida.

5.13. Promoção de cultura de segurança da informação corporativa, com atenção especial à cibernética, por meio de programa permanente de sensibilização, conscientização e capacitação.

5.14. Observância aos requisitos de segurança da informação corporativa e cibernética na contratação de serviços ou de pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários.

5.15. Concessão de acesso, a funcionários e terceiros, somente às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal.

5.16. Identificação de forma clara e inequívoca, por meio do controle de acesso, do usuário do ativo de informação.

5.17. 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.

5.18. Preservação do acervo histórico e documental corporativo dos Correios, consoante tabela de temporalidade e legislação vigentes.

5.19. Proteção da privacidade de dados de maneira a garantir a segurança adequada dos dados pessoais, incluindo proteção contra violações inerentes, usando medidas técnicas ou organizacionais apropriadas guardando alinhamento com a legislação de proteção de dados aplicável (em particular, a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, "LGPD") notadamente quanto aos seus princípios e bases legais.

5.20. Respeito aos direitos do titular dos dados pessoais.

5.21. Os Correios podem realizar o tratamento de dados, observando os requisitos legais, em especial para as informações pessoais, para atendimento dos objetivos institucionais.

6. Sistema de Gestão de Segurança da Informação Corporativa e de Proteção de Dados

6.1. 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.

6.2. O SGSI adotado pelos Correios é composto pela POSIC e pelos processos a seguir:

a) planejar a proteção de ativos de informação e prevenir incidentes e crimes: deve-se identificar ativos de informação, suas ameaças, vulnerabilidades e proprietário, classificar ativos de informação, avaliar vulnerabilidades dos ativos de informação e modelar os critérios e métodos de prevenção e proteção dos ativos de informação.

b) mitigar vulnerabilidades dos ativos de informação: 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: definir 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.

Nota: para cada um dos processos que compõem o SGSI/Correios deve ser observada a pertinência de elaboração de instruções normativas e procedimentos de forma a disciplinar seu entendimento.

7. Responsabilidades

7.1. 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).

7.2. Diretoria Executiva dos Correios (DIREX):

a) aprovar as diretrizes de segurança de informação e proteção de 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).

7.3. 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; e,

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

7.4. 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; e

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

7.5. Gestor do Ativo de Informação:

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

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

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

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

e) 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.

7.6. 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; e

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

7.7. Curador de Dados:

a) gerenciar os metadados;

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.

7.8. Empregados, usuários, prestadores de serviço, contratados e terceirizados:

a) cumprir as políticas, as instruções normativas, os procedimentos e as orientações de segurança da informação dos Correios;

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) comunicar ao Comitê de Gestão de Segurança da Informação (COGSI) qualquer descumprimento ou violação desta Política ou demais normativos correlatos.

8. Penalidades

8.1. Os casos de violação da Política de Segurança da Informação ou de quebra de segurança, ocorrerão de acordo com as normas existentes no ordenamento jurídico vigente sobre penalidades ao agente público federal relativas ao assunto.

9. Revisão

9.1. A periodicidade para a revisão desta Política de Segurança da Informação é de no máximo 4 (quatro) anos.

10. Referências

10.1. Decreto nº 8.945, de 27 de dezembro de 2016;

10.2. Decreto nº 9.637, de 26 de dezembro de 2018 - Política Nacional de Segurança Nacional;

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

10.4. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

10.5. Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI);

10.6. Lei nº 13.303, de 30 de junho de 2016;

10.7. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados pessoais (LGPD);

10.8. NBR ISO/IEC 27001:2013: sistemas de gestão de segurança da informação;

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

10.10. Portaria GSI/PR nº 93, de 26 de setembro de 2019;

10.11. Portaria MCTIC nº 4.711, de 18.08.2017;

10.12. Resolução CGPAR nº 11, de 10 de maio de 2016.