Política Corporativa de Gestão de Riscos



SUMÁRIO

Identificação Geral ..... pág. 3
1. Objetivo ..... pág. 4
2. Abrangência ..... pág. 4
3. Definições ..... pág. 4
4. Princípios ..... pág. 6
5. Diretrizes ..... pág. 7
6. Responsabilidades ..... pág. 7
7. Disposições Gerais ..... pág. 10
8. Referências ..... pág. 11

IDENTIFICAÇÃO GERAL

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

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

Empresa Pública de Capital Fechado

Elaboração: Departamento de Compliance e Riscos – DECRI/DIGOE

Aprovações:

1. Ata da 5ª Reunião Ordinária do Conselho de Administração, de 31/05/2017, 1ª versão
2. Ata da 4ª Reunião Ordinária do Conselho de Administração, de 27/04/2022, 2ª versão
3. Ata da 12ª Reunião Ordinária do Conselho de Administração, de 18/12/2024, 3ª versão

Documento é público

Em conformidade com o inciso I do art. 23 da Resolução nº 48/2023 da Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União - CGPAR, o Conselho de Administração dos Correios subscreve a presente Política Corporativa de Gestão de Riscos.

1 OBJETIVO

1.1 Estabelecer princípios, diretrizes e responsabilidades que devem nortear a gestão e a governança de riscos nos Correios, visando subsidiar a tomada de decisão e o tratamento adequado dos riscos, respeitando os aspectos regulatórios e as necessidades das partes interessadas, reduzindo os riscos a níveis aceitáveis, fortalecendo a governança corporativa e aumentando a probabilidade do cumprimento e consecução da missão, visão e dos objetivos institucionais.

2 ABRANGÊNCIA

2.1 Esta Política aplica-se a toda a estrutura de governança dos Correios, gestores, empregados e as suas relações com as partes interessadas.

3 DEFINIÇÕES

3.1. As definições utilizadas nesta Política são:

a) alta administração: composta pelos membros do Conselho de Administração e da Diretoria Executiva;

b) analista de riscos: profissional que atua no órgão corporativo de gestão de riscos;

c) apetite a risco: os tipos e o nível de risco, de forma abrangente, que uma organização está disposta a aceitar na busca de valor;

d) categoria de riscos: classificação dos tipos de riscos definidos pelos Correios que podem afetar o alcance dos objetivos organizacionais, observadas as características e particularidades que representam o risco;

e) disrupção: incidente, antecipado ou previsto, que resulta em desvios negativos e não planejados na entrega esperada de produtos e serviços de acordo com os objetivos da organização;

f) gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

g) gestor de risco: profissional designado pelo proprietário do risco. Pode ser gestor de processos, projetos e/ou área de atuação;

h) limite de exposição a riscos: determina os níveis de riscos aceitáveis pela organização para realização de sua estratégia e/ou execução de seus processos;

i) método de gerenciamento de riscos: conjunto estruturado de procedimentos e práticas utilizadas que compreende as etapas de estabelecimento de contexto, identificação, análise, avaliação, tratamento e monitoramento/comunicação de riscos associados aos diversos contextos, tais como: processos, projetos, contextos decisórios, produtos e serviços, estratégia Correios, entre outros;

j) modelo de governança de riscos: estabelece o monitoramento como uma atividade contínua, contemplando os aspectos relacionados aos papéis e responsabilidades de todos os envolvidos, assim como a supervisão dos riscos. As reuniões periódicas facilitam o reporte de informações relevantes de

maneira hierárquica ascendente, enquanto as decisões são disseminadas de forma descendente, garantindo uma gestão de riscos eficaz e coordenada em todos os níveis da organização;

k) nível de risco: magnitude de um risco expressa em termos de combinação dos seus impactos e de suas probabilidades;

l) partes interessadas (*stakeholders*): pessoas físicas ou jurídicas, grupos de pessoas ou órgãos públicos ou entidades privadas que podem afetar, ser afetados ou se sentirem afetados por uma decisão ou atividade da Empresa. Principais partes interessadas: empregados, clientes, fornecedores, credores, parceiros, governo e sociedade;

m) planos de continuidade de negócios: informação documentada que orienta a organização para responder a uma disrupção e retomar, recuperar e restaurar a entrega de produtos e serviços de acordo com os objetivos de continuidade de negócios;

n) Política Corporativa de Gestão de Riscos: declaração das intenções e diretrizes de riscos de uma organização;

o) ponto focal de riscos: profissional que atua nos órgãos da Empresa, como elo entre os proprietários e gestores de riscos e o órgão corporativo de gestão de riscos nas atividades relacionadas ao tema;

p) probabilidade: chance de algo acontecer;

q) proprietário do risco: papel exercido pela pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco. Nos Correios, o proprietário do risco é o diretor (podendo ser delegado para o respectivo superintendente executivo) e os gestores dos órgãos vinculados ao Conselho de Administração e à Presidência;

r) risco: efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças;

s) riscos prioritários: riscos de maior nível que afetam os objetivos organizacionais e riscos estratégicos, independentemente de sua criticidade;

t) sistema de gestão de riscos: conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos que permeia toda a organização. O sistema é composto pela Política Corporativa de Gestão de Riscos e pelos processos gerir estrutura de riscos e gerenciar riscos, bem como pelas estruturas organizacionais e seus relacionamentos conforme modelo das Três Linhas do *Institute of Internal Auditors* – IIA e pelos planos de Gestão de Riscos e de Tratamento de Riscos Estratégicos, em consonância com a governança corporativa dos Correios, com as legislações aplicáveis ao tema e com as melhores práticas de mercado;

u) processo gerir estrutura de riscos: coordenar, desenvolver, implementar e disseminar modelos, metodologias, normas e instrumentos de gestão corporativa de riscos da Empresa, de forma alinhada à estratégia e às diretrizes de governança corporativa da organização, além de monitorar e reportar os riscos corporativos com vistas à criação, preservação e obtenção de valor dos Correios, bem como elaborar políticas e diretrizes do modelo de gestão de riscos corporativos, aplicáveis aos Correios, podendo estender-se às suas entidades controladas, coligadas, patrocinadas, mantidas e subsidiárias;

v) processo gerenciar riscos: aplicar o Método de Gerenciamento de Riscos, com o objetivo de identificar, analisar, avaliar, tratar e monitorar os principais riscos dos processos, projetos e/ou atividades da empresa;

w) tolerância: limites de variação aceitável da performance com relação ao alcance dos objetivos de negócio;

x) Três Linhas: modelo que clarifica as funções e os deveres dos papéis e responsabilidades envolvidos no sistema de gestão de riscos e divide os papéis em três grupos separados, mas integrados, dentro da organização. Tem como objetivo principal otimizar as funções do Sistema de Gestão de Riscos;

y) 1ª linha: representada pelos empregados, gestores e órgãos que possuem a responsabilidade do gerenciamento e da propriedade dos riscos. No que concerne a gerenciamento de riscos é responsável por: liderar e dirigir ações de gerenciamento de riscos; manter um diálogo contínuo com o órgão de governança e reportar riscos; e estabelecer e manter estruturas e processos apropriados para o gerenciamento de riscos;

z) 2ª linha: responsável fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo: o desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidade; o atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade do gerenciamento de riscos. Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos;

aa) 3ª linha: representada pela atividade de auditoria interna governamental. No que concerne ao gerenciamento de riscos, tem como atribuição comunicar a avaliação e assessoria independentes e objetivas ao Conselho de Administração e à Presidência sobre gerenciamento de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais, promover e facilitar a melhoria contínua.

4 PRINCÍPIOS

4.1 Constituem princípios norteadores das atividades tratadas nesta Política:

a) comprometimento: a alta administração está comprometida com a gestão de riscos;

b) proteção: a gestão de riscos cria e protege o valor da organização, pois promove a melhoria contínua do desempenho institucional, fortalece os controles internos, encoraja a inovação e proporciona garantia razoável no alcance de objetivos organizacionais;

c) integração: a gestão de riscos é parte integrante de todos os processos organizacionais;

d) transparência: os riscos que comprometem o alcance dos objetivos são explicitados, por meio da disponibilização às partes interessadas de informações oportunas, precisas e tempestivas, resguardadas àquelas de caráter restrito e sigiloso, não se restringindo apenas a informações impostas por disposições de leis ou regulamentos, de modo a proporcionar o acompanhamento e o entendimento da atuação dos Correios e seu grupo econômico, de forma inequívoca;

e) ser estruturada: a gestão de riscos é sistemática, estruturada e oportuna;

f) inclusão: as partes interessadas são consultadas e comunicadas;

g) adaptação: a gestão de riscos é dinâmica e capaz de reagir às mudanças;

h) independência: a gestão de riscos tem *status* formal, com atuação independente na condução e na implementação de suas ações, com acesso irrestrito a quaisquer informações e documentos atinentes à Empresa e fundamenta-se nas melhores informações disponíveis;

i) melhoria contínua: a gestão de risco é melhorada continuamente por meio do aprendizado e experiência adquirida;

j) aculturamento: a gestão de riscos considera que a cultura organizacional e o comportamento humano influenciam significativamente na gestão de riscos.

5 DIRETRIZES

5.1 Constituem diretrizes norteadores das atividades tratadas nesta Política:

a) a gestão de riscos deve ser totalmente integrada ao planejamento estratégico, sendo considerada em todas as suas fases de construção, bem como, integrada aos processos organizacionais, políticas e tomada de decisão;

b) o processo decisório deve considerar as informações dos riscos para fazer escolhas conscientes e fundamentadas, priorizar ações e distinguir entre formas alternativas de ação;

c) a gestão de riscos deve levar em consideração os limites de exposição a riscos estabelecidos;

d) a medição do desempenho do sistema de gestão de riscos deve ser realizada mediante atividades contínuas ou avaliações independentes ou a combinação de ambas;

e) o gerenciamento de riscos deve ser continuamente revisitado, à luz de novos riscos, contextos internos e externos, situação das ações de tratamento previstas, necessidades de novas ações, de modo a garantir que os riscos mais relevantes da organização sejam gerenciados de maneira eficaz, não devendo ultrapassar o prazo de dois anos, em relação ao último realizado;

f) o monitoramento dos riscos prioritários deve perpassar os níveis estratégico, tático e operacional, conforme Modelo de Governança de Riscos;

g) o desenvolvimento contínuo dos empregados em gestão de riscos deve ser assegurado de forma adequada às suas atribuições;

h) a alta administração deve assegurar a existência de mecanismos que permitam ao órgão corporativo de gestão de riscos atuação independente e autônoma, de modo a garantir a imparcialidade em todas as suas operações;

i) a implementação de controles para mitigação dos riscos deve observar o custo-benefício e agregação de valor à organização;

j) deve ser implementado o sistema de gestão de riscos abrangendo normas (política, manuais, entre outros), processos, métodos, modelos e ferramentas de governança e de gestão que suportem a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos nos Correios, possibilitando a obtenção de informações relevantes à tomada de decisão nos níveis estratégico, tático e operacional para alcance dos objetivos organizacionais;

k) a gestão de riscos deve ser aplicada aos projetos, processos, produtos e serviços dos Correios, em processos decisórios, além de outros contextos relevantes.

6 RESPONSABILIDADES

6.1 Constituem responsabilidades do Conselho de Administração:

a) aprovar a Política Corporativa de Gestão de Riscos dos Correios, assim como suas revisões, realizando o acompanhamento da sua efetividade e aplicabilidade;

Documento é público

b) determinar a implantação, monitorar e supervisionar a adequação do sistema de gestão de riscos estabelecido para a prevenção e a mitigação dos riscos prioritários a que estão expostos os Correios, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude;

c) monitorar os riscos prioritários, seus indicadores e as medidas de tratamento, certificando-se que os riscos mais relevantes da organização foram identificados e assegurando-se que esses riscos estão sendo gerenciados de maneira eficaz;

d) atribuir formalmente a responsabilidade pela área de gerenciamento de riscos a membro da Diretoria Executiva;

e) aprovar os limites de exposição a riscos;

f) acompanhar a execução do plano anual de gestão de riscos.

6.2 Constituem responsabilidades da Diretoria Executiva dos Correios:

a) propor ao Conselho de Administração o encaminhamento da Política Corporativa de Gestão de Riscos dos Correios, assim como suas revisões;

b) aprovar políticas, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos, assim como supervisionar a sua aplicação, promovendo a integração dos agentes responsáveis;

c) liderar e supervisionar a institucionalização da gestão de riscos, oferecendo suporte necessário para sua efetiva implementação nos Correios e nas entidades controladas, mantidas, patrocinadas e subsidiárias;

d) supervisionar e monitorar os riscos estratégicos e prioritários que podem comprometer o atingimento dos objetivos organizacionais, bem como as respectivas medidas de mitigação, certificando-se que os riscos mais relevantes da organização foram identificados e assegurando-se que esses riscos estão sendo gerenciados de maneira eficaz;

e) propor os limites de exposição a riscos para aprovação pelo Conselho de Administração;

f) emitir recomendações e orientações para o aprimoramento da gestão de riscos e monitorá-las;

g) institucionalizar estruturas adequadas de gestão de riscos;

h) promover o desenvolvimento contínuo dos empregados e incentivar a adoção de boas práticas de gestão de riscos;

i) aprovar o plano anual de gestão de riscos;

j) avaliar se os procedimentos de gestão de riscos estão aderentes à respectiva política.

6.3 Constituem responsabilidades do Comitê de Auditoria:

a) assessorar o Conselho de Administração, auxiliando este, entre outros, no monitoramento da qualidade do gerenciamento de riscos;

b) avaliar e monitorar exposições de risco da empresa;

c) analisar relatórios sobre as atividades desenvolvidas pela área de gestão de riscos.

6.4 Constituem responsabilidades do proprietário do risco (1ª linha):

a) assegurar que o risco seja gerenciado de acordo com a Política Corporativa de Gestão de Riscos;

b) definir os gestores de riscos sob sua responsabilidade;

c) patrocinar as iniciativas em gerenciamento de riscos de forma a disponibilizar os recursos necessários;

d) atuar, dentro de sua alçada, na aprovação, validação e monitoramento do gerenciamento dos riscos dos contextos sob sua responsabilidade;

e) comunicar às 2ª e 3ª linhas ocorrência ou evidência de eventos que possam afetar criticamente os Correios estendendo-se aos entes abrangidos por esta Política quando pertinente.

6.5 Constitui responsabilidade do gestor do risco (1ª linha):

a) identificar, analisar, avaliar, tratar e monitorar os riscos associados aos diversos contextos dos Correios, tais como: processos, projetos, contextos decisórios, produtos e serviços dos Correios e estratégia Correios, entre outros;

b) estabelecer e revisar os Planos de Contingência ou de Continuidade de Negócios considerando-os como um controle para reduzir a materialização dos riscos de disrupção e instrumento de resposta para reduzir os impactos dela resultantes;

c) monitorar e reportar tempestivamente ao órgão corporativo de gestão de riscos a materialização de riscos prioritários e/ou estratégicos e o plano de tratamento a ser imediatamente acionado para mitigar os impactos no alcance dos objetivos organizacionais.

6.6 Constitui responsabilidade do ponto focal de riscos (1ª linha):

a) apoiar e multiplicar as ações de gerenciamento de riscos, prezando pela manutenção da cultura, ética, integridade e transparência;

b) disseminar a cultura de gestão de riscos;

c) fomentar o desdobramento de orientações quanto à observância desta Política e do processo gerenciar riscos, no âmbito das diretorias e das Superintendências Estaduais - SEs;

d) apoiar/executar a gestão de riscos no âmbito das diretorias e SEs, conforme suas particularidades e necessidades;

e) participar e/ou indicar pessoas para compor equipe multidisciplinar de mapeamentos de riscos corporativos.

6.7 Constituem responsabilidades do órgão corporativo de gestão de riscos (2ª Linha):

a) propor a Política Corporativa de Gestão de Riscos que deverá ser periodicamente revisada e aprovada pelo Conselho de Administração e comunicada a todo o corpo funcional da organização;

b) coordenar os processos de identificação, análise, avaliação e tratamento dos riscos prioritários, bem como monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;

c) propor critérios, métodos, padrões, limites de exposição a riscos e ferramentas de gestão corporativa de riscos que possibilitem o gerenciamento dos riscos e de controles de forma contínua e sistêmica;

d) implementar e monitorar o processo gerir estrutura de riscos verificando continuamente a adequação e a eficácia da gestão de riscos;

e) promover a cultura de gestão de riscos, disseminando o conhecimento e a importância do Gerenciamento de Riscos, bem como a responsabilidade de cada área dos Correios;

f) assessorar metodologicamente e tecnicamente, por meio dos analistas de riscos, as áreas na execução do processo gerenciar riscos no que tange à gestão de riscos;

g) elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria;

h) elaborar Plano Anual de Gestão de Riscos de acordo com o Plano Estratégico e outros direcionadores relevantes, submetendo-os às instâncias devidas para aprovação;

i) fornecer apoio técnico e metodológico para que os gestores responsáveis pelos principais processos de trabalho da organização identifiquem seus respectivos riscos e estabeleçam planos de contingência ou de continuidade de negócios;

j) reportar os riscos mais relevantes da organização aos órgãos colegiados, a partir das informações geradas pelos proprietários de riscos e outras de seu conhecimento, de forma a subsidiar a atuação dos referidos órgãos no que tange seus papéis e responsabilidades.

6.8 Constituem responsabilidades do órgão corporativo de controle interno (2ª linha):

a) assessorar os órgãos de 1ª linha na revisão dos controles internos existentes e na definição de novos controles quando do mapeamento assistido de riscos, nos processos críticos;

b) promover as avaliações de controles internos nos processos operacionais, de negócios, de suporte e nas unidades, conforme planejamento definido;

c) produzir e disponibilizar informações sobre as avaliações de controles internos na retroalimentação da gestão de riscos.

6.9 Constitui responsabilidade da Auditoria (3ª Linha) avaliar a efetividade do gerenciamento de riscos, contribuindo, assim, para sua melhoria e, consequentemente, para a consecução dos objetivos dos Correios.

7 DISPOSIÇÕES GERAIS

7.1 O desdobramento desta Política em documentos e/ou normativos específicos deve estar alinhado aos princípios e diretrizes nela estabelecidos.

7.2 Em função da complexidade e abrangência dos Correios, a implementação desta Política é aprimorada continuamente, a partir do desenvolvimento da maturidade da Empresa neste tema, e abrange, se necessário, a adequação de estruturas, alterações de processos e de normativos.

7.3 O detalhamento do Método de Gerenciamento de Riscos e suas particularidades concernentes ao gerenciamento de riscos, tais como identificação, análise, avaliação, tratamento, monitoramento/comunicação, estarão explanados em manual de procedimentos, cujo propósito é veicular instruções para serem executadas de forma sistematizada e segmentada disseminando-as como

Documento é público

instrumento facilitador do funcionamento, direcionamento e práticas de gestão de riscos na organização.

7.4 Os casos omissos e as dúvidas que porventura venham a surgir na aplicação desta Política devem ser submetidos ao órgão corporativo de gestão de riscos, para apreciação e, por sua vez, submetidos para deliberação em instâncias superiores.

8 REFERÊNCIAS

8.1 Fundamentação legal e normativa que orienta esta Política:

a) Lei nº 13.303/2016;

b) Decreto nº 8.945/2016 – regulamentador da Lei nº 13.303/2016;

c) Estatuto Social dos Correios;

d) Instrução Normativa Conjunta MP/CGU nº 01/2016;

e) Resolução nº 48/2023 da CGPAR;

f) Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;

g) COSO II - ERM (*Committee of Sponsoring Organizations of the Treadway Commission*) – (*Enterprise Risk Management*);

h) Código das Melhores Práticas de Governança Corporativa; São Paulo, SP: IBGC, 6ª edição 2023;

i) Modelo das Três Linhas do *Institute of Internal Auditors* – IIA;

j) Instrução Normativa CGU nº 03/2017;

k) Regimento Interno do Conselho de Administração; e

l) Regimento Interno da Diretoria Executiva.

Documento é público