# Política de Gerenciamento de Risco Operacional

Agosto de 2019

**Elaboração:** Risco

**Aprovação:** Diretoria Executiva

**Classificação do Documento:** Público

# ÍNDICE

# 1. INTRODUÇÃO

O gerenciamento de risco operacional permite identificar, avaliar e administrar riscos diante de incertezas além de integrar o processo de criação e preservação de valor para as instituições do Conglomerado. O processo é conduzido pela Diretoria Executiva e pelos demais colaboradores e é aplicado no estabelecimento de estratégias, de forma compatível com o apetite a risco de cada instituição, possibilitando um nível razoável de garantia em relação à realização de seus objetivos.

# 2. OBJETIVO

Esta Política de Gerenciamento de Risco Operacional ("a Política") tem por objetivo estabelecer os fundamentos associados ao processo de gerenciamento integrado de risco operacional em conformidade com a Resolução CMN 4.557, de 23 de fevereiro de 2017.

# 3. ABRANGÊNCIA

Estão sujeitas às regras e premissas definidas nesta política: (i) Todas as empresas e instituições pertencentes ao Conglomerado Plural; (ii) Todos os colaboradores e, (iii) Qualquer empresa prestadora de serviços e/ou funcionários terceirizados.

# 4. DEFINIÇÕES

Os principais termos contidos nesta política corporativa envolvem as seguintes definições:

## 4.1. Risco Operacional

Para efeitos desta política, define-se o risco operacional como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. O risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como as sanções em razão de descumprimento de dispositivos legais e as indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição também são consideradas.

## 4.2. Evento de Risco Operacional

Define-se como evento de risco operacional o incidente relativo à materialização do risco operacional que causa impacto negativo na instituição. Entre os eventos de risco operacional, incluem-se:

- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;
- Práticas inadequadas relativas a clientes, produtos e serviços;
- Danos a ativos físicos próprios ou em uso pela instituição;
- Eventos que acarretem na interrupção das atividades da instituição;
- Falhas em sistemas de tecnologia da informação;
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades da instituição.

### 4.3. Causas de Risco Operacional

As causas são ações ou um conjunto de circunstâncias que levam à ocorrência de um evento de risco operacional, normalmente relacionada à deficiência ou ausência de controles adequados. Podem ser segregadas em quatro fatores de risco:

- **Pessoas**: Ações humanas intencionais ou não (erros humanos) que podem causar distintos eventos de risco operacional ou problemas decorrentes da falta de recursos humanos (seja na quantidade ou na capacidade técnica).
- **Processos:** Deriva da interrupção, falha ou falta de controle, desenho inadequado de processos dentro das linhas de negócio ou em processos de apoio.
- **Sistemas:** Deficiências decorrentes do desempenho dos sistemas; Sistemas não adequados, sistemas obsoletos, falhas com a comunicação externa, alterações efetuadas em sistemas (rotinas) que incorrem em eventos em áreas distintas a área de Tecnologia. Este fator de risco considera a interrupção de comunicação para terceiros.
- **Fatores externos:** Este fator de risco é oriundo de ocorrências externas que impactam negativamente nas entidades pertencentes ao Conglomerado financeiro e ao consolidado econômico-financeiro e relacionam-se com a deficiência decorrente da incapacidade ou ineficiência em tratar tais ocorrências.

## 5. ESTRATÉGIA

A estratégia definida pela Diretoria é que a Instituição utilize as melhores práticas para atuar de forma preventiva mantendo um framework robusto e proporcional à dimensão e a relevância das respectivas exposições para mitigar o risco operacional e os efeitos agregados dos demais riscos que podem afetar a realização dos objetivos da Instituição.

## 6. ESTRUTURA DE GERENCIAMENTO DE RISCO OPERACIONAL

A estrutura de gerenciamento de risco operacional adotada tem como objetivo a identificação, avaliação, mensuração, monitoramento, controle e mitigação do risco operacional e deve estar compatível com o modelo de negócio, com a natureza das operações e com a complexidade dos produtos e serviços, das atividades e dos processos. A estrutura deve conter mecanismos que permitam a implementação e a disseminação da cultura de risco operacional, das políticas, dos processos e de infraestrutura condizentes com as entidades pertencentes ao Conglomerado. Assegurar a aderência e comprometimento de todos os colaboradores para a adequada gestão do risco operacional, Continuidade de Negócios e dos objetivos da Instituição.

O gerenciamento de risco operacional possui a seguinte estrutura:

O Grupo Plural entende que o risco operacional deve ser gerenciado de forma integrada. Nesse contexto, a Instituição adota o modelo de Três Linhas de Defesa. Este modelo é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controles por meio do esclarecimento dos papéis e responsabilidades essenciais dentro da instituição.

# 7. RESPONSABILIDADES

Em linha com o escopo desta política, seguem abaixo as responsabilidades das principais áreas envolvidas nos processos de gerenciamento de riscos:

## 7.1. Da Diretoria Executiva

- Aprovar e revisar com periodicidade mínima anual as políticas, estratégias e limites para o gerenciamento de risco operacional, bem como o programa de testes de estresse e as políticas para gestão de continuidade de negócios;
- Definir os níveis de apetite por riscos que as entidades pertencentes ao Conglomerado Prudencial devem aceitar e revisá-los com periodicidade mínima anual, com auxílio do Comitê de Riscos e do CRO;
- Manifestar-se sobre as ações incluídas nos relatórios Controles Internos, bem como fazer constar nos relatórios, sua responsabilidade sobre as informações divulgadas;
- Assegurar a aderência da instituição às políticas, estratégias e limites de gerenciamento de riscos;
- Garantir que a estrutura de remuneração da instituição não incentive comportamentos incompatíveis com os níveis de apetite a risco dispostos na RAS;
- Assegurar a correção tempestiva das deficiências da estrutura de gerenciamento de riscos;
- Promover a disseminação da cultura de gerenciamento de riscos na instituição;
- Autorizar, quando necessário, exceções à política, aos procedimentos, aos limites e aos níveis de apetite por riscos fixados na RAS;
- Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos e de gerenciamento de capital, de forma independente, objetiva e efetiva;
- Indicar o diretor responsável pela Unidade de Gerenciamento de Riscos.

## 7.2. Do Comitê de Risco Operacional, Controles Internos e Compliance

- Aprovar e revisar a política de gerenciamento de risco operacional anualmente;
- Compreender, de forma abrangente e integrada, os riscos que podem impactar o capital e a liquidez;
- Assessorar a Alta Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à disseminação da cultura, mitigação de riscos e da conformidade com as normas aplicáveis;
- Estabelecer diretrizes para garantir o cumprimento à regulamentação vigente, inibir riscos incompatíveis e/ou desnecessários às entidades pertencentes ao Conglomerado, aumentar a eficácia das áreas de negócios, melhorar a efetividade dos controles e minimizar o impacto aos riscos a que estão sujeitos.

## 7.3. Do Chief Risk Officer ("CRO")

- Supervisionar o desenvolvimento, implementação e desempenho da estrutura de gerenciamento de risco operacional, incluindo seu aperfeiçoamento;
- Avaliar e garantir a adequação, à RAS e aos objetivos estratégicos da instituição, da política, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de risco de operacional;
- Capacitar adequadamente os integrantes da Unidade de Gerenciamento de Riscos acerca da política, dos processos, dos relatórios, dos sistemas e dos modelos da estrutura de gerenciamento de riscos, mesmo que desenvolvidos por terceiros;
- Subsidiar e participar no processo de tomada de decisões estratégicas relacionadas ao gerenciamento de risco operacional, auxiliando a Diretoria Executiva.
- Indicar as diretrizes a serem seguidas no programa de testes de estresse.

## 7.4. Da Área de Auditoria Interna

- Avaliar periodicamente os processos e procedimentos relativos ao gerenciamento de riscos e de capital;
- Realizar anualmente testes de avaliação dos sistemas utilizados no gerenciamento de risco operacional com o objetivo de verificar a aderência aos fundamentos estabelecidos nesta política;
- Identificar e avaliar riscos potenciais para a Organização e suas linhas de negócios;
- Desenvolver um plano de auditoria anual baseado em risco e um planejamento cíclico de longo prazo com possibilidade de ajustes ao longo do tempo em caso de necessidade;

- Revisar a adequação dos controles estabelecidos para assegurar conformidade com as políticas, procedimentos, leis, regras e objetivo do negócio;
- Avaliar, quando necessário, a confiabilidade e segurança das informações financeiras e gerenciais, além dos sistemas e operações que geram esses dados;
- Avaliar os métodos de salvaguardas de ativos da organização e seus clientes;
- Avaliar e revisar o ambiente tecnológico da Organização através da adoção de um plano específico de auditoria de sistemas. O plano de auditoria de sistemas deve considerar no mínimo: os controles de mudanças em infraestrutura e sistemas aplicativos; a segurança física ao ambiente de processamento de dados; a segurança lógica de acesso aos sistemas aplicativos, ambiente de rede e banco de dados; manutenção de sistemas aplicativos, rede; e o plano de continuidade de negócios;
- Acompanhar ('follow-up') os pontos identificados para assegurar o cumprimento das ações recomendadas, no prazo estabelecido;
- Conduzir revisões pontuais (ad hoc) ou investigações a pedido do Comitê de Auditoria ou da alta administração.

### 7.5. Da Unidade de Gerenciamento de Riscos

- Elaborar e documentar as políticas e estratégias para o gerenciamento do risco de operacional;
- Implementar estrutura, disseminar o conhecimento e subsidiar as demais áreas para aderência e comprometimento das regulamentações que visam o gerenciamento de risco operacional;
- Auxiliar na definição de apetite de risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Aplicar metodologia para identificar, avaliar, monitorar, mensurar, controlar e mitigar continuamente as causas, dos eventos de risco operacional, junto aos gestores, coordenando e garantindo planos de ação para corrigir de forma tempestiva e assertiva as deficiências de controle e submeter ao Comitê de Riscos e a Diretoria Executiva;
- Monitorar o gerenciamento dos riscos da 1° linha de defesa;
- Elaborar relatório consolidado de Risco Operacional, contemplando inclusive pontos relevantes identificados por Compliance e Controles Internos, com periodicidade mínima anual e submeter ao Comitê de Risco Operacional, Controles Internos e Compliance;
- Documentar, armazenar, classificar e agregar as informações referentes às perdas associadas ao risco operacional;

- Garantir, em conjunto com a área de tecnologia da informação, processos para prover a continuidade de negócios;
- Identificar previamente os riscos inerentes a novas atividades e produtos realizando análise de sua adequação aos procedimentos, controles e melhores práticas adotados no Conglomerado Plural;
- Disseminar à instituição, em seus diversos níveis, o apetite a risco documentado na RAS, bem como o procedimento para reporte de ocorrência relacionadas a não observância dos níveis de apetite por riscos.

### 7.6. Da Área de Controles Internos

- Modelar novos processos operacionais ou atuar na reengenharia de processos e atividades existentes;
- Avaliar a eficiência dos controles internos com base em riscos;
- Apoiar na estruturação e gestão dos riscos corporativos;
- Fortalecer no processo de prevenção de fraude corporativa;
- Apoiar a manutenção de processos operacionais alinhados com a estratégia e apetite a risco da instituição.

### 7.7. Da Área de Compliance

- Monitorar riscos específicos, como, por exemplo, a não conformidade com leis e regulamentos aplicáveis a instituição;
- Reportar eventuais inconsistências diretamente a Diretoria Executiva;
- Orientar sobre processos de gerenciamento de riscos e conformidade;
- Identificar mudanças no cenário regulatório e de riscos, e alertar a 1ª Linha de Defesa de tais inovações;
- Realizar testes e avaliação de aderência das atividades institucionais às normas legais, infralegais, às recomendações emitidas por órgãos de supervisão e auto reguladores, assim como às políticas internas, conforme plano anual de testes de conformidade aprovado pela Diretoria Executiva;
- Auxiliar na definição de apetite de risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Identificar e reportar ao COAF os atos, omissões e operações que possam auxiliar ou cooperar de alguma forma para a identificação dos delitos de fraude, lavagem de dinheiro e/ou financiamento ao terrorismo;

- Elaborar treinamentos e ações de disseminação de cultura de conformidade e controle de riscos.

### 7.8. Dos Gestores e Colaboradores

- Identificar os riscos operacionais oriundos do exercício de suas atividades, considerando também os serviços terceirizados utilizados;
- Estabelecer e gerenciar os controles de risco inerentes as suas atividades do dia a dia.
- Avaliar regularmente o serviço pactuado com prestadores de serviços terceirizados;
- Informar à Unidade de Gerenciamento de Riscos os eventos de risco operacional.

### 7.9. Do Jurídico

- Identificar e mitigar o risco legal na elaboração dos contratos firmados pela instituição;
- Incluir nos contratos firmados pela instituição cláusulas que estabeleçam claramente os papéis e as responsabilidades dos prestadores de serviços terceirizados.
- Garantir a inclusão das cláusulas necessárias nos contratos de TI conforme Resolução N° 4.658.

### 7.10. Da Área de Tecnologia

- Assegurar a integridade, segurança e disponibilidade dos dados e dos sistemas de informação;
- Definir mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

## 8. DIRETRIZES DE GERENCIAMENTO DE RISCO OPERACIONAL

A metodologia utilizada está em linha com o *framework* definido nos documentos: (i) "*Principles for the Sound Management of Operational Risk"* emitido em junho de 2011 pelo *Basel Committee on Banking Supervision* e (ii) "*Integrated Framework: Application Techniques"* publicado em setembro de 2011 pelo COSO - *Committee of Sponsoring Organizations of the Treadway Commission*. Neste modelo, a gestão de riscos operacionais considera os seguintes elementos:

- Ambiente Interno

- Fixação de Objetivos
- Identificação de Eventos
- Avaliação de Riscos
- Atividade de Controle
- Resposta a Risco
- Informações e Comunicações
- Monitoramento

Assim, o Conglomerado Plural deve possuir um ambiente interno propício para a prática de controles internos e gestão de riscos onde os objetivos estratégicos sejam fixados, os eventos de risco identificados e avaliados, uma resposta para a ocorrência dos riscos mapeados deve ser estabelecida. Deve haver atividades de controle, um fluxo de informações e comunicações na empresa e, por fim, um monitoramento contínuo dos riscos relevantes.

A gestão do risco operacional compreende uma série de atividades e controles que dão sustentação à gestão da Instituição. O detalhamento dos procedimentos e ferramentas utilizadas são abordadas no Manual de Gerenciamento de Riscos.

## 9. APROVAÇÃO E REVISÃO

Esta política será aprovada e revisada com periodicidade mínima anual pela Diretoria Executiva.

www.bancoplural.com

**São Paulo SP**
Rua Surubim, 373
1º andar Vila Olímpia
CEP 04571-050
Tel: +55 11 3206 8000

**Rio de Janeiro RJ**
Praia de Botafogo, 228
9º andar Botafogo
CEP 22250-906
Tel: +55 21 3923 3000

**New York NY**
Escritório Parceiro
545 Madison Av. 8th Floor
10022 - NY - USA
Tel: +1 212 388 5600

**Miami FL**
Escritório Parceiro
777 Brickell Av. Suite 500
33131 - FL - USA
Tel: +1 212 388 5600