



BANCO
FIBRA

**POLÍTICA DE GERENCIAMENTO DE
RISCO OPERACIONAL E CONTROLES
INTERNOS**

Versão 15 - Nov/22

1. DEFINIÇÃO

Este normativo tem por objetivo estabelecer diretrizes e fundamentos associados à estrutura e ao processo de gerenciamento do risco operacional e à atuação de controles internos no Banco Fibra S.A e empresas que compõem o seu conglomerado prudencial.

2. PÚBLICO-ALVO

Banco Fibra S.A., inclusive sua Filial em Cayman e empresas que compõem o seu conglomerado prudencial (doravante denominadas “Banco Fibra” ou “Banco”).

3. DESCRIÇÃO

3.1. CONCEITO DE RISCO OPERACIONAL

Risco Operacional é a possibilidade de perdas decorrentes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, ou por eventos externos, incluindo perdas legais.

O conceito de Risco Operacional inclui o Risco Legal, que consiste na possibilidade de perda decorrente à inadequação ou deficiência em contratos firmados, ao descumprimento de leis ou regulamentações aplicáveis, ou associado a indenizações por danos a clientes ou terceiros dado a inadequação de produtos, serviços ou contratos.

3.2. CONCEITO DE CONTROLES INTERNOS

Controles Internos é o conjunto de procedimentos estabelecidos pela instituição com a finalidade de reduzir os riscos operacionais presentes em suas atividades, seus sistemas de informações financeiras, operacionais e gerenciais.

4. ESCOPO DO GERENCIAMENTO DE RISCO OPERACIONAL

A estrutura de gerenciamento de riscos operacionais do Banco Fibra considera o tamanho e a complexidade de seus negócios, o que permite o acompanhamento, monitoramento e o controle dos riscos aos quais está exposto.

A estrutura compõe a realização da identificação e avaliação de riscos operacionais, com o objetivo de selecionar os riscos relevantes que possam impedir a criação, preservação e



realização de valor para a Instituição, ou que podem corroer o valor existente, com a possibilidade de impactos em resultados, capital, liquidez e reputação.

O processo de gerenciamento de riscos operacionais permeia por toda a Instituição, alinhado às diretrizes da Alta Administração e dos executivos, que, por meio de comitês e demais reuniões internas, definem os objetivos estratégicos de acordo com o apetite ao risco. A abordagem de gerenciamento adotada é o modelo de três linhas de defesa:

Primeira Linha de Defesa: representada pelos gestores das áreas de negócio e/ou suporte, que geram exposição a riscos, onde o processo ocorre. São responsáveis pela gestão dos riscos inerentes às suas atividades, implementando e/ou aperfeiçoando os controles e ações mitigatórias necessárias.

Especificamente no âmbito do Risco Legal, com objetivo de resguardar a instituição de eventuais perdas, o Jurídico atua na análise de todos os contratos firmados nas negociações com os clientes e na contratação de terceiros.

Segunda Linha de Defesa: representada pela área de Controles Internos, Risco Operacional e Processos, tem a responsabilidade de auxiliar a primeira linha na identificação de riscos e sua mitigação, avaliar a qualidade do ambiente de controle na primeira linha e atuar de forma consultiva, sugerindo revisão de processos ou novos controles à primeira linha de defesa.

Terceira Linha de Defesa: Cabe à Auditoria Interna este papel. É responsável por avaliar, periodicamente, todos os elementos, de qualquer linha de defesa, verificando a eficácia da governança, do gerenciamento dos riscos e controles e o alcance dos objetivos esperados.

As três linhas desempenham papéis independentes e complementares na governança de Controles Internos e Riscos Operacionais.

4.1. CATEGORIAS DE RISCO OPERACIONAL

Para efeito de categorização, o Banco Fibra utiliza as mesmas definições pertinentes ao Banco Central do Brasil, e outros reguladores e autorreguladores, quando aplicável:

- 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;
- Situações que acarretem a interrupção das atividades da instituição;
- Falhas em sistemas, processos ou infraestrutura de tecnologia da informação;



- Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição.

Adicionalmente às oito categorias de risco operacional mencionadas acima, a estrutura de Gerenciamento de Risco Operacional também considera os eventos relacionados ao Risco Social, Ambiental e Climático, conforme definido nas normas do Banco Central do Brasil em vigor.

4.2. ETAPAS DO GERENCIAMENTO DE RISCO OPERACIONAL

- Identificação: Consiste em mapear os processos, identificar os riscos, associar os riscos aos processos e identificar os controles mitigatórios;
- Mensuração e avaliação: Compreende medir cada risco operacional identificado e avaliar sua exposição aos demais riscos aplicáveis à Instituição, cujas métricas possuem critérios aprovados pela instituição (Anexo II);
- Mitigação e controle: Desenvolver planos de ação para manter a exposição ao risco em patamares aceitáveis;
- Monitoramento: Testar controles existentes para garantir efetiva mitigação de riscos (teste de efetividade), monitorar o ambiente de controles internos e o nível de exposição ao risco;
- Reporte: Manter a administração informada sobre os riscos operacionais e a qualidade do ambiente de controles internos.

4.3. TESTE DE EFETIVIDADE DE CONTROLES

Com o objetivo de garantir que o sistema de controles internos da instituição é efetivo em relação à mitigação dos riscos para os quais foram implementados, é de responsabilidade da área de Controles Internos, Risco Operacional e Processos, a realização de testes periódicos dos controles mapeados, de acordo com cronograma de testes definido para cada ano. Este cronograma é definido usando como critério a classificação de Controles Regulatórios, Chave e Não Chave:

- Controles Regulatórios são aqueles que atendem a alguma regulamentação vigente;
- Controles Chave são todos aqueles que tem papel fundamental na mitigação do risco e sua falta resulta no aumento do Risco Residual, ou seja, uma falha no processo impactaria de maneira significativa o Banco, dentro dos pilares Financeiro, Reputacional, Legal/Normas Internas e Relação com o Cliente; e
- Controles Não Chave são todos aqueles controles complementares e/ou secundários, dada a existência de outro controle mitigante existente.



5. RESPONSABILIDADES DA ÁREA DE CONTROLES INTERNOS, RISCO OPERACIONAL E PROCESSOS

- Desenvolver e disponibilizar ferramentas e técnicas para identificação, mensuração e avaliação, mitigação e controle, monitoramento e reporte do risco operacional;
- Coordenar a avaliação de riscos em mudanças significativas nos processos existentes, bem como em projetos de Melhoria Contínua;
- Elaborar e aprovar, junto ao Comitê de Gestão de Riscos, o plano de trabalho de Controles Internos, de modo a mapear processos e avaliar a qualidade e efetividade do ambiente de controles internos nas áreas internas, bem como nos processos da Instituição;
- Desenvolver e programar o processo de coleta das informações de eventos de risco operacional;
- Manter a base de perdas operacionais, garantindo a devida classificação do risco nas perdas ocorridas (risco de crédito, risco de mercado, risco social, risco ambiental e risco climático);
- Proceder com o armazenamento de informações e documentos referentes a eventos de risco operacional, com ou sem perdas financeiras associadas;
- Reportar ocorrências e deficiências relevantes à Alta Administração;
- Acompanhar o efetivo cumprimento dos planos de ação criados em decorrência dos riscos operacionais identificados, de acordo com os prazos e responsabilidades planejados;
- Promover os programas de treinamento e comunicação para conhecimento do risco operacional, com a finalidade de disseminar uma cultura organizacional, atenta à importância dos controles internos capazes de mitigar o risco operacional;
- Participar do processo de aprovação e revisão de produtos;
- Elaborar os relatórios de Riscos Operacionais e de Controles Internos, conforme moldes exigidos pelas normas e regulações normas do Banco Central do Brasil, e outros reguladores e autorreguladores, quando aplicável
- Realizar a avaliação anual dos prestadores de serviços terceirizados considerados relevantes;
- Aplicar anualmente a Autoavaliação de Riscos e Controles Internos nas áreas internas, através do *Control Self Assessment (CSA)*;
- Realizar, periodicamente, através dos testes de efetividade, a avaliação do desenho e da eficácia dos controles internos existentes; E
- Coordenar a atuação dos Assistentes de Controles Internos (ACIRs), assegurando adequada capacitação sobre risco operacional.



6. INDICADORES DE APETITE A RISCO

O objetivo do Banco Fibra é manter o risco operacional em níveis apropriados ao porte e complexidade das operações da organização, em conjunto à melhoria contínua de processos internos.

Faz parte da atividade bancária a assunção de riscos para o alcance das metas e dos objetivos estratégicos traçados. Para isso, são definidos níveis de riscos que são aceitáveis de serem incorridos, através de controles que servem para identificá-los, qualificá-los, monitorá-los, mitigá-los e reportá-los nos devidos fóruns e Comitês.

O Banco Fibra estabeleceu uma governança de riscos e capital que permite que os objetivos estratégicos sejam alcançados dentro dos níveis de apetite de riscos.

Os indicadores de apetite a risco na dimensão de Risco Operacional visam o monitoramento e controle do risco operacional potencial, assim como a atuação na resolução dos problemas ocorridos e a implantação de mitigadores dos riscos identificados, buscando a adequada mitigação de riscos potenciais acima do apetite do Banco.

Estabelece o apetite do Banco à exposição ao risco residual como baixo, reduzindo a possibilidade de perdas associadas a falhas operacionais. Considera os riscos potenciais e controles mitigatórios existentes na Matriz de Riscos e as falhas operacionais ocorridas, classificados de acordo com a metodologia apresentada no Normativo Interno de Gerenciamento de Risco Operacional e Controles Internos.

