



**Política de Gerenciamento de Risco de  
Mercado e Operacional**

Revisão em:  
30/04/2019

Publicação em:  
18/10/2017

Versão  
3.0

# **Política de Gerenciamento de Risco de Mercado e Operacional**

## Sumário

<b>1. Estrutura</b> .....	4
Diretoria de Risco .....	4
Diretor Responsável: .....	4
Comitê de Gerenciamento de Risco .....	4
Superintendência de Risco .....	4
Compliance .....	4
<b>2. Risco de Mercado</b> .....	4
<b>3. Definições</b> .....	5
a. Risco de Mercado .....	5
b. VaR .....	5
3.1 Metodologia .....	5
<b>4. Risco Operacional</b> .....	5
4.1 Definições de Risco Operacional .....	5
I) Fraudes internas .....	6
II) Fraudes externas .....	6
III) Falha humana .....	6
IV) Demandas trabalhistas .....	6
V) Segurança deficiente do local de trabalho .....	6
VI) Práticas inadequadas relativas a clientes, produtos e serviços .....	6
VII) Danos a ativos físicos próprios ou de terceiros .....	6
VIII) Interrupção das atividades da instituição .....	6
IX) Falhas em sistemas de tecnologia da informação .....	6
X) Falhas na execução, no cumprimento de prazos e/ou no gerenciamento de atividades da instituição. ....	6
XI) Risco legal associado à inadequação ou deficiência em contratos firmados pela instituição. ...	7
XII) Sanções em razão de descumprimento de dispositivos legais .....	7
XIII) Indenização por danos a terceiros decorrentes das atividades desenvolvidas pela instituição..	7
4.2 Princípios Mitigadores .....	7
I) Princípio da Formalização .....	7
II) Princípio da Disseminação .....	7
III) Princípio da Atualização .....	7
IV) Princípio da Avaliação .....	7
4.3 Componentes do Risco Operacional .....	7

Identificação/Avaliação dos Riscos.....	8
Resposta ao Risco .....	8
Informação e Comunicação.....	8
Monitoramento .....	8
5. Revisão da Norma.....	8

## 1. Estrutura

### Diretoria de Risco

Responsável por representar o Conglomerado junto ao Banco Central do Brasil e responsável pela execução do gerenciamento de riscos.

#### **Diretor Responsável:**

Luis Eduardo da Costa Carvalho

### Comitê de Gerenciamento de Risco

Composto pelo Diretor de Risco, Superintendente de Risco e Compliance.

### Superintendência de Risco

Responsáveis por controlar e cobrar as áreas da empresa o suporte necessário para execução do gerenciamento de riscos.

### Compliance

Responsável por assegurar o cumprimento das normas internas e da legislação em vigor de que trata esta política.

## 2. Risco de Mercado

A LECCA possui uma estrutura de Risco de Mercado, capaz de identificar, avaliar, monitorar, controlar e mitigar os riscos de mercado, a fim de assegurar que:

- os riscos de mercado aos quais a instituição esteja exposta sejam identificados, avaliados, monitorados e minimizados em um nível aceitável;
- os riscos inerentes a novas atividades e produtos sejam avaliados previamente quanto à adequação aos procedimentos e controles da instituição;
- a estrutura de gerenciamento de risco, suas políticas e estratégias sejam continuamente revisadas, considerando-se as exposições em ativos e passivos e a identificação prévia inerente às novas atividades e produtos sujeitos ao risco de mercado;
- a realização de testes de estresse para determinação de revisão das políticas e limites operacionais para adequação do capital;
- a adequação de sistema e ferramentas para a gestão do risco de mercado e sua interface com os órgãos reguladores;
- a Instituição compreenda claramente os objetivos do processo de Gestão de Riscos

de Mercado, os papéis, funções e responsabilidades atribuídas aos seus diversos níveis hierárquicos;

- haja disponibilização das informações estruturadas para decisões da alta administração e para o acesso público;
- os objetivos estratégicos da instituição sejam atendidos;
- a LECCA atenda aos critérios regulamentares vigentes.

### 3. Definições

#### a. Risco de Mercado

O Conselho Monetário Nacional define como Risco de Mercado a possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira.

A definição acima inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).

#### b. VaR

É a medida da máxima perda esperada de uma carteira sob condições normais de mercado, dados um nível de confiança e um horizonte de tempo. No caso da LECCA, o nível de confiança é de 90% e o horizonte temporal de um dia.

#### 3.1 Metodologia

A LECCA monitora e controla o risco de mercado baseado no cálculo do Valor em Risco (VaR), nas suas versões regular e de *stress*. Esta metodologia está de acordo com o órgão regulador e está adequada às características das operações do Conglomerado LECCA.

### 4. Risco Operacional

A LECCA possui uma estrutura de Risco Operacional, em conformidade com a Resolução CMN nº 3380/09, capaz de identificar, avaliar, monitorar, controlar e mitigar os riscos operacionais aos quais o Conglomerado Financeiro esteja exposto, de acordo com a natureza e complexidade dos seus produtos, serviços, atividades, processos e sistemas.

#### 4.1 Definições de Risco Operacional

Os riscos operacionais são definidos como possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas e/ou eventos externos. Para fins desta política, são considerados como riscos operacionais, além de outros, os seguintes pontos:

**I) Fraudes internas**

Possibilidade de adulteração de controles, descumprimento intencional de normas, vazamento de informação privilegiada, divulgação intencional de informações incorretas, desvio de valores e quaisquer outros comportamentos fraudulentos por parte de colaboradores e/ou prestadores de serviços.

**II) Fraudes externas**

Ações intencionais executadas por entidades externas, pessoas físicas ou jurídicas, com o objetivo de lesar as instituições, mediante acesso aos sistemas de informação, documentos, falsificações, furtos, roubos e atos de vandalismo.

**III) Falha humana**

Decorrente de equívoco, omissão, distração ou negligência de colaboradores ou terceiros contratados para a execução de atividades operacionais.

**IV) Demandas trabalhistas**

Descumprimento de cláusulas dos contratos de trabalho e de normas previstas na CLT – Consolidação das Leis do Trabalho, Decreto-Lei n° 5.452, de 01/05/1943, pagamento incorreto de verbas rescisórias e/ou alto número de reclamações trabalhistas.

**V) Segurança deficiente do local de trabalho**

Instalações e equipamentos em desacordo com as normas vigentes e/ou alto índice de acidentes de trabalho.

**VI) Práticas inadequadas relativas a clientes, produtos e serviços**

Formalização de negócios em desacordo com as respectivas normas ou manuais internos, cláusulas contratuais, normas legais e/ou que não atendam às necessidades demandadas pelos clientes.

**VII) Danos a ativos físicos próprios ou de terceiros**

Danos causados por vandalismo, desastres ou fenômenos naturais, como por exemplo, tempestades, inundações e/ou vendaval.

**VIII) Interrupção das atividades da instituição**

Danos causados por greve falta de energia, sabotagem e/ou falha nos servidores e estações de trabalho.

**IX) Falhas em sistemas de tecnologia da informação**

Qualquer descontinuidade das atividades apoiadas por serviços tecnológicos, motivadas por falta de meios seguros de acesso, falhas de manutenção dos sistemas, erros na preparação de backups, falta de proteção de firewalls, inadequação de sistemas operacionais e aplicativos e/ou impossibilidade de recuperação de dados por queda de energia ou quebra de equipamentos.

**X) Falhas na execução, no cumprimento de prazos e/ou no gerenciamento de atividades da instituição.**

Comercialização de produtos em desacordo com as respectivas normas ou manuais internos e/ou normas legais.

**XI) Risco legal associado à inadequação ou deficiência em contratos firmados pela instituição.**

Possibilidade de questionamento jurídico na execução dos contratos firmados pela instituição e/ou sanções por parte de órgãos fiscalizadores em função da inobservância de leis, regulamentos e normas legais.

**XII) Sanções em razão de descumprimento de dispositivos legais**

Penalidades administrativas ou financeiras motivadas pelo descumprimento de normas.

**XIII) Indenização por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.**

Indenizações pagas a clientes pelo não cumprimento da legislação pertinente aos produtos comercializados

**4.2 Princípios Mitigadores**

A gestão dos riscos operacionais será norteadada pelos seguintes princípios:

**I) Princípio da Formalização**

Todos os processos operacionais do Conglomerado deverão estar mapeados e vinculados às normas, procedimentos e/ou manuais que regulem a sua execução, com clara definição das responsabilidades de todos os envolvidos.

**II) Princípio da Disseminação**

As normas e os procedimentos mencionados anteriormente devem estar acessíveis a todos os empregados e colaboradores, assim como o conceito de risco operacional. A área de Processos é será a responsável pela publicação, atualização e divulgação de todos os normativos, que estão disponibilizados na intranet e com total acesso a todos os colaboradores. Todos os processos internos foram mapeados por Consultoria Especializada, existindo Manuais e Instruções de Trabalho para todos os setores. A revisão dos normativos ocorre periodicamente e conforme determina a legislação competente ou por demanda da diretoria.

**III) Princípio da Atualização**

A política de Gerenciamento do Risco Operacional deverá ser objeto de permanente atualização, objetivando seu aperfeiçoamento, devendo ser atualizada, no mínimo, anualmente,

**IV) Princípio da Avaliação**

Toda alteração de procedimentos internos ou lançamento de novos produtos exigirá uma avaliação dos riscos operacionais incidentes.

**4.3 Componentes do Risco Operacional**

Baseado no princípio da formalização, todos os processos operacionais serão mapeados e divulgados. A sua revisão deverá ser feita pelo Comitê de Riscos com periodicidade semestral, quando poderão ser promovidas reuniões multidisciplinares para a discussão de melhores práticas operacionais. O mesmo procedimento deve ser adotado quando forem implementados novos processos, em conformidade com o Princípio da Avaliação.

**Identificação/Avaliação dos Riscos**

Caberá ao Diretor de Riscos avaliar os riscos implícitos nos processos, que deverá ser revisada e aprovada pelo Comitê nas revisões semestrais, alterações de procedimentos ou lançamentos de novos produtos. Essa avaliação deverá estar alinhada com as categorias de risco definidas na Resolução nº. 3.380/06 do CMN.

**Resposta ao Risco**

Entende-se como resposta ao risco a decisão de acatar ou mitigar os riscos identificados. Essa decisão deve levar em consideração a probabilidade e os impactos gerados no caso da materialização do risco, bem como a análise de custo x benefício da ação mitigatória.

**Informação e Comunicação**

Eventuais deficiências e solicitação de revisão ficará a cargo do Comitê de Riscos e/ou Compliance, que comunicará ao departamento de Processos a necessidade de atualização da política, bem como a respectiva divulgação e publicação.

**Monitoramento**

A Superintendência de Risco deverá monitorar os processos e informar ao Comitê de Riscos as ocorrências de falhas nos processos através de relatórios de controles. Esse monitoramento também deverá ser feito pelos responsáveis de cada departamento.

A materialização do risco deve ser registrada no relatório de ocorrência, devendo, ainda, ser identificada a conta em que a ocorrência será contabilizada.

**5. Revisão da Norma**

A Norma de Risco de Crédito, Mercado e Operacional, incluindo seus respectivos processos e controles será revisada anualmente, conforme estabelecido nas Resoluções 3.380/06 e 3.464/07 do CMN.