

**ESTRUTURA PARA**

**GERENCIAMENTO DE RISCO OPERACIONAL**

**RESOLUÇÃO 3380 - BACEN**

## **RELATÓRIO – BACEN RESOLUÇÃO 3380**

### **A. OBJETIVO**

Este documento foi elaborado visando atender a Resolução 3380 do Banco Central do Brasil:

*"Determina às instituições financeiras a implementação de estrutura de gerenciamento de risco operacional, capacitada a identificar, avaliar, monitorar, controlar e mitigar riscos associados a cada instituição, bem como o risco decorrente de serviços terceirizados".*

## **2. ESTRUTURA DE GERENCIAMENTO DE RISCOS OPERACIONAIS,**

A estrutura de Gestão de Risco Operacional foi montada não somente para atender a legislação, mas também para planejar, homogeneizar, identificar, mapear, mitigar, analisar e definir plano de ação de melhorias.

### **A. Frameworks Usadas**

Na montagem da estrutura de gerenciamento de risco operacional foram utilizadas as frameworks:

- **COSO** – *Committee of Sponsoring Organizations e*
- **COBIT** – *Control Objectives for Information and Technology.*

### **B. Metas**

As seguintes metas foram previstas para serem alcançadas:

- Assegurar aos Clientes mais informações e proteção aos seus interesses
  - Melhorar o desempenho e melhorar o valor patrimonial
  - Facilitar o acesso ao capital a um custo menor
-

- Proteger contra os eventuais abusos do poder
- Possibilitar o aumento e valorização das ações
- Tornar a instituição mais competitiva
- Valorizar a imagem institucional
- Propiciar o conhecimento dos requisitos necessários para aderência às normas e postulados legais
- Identificar os Riscos envolvidos nos processos da instituição
- Implantar a Gestão de Risco Operacional
- Definir os Planos de Ação e Melhorias para os Riscos de maior exposição (Risco Líquido)
- Elaborar documentação dos processos mapeados
- Buscar a padronização de processos e procedimentos
- Efetuar Treinamento dos principais gestores dos processos.

### **C. Atribuições da Área de Controles Internos**

A estrutura de Gestão de Risco Operacional, visa possibilitar a Área de Controles Internos desempenhar as seguintes atividades:

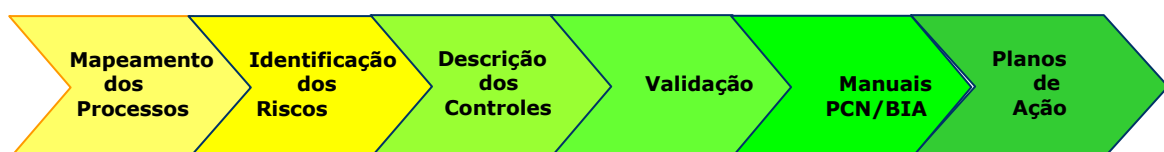
- Monitoramento dos processos de forma a evitar conflito de interesses;
  - Avaliar se os acessos às informações dos funcionários é correta e os mesmos possuem o conhecimento adequado de suas tarefas e responsabilidades;
  - Realização de testes periódicos de segurança dos Sistemas Informáticos, bem como dos planos de contingência;
  - Monitoramento da aplicação dos padrões Éticos e de Integridade e controle da correta aplicação do código de ética;
  - Investigar, quando informado ou por iniciativa própria, com prévia concordância da Superintendência, as eventuais ocorrências de anomalias, informando em caso positivo à Superintendência para as devidas providências.
  - Com a prévia anuência da Superintendência sugerir a criação de funções, controles, alterações de normativas e procedimentos..
  - Análise e categorização de erros (intencionais e não intencionais), sugerindo controles;
  - Manter informada a Superintendência da instituição através de comunicados e relatórios, sobre a constatação de eventuais riscos operacionais.
-

- Além das atividades acima relacionadas, o *Compliance* deverá acompanhar eventuais riscos relacionados a:
  - Imagem da instituição;
  - Novos produtos e serviços;
  - Ausência de segregação de funções;
  - Descumprimento de limites;
  - Processos de apuração de risco operacional;
  - Processos de Liquidação Financeira;
  - Incorreta emissão/custódia de contratos e garantias.

### **3. ETAPAS DA GESTÃO DE RISCO OPERACIONAL**



### **4. FASES DO PROJETO DE GESTÃO DE RISCO OPERACIONAL**



## **A. Mapeamento De Processos, Riscos E Controles**

- Levantamento de Informações
  - Entrevistas com os principais executivos da Organização
  - Entrevistas com os funcionários operacionais
  - Levantamento dos procedimentos dos processos
- Descrição detalhada dos processos
- Elaboração de Fluxos Macro dos Processos
- Discussão com os responsáveis pelas áreas / processos
- Inserir dados nas Matrizes de Gestão de Riscos Operacionais.

## **B. Matriz De Riscos E Controles**

As Matrizes de Riscos e Controles foram construídas de acordo com as características e peculiaridades da instituição.

A estrutura das matrizes foi projetada para visualizar as informações consolidadas de acordo com as necessidades da empresa (Empresa, Ciclo, Produto/Processo, etc.), entre elas:

- Tipos de riscos existentes
- Graus de impacto nos negócios;
- Probabilidades de ocorrência dos riscos;
- Tipos de controles existentes;
- Responsáveis pela execução dos controles;
- Graus de eficiência/eficácia dos controles, etc.

Além disso, cada Matriz (produto / processo / etapa / área / etc.) apresenta um indicador de risco, que chamamos de Risco Líquido. O Risco Líquido é o risco residual que pode ser simplificado no conceito abaixo:

<b>RISCO LÍQUIDO = RISCO BRUTO – CONTROLE</b>
---

As matrizes são reavaliadas semestralmente, sendo emitidos os seguintes tipos de relatórios:

- Evolução dos riscos e controles no tempo (semestral - histórico)
  - Quantidade de riscos e controles mapeados
  - Consolidação das Matrizes
  - As áreas e processos de maior exposição ao risco.
-

### **C. Documentação/Compliance**

A documentação dos processos tem como principais objetivos, dentro da estrutura de controles:

- Centralizar as diversas informações sobre os processos numa base única de fácil acesso / consulta / atualização;
- Permitir aos funcionários um melhor entendimento dos processos;
- Estabelecer padrões para documentação com visão corporativa.

Para todos os procedimentos serão gerados manuais, e também faz parte deste segmento e tem como objetivo detalhar os procedimentos adotados para execução das atividades ou de prestação de serviços dentro de cada área de negócios.

As documentações que inicialmente estarão contidas nesta base serão:

- Organograma
- Descrição das atividades e processos
- Fluxo básico dos processos
- Manual interno dos procedimentos da área

Essas documentações deverão ser constantemente avaliadas e alteradas na inclusão, alteração ou exclusão de funcionários, processos e procedimentos.

### **4. PLANOS DE AÇÃO E MELHORIAS**

A base de dados "Plano de Ação" ou "Follow Up" terá a finalidade de registrar e monitorar os diversos planos de ação de melhorias da Gestão de Controles Internos, gerados de relatórios de recomendações de auditorias internas e externas, órgãos fiscalizadores (Banco Central, CVM, etc.)

A base terá informações como:

- Origem (área / processo / produto / órgão)
  - Aspecto a ser melhorado (ponto / item / vulnerabilidade)
  - Área Responsável pela melhoria
  - Responsável
  - Cargo do responsável
  - Descrição do Plano
  - Data de implantação
-

A Gestão de Risco Operacional irá gerenciar, através de envio de e-mails, as datas prometidas de implantação, com cobranças aos responsáveis e com ciência de seus superiores de acordo com pré-configuração do sistema.

Também permitirá postergações de datas, sempre com justificativa, e deverá ser alimentado pelo agente de *Compliance* da área na sua implantação.

## **5. CRONOGRAMA DE ATIVIDADES**

## **6. ATIVIDADES COMPLEMENTARES**

### **A. Programas de Compliance**

#### **▪ Objetivo**

Estes programas são elaborados para assegurar a conformidade entre as atividades, produtos e serviços da empresa e as normas legais e regulamentares a eles aplicáveis, garantindo o seu cumprimento. Com o objetivo de avaliar a aderência à legislação e às normas internas, as mesmas são acompanhadas e verificadas sistematicamente por meio dos Programas de *Compliance*.

#### **▪ Composição**

Formados por questionários com assertivas relacionadas a circulares, manuais ou leis, abrangendo também práticas de gestão e usos e costumes. Os questionários são elaborados pelos gestores e agentes de *Compliance* e corporativamente pelo *Compliance*.

- Há diversos questionários na nossa base de dados, onde para cada área existirá um conjunto específico que programas. Cada Programa terá um período ou uma data definida para ser aplicado, que será gerenciado pelo sistema, através de um sistema de agenda com envio automático de e-mail aos aplicadores de programa.
- A Gestão de Risco Operacional, através das matrizes, também gerenciará a aplicação dos Programas, avisando ao Diretor responsável da área, com cópia ao *Compliance Officer*, dos atrasos e não validação dos itens.

### **B. DICIONÁRIO DE RISCOS**

---

Os riscos de natureza interna e externa devem ser identificados e avaliados, porque podem impedir ou ameaçar o alcance de objetivos de negócio da organização. Essas ações devem ser contínuas, abrangendo:

- Identificação, análise e catalogação dos riscos;
- Medição do impacto nos objetivos de negócios ou serviços;
- Gerenciamento e acompanhamento dos riscos;
- Dimensionamento dos controles necessários;
- Análise do conforto em relação ao risco residual.

Para auxiliar os agentes de *Compliance* no gerenciamento de seus riscos e para a adequada identificação, catalogação e avaliação dos riscos é necessário que a instituição padronize uma conceituação dos riscos.

O Dicionário de Riscos será apresentado em formato de texto, onde existe a definição de cada risco, subtipos e exemplificação.