

## Procedimentos de Gerenciamento do Risco Operacional

### Resumo

Descreve os conceitos e procedimentos de gerenciamento do risco operacional

### Sumário

1. Objetivo.....	2
2. Público-alvo .....	2
3. Conceitos Gerais .....	2
3.1. Ferramenta utilizada para Gestão do Risco Operacional .....	2
3.2. Indicador-chave de Risco ou KRI (Key Risk Indicator) .....	2
3.3. Apontamentos.....	2
3.4. Ocorrências.....	2
3.5. Dicionário de Riscos .....	2
3.6. Tipo de Ação.....	2
3.7. Tipo de Causa.....	2
3.8. Apetite ao Risco.....	3
3.9. Tipos de Controle.....	3
3.10. Característica do Controle .....	3
3.11. Testes dos Controles .....	3
3.12. Avaliação de Riscos.....	4
3.13. Matriz de Riscos e Controles .....	4
3.14. Risco Bruto .....	4
3.15. Risco Residual .....	4
3.16. “Heat-map” das ocorrências e apontamentos das áreas .....	4
4. Processos de Gestão do Risco Operacional .....	5
4.1. Principais envolvimento no evento de Risco Operacional.....	5
4.2. Mapa de Processos .....	5
4.3. Identificação dos Riscos Operacionais .....	5
4.4. Análise dos riscos .....	6
4.5. Avaliação dos riscos .....	6
4.6. Tratamento do risco .....	6
4.7. Monitoramento e Análise Crítica .....	7
4.8. Comunicação e Consulta.....	8
5. Matriz RACI.....	8
6. Referência cruzada com outros Instrumentos Normativos Internos.....	8
7. Alinhamento com Órgãos Reguladores e Legislações .....	9
8. Informações de Controle.....	9

## Procedimentos de Gerenciamento do Risco Operacional

### 1. Objetivo

Descrever os conceitos e procedimentos de gerenciamento do risco operacional.

### 2. Público-alvo

Empresas financeiras do Grupo Paulista (PAULISTA).

### 3. Conceitos Gerais

#### 3.1. Ferramenta utilizada para Gestão do Risco Operacional

O Sistema OpAdvanced é a ferramenta corporativa para registro das ocorrências de erros operacionais e acompanhamento dos planos de ação para sua mitigação.

As instruções para sua utilização estão descritas no Anexo **SCI-03.A** - Manual de Operação do Sistema OpAdvanced.

#### 3.2. Indicador-chave de Risco ou KRI (Key Risk Indicator)

v. **SCI-01** – Sistema de Controles Internos do Conglomerado Paulista, item 3.4

#### 3.3. Apontamentos

v. **SCI-01** – Sistema de Controles Internos do Conglomerado Paulista, item 3.6

#### 3.4. Ocorrências

v. **SCI-01** – Sistema de Controles Internos do Conglomerado Paulista, item 3.7.

#### 3.5. Dicionário de Riscos

O Dicionário de Riscos é o padrão para a classificação e constituição de uma base de dados para o gerenciamento e entendimento das vulnerabilidades.

O Dicionário de Riscos está definido em três níveis hierárquicos (v. Anexo SCI-03.B – Dicionário de Riscos):

- Categoria
- Evento
- Tipo

#### 3.6. Tipo de Ação

No registro do Plano de Ação, são utilizadas as seguintes classificações para a mitigação do risco:

Tipo de ação	Descrição
Normatização	Criar normas e procedimentos para atenuar o risco.
Automação	Automatizar o processo para reduzir o risco.
Recomendação	Recomendar melhoria do processo.
Treinamento	Capacitar a equipe.
Coleta de Informações/Documento	Gerar evidências para a efetividade do controle.

#### 3.7. Tipo de Causa

Os motivos da causa que originaram uma perda esperada ou inesperada no processo podem ser:

- Falta de segregação de função
- Falta de treinamento
- Desconhecimento da norma
- Falta de divulgação de normas, políticas e lei

## Procedimentos de Gerenciamento do Risco Operacional

- Inexistência de norma ou política
- Norma não cumprida
- Controle inexistente
- Controle mal executado
- Processo não definido
- Processo mal desenhado
- Infraestrutura deficiente, insuficiente ou inexistente

### 3.8. Appetite ao Risco

A estratégia adotada pela instituição em relação ao risco identificado pode ser:

Estratégia	Descrição
Gerenciar	Identificar meios para que o risco seja reduzido.
Assumir	Correr o risco por ser inerente ao modelo de negócio.
Transferir	Identificar meios para que o risco possa ser transferido para terceiros.
Evitar	Tomar ações para eliminar completamente todos os elementos de exposição a um risco específico.

### 3.9. Tipos de Controle

Os controles internos para mitigar o risco da instituição podem ser classificados como:

Tipos de Controles	Descrição
Conciliação	Consiste no confronto de informações de origens distintas, com o objetivo de detectar inconsistências.
Autorizações	Buscam permitir o encaminhamento de uma operação/transação após conferência.
Acesso Lógico	Busca o controle de acesso/alcance de funcionários e/ou clientes a arquivos eletrônicos e sistemas computacionais.
Alçadas e Limites	Atuação ou influência de um gestor, quanto a sua condição de aprovar valores ou assumir posições em nome da instituição.
Acesso Físico	Consiste no controle da entrada/saída de funcionários, clientes e/ou equipamentos em determinadas áreas da instituição.
Normatização Interna	Compreende o estabelecimento formal de normas internas, para a execução das atividades inerentes à unidade.
Segregação de Funções	Envolve a separação das responsabilidades sobre atividades conflitantes, por meio de organograma ou estabelecimento de regras.

### 3.10. Característica do Controle

As características dos controles internos são classificadas como:

Classificação	Descrição
Manual	controle em que uma parte significativa depende de intervenção manual.
Automático	controle executado de forma automática por sistemas informatizados.
Detectivo	controles que visam à identificação da ocorrência do erro operacional.
Preventivo	controles que visam evitar a ocorrência do erro operacional.

### 3.11. Testes dos Controles

O plano de teste dos controles leva em consideração o período de execução do controle e a quantidade de amostras necessárias para avaliação da qualidade do controle no processo, conforme segue:

Frequência do controle	Qtd. amostras de execução
Anual	1
Semestral	2

## Procedimentos de Gerenciamento do Risco Operacional

Frequência do controle	Qtd. amostras de execução
Trimestral	2
Mensal	4
Quinzenal	6
Semanal	12
Diário	24
Eventual	2

### 3.12. Avaliação de Riscos

Ferramenta utilizada para avaliar os riscos do processo, que leva em consideração a probabilidade de ocorrência *versus* a consequência, relacionado quantitativamente à perda financeira.

Classificação da Probabilidade:

Probabilidade	Descrição
Quase Certa	Uma vez por semana
Muito Frequente	Uma vez ao mês
Frequente	Uma vez no trimestre
Rara	Uma vez ao ano
Muito Rara	Uma vez a cada 5 anos

Classificação da Consequência (valor da perda):

Classificação	Valor da perda
Irrelevante	Menor que R\$ 21.000,00
Baixa	Entre R\$ 21.000,00 e R\$ 29.999,99
Média	Entre R\$ 30.000,00 a R\$ 89.999,99
Alta	Entre R\$ 90.000,00 a R\$ 149.999,99
Crítico	Maior que R\$ 150.000,00

### 3.13. Matriz de Riscos e Controles

Ferramenta utilizada para avaliação dos processos operacionais, identificando os riscos associados e os controles internos implementados para sua mitigação.

### 3.14. Risco Bruto

Avaliação do risco no processo, sem considerar os controles implementados.

### 3.15. Risco Residual

Avaliação do risco no processo, considerando a implementação de controles para sua mitigação.

### 3.16. “Heat-map” das ocorrências e apontamentos das áreas

Gráfico de acompanhamento dos registros de ocorrências e apontamentos por área, ponderando-se sua gravidade e quantidade.

São utilizados os seguintes critérios para sua elaboração:

- Quantidade de registros por área
- Criticidade da Origem conforme tabela abaixo:

Origem	Peso
Regulador/Fiscalizador	6
Auditoria Externa	5
Auditoria Interna – Risco Alto	4

## Procedimentos de Gerenciamento do Risco Operacional

Origem	Peso
Auditoria Interna – Risco Médio	3
Auditoria Interna – Risco Baixo	2
Ocorrência Interna	1

### 4. Processos de Gestão do Risco Operacional

#### 4.1. Principais envolvimento no evento de Risco Operacional

**Área Impactada:** Unidade Organizacional que tem suas atividades prejudicadas por um evento de Risco Operacional.

**Área Responsável:** Unidade Organizacional que possui a atribuição de operacionalizar o plano de ação para mitigação do evento de Risco Operacional.

#### 4.2. Mapa de Processos

O Mapa de Processos do Grupo Paulista está organizado em 4 macroprocessos (nível 1, listados a seguir), que se subdividem em processos (nível 2), que por sua vez, agrupam os sub-processos (nível 3) e podem ser desdobrados em atividades (nível 4). Cada área gestora é responsável pelo detalhamento e manutenção dos processos a partir do nível 2, alinhado à necessidade de estabelecimento de controles. (v. Anexo SCI-03.C – Mapa de processos do Grupo Paulista)

1. Front-Office
2. Back-Office
3. Controle
4. Suporte

#### 4.3. Identificação dos Riscos Operacionais

A identificação dos riscos operacionais considera os apontamentos realizados pelas auditorias interna e externa e pelos órgãos reguladores. Também são consideradas as ocorrências de erro operacional registradas pelos gestores dos processos e as variações identificadas pelos processos de monitoramento de indicadores-chave de riscos (KRI).

Os indicadores-chave de riscos atualmente acompanhados são:

- Operações day-trade
- Reespecificação de operações
- Negócios Diretos
- Suitability de investidores
- Análise de PLD
- Atualização cadastral
- Limites na execução de ordens (GTS e Mega Bolsa)
- Transmissão de ordens
- Operações realizadas por analistas de investimento
- Movimentação da Conta Erro – Mesa Socopa
- Multas decorrentes de notificações de órgãos reguladores e fiscalizadores
- Não-conformidades dos programas de compliance (v. **SCI-05** – Procedimentos dos Programas de Compliance)
- Perdas operacionais registradas pela contabilidade (v. **item 4.2.1**)

##### 4.3.1. Perdas Operacionais

As perdas operacionais decorrentes nas falhas de processo são capturadas a partir das seguintes contas COSIF classificadas com essa finalidade:

## Procedimentos de Gerenciamento do Risco Operacional

Conta Contábil – Banco Paulista	Descrição
8.1.7.69.00.01.03-9	TRIBUTOS-FEDERAIS-OUTROS
8.1.7.69.00.04.02-9	MULTAS - OUTRAS
8.1.7.77.00.00.01-7	DESP. MULTAS APLIC. P/ BCO.CENTRAL
8.1.8.30.99.00.04-6	PROV.PERDAS-CLIENTES
8.1.9.99.00.01.28-5	DESP.CLIENTES CDC
8.1.9.99.00.01.78-0	OUTRAS
8.1.9.99.00.01.40-7	DESP. FINANCERIA DEFICIENCIA NA RESERVA

Conta Contabil – Socopa	Descrição
8.1.7.54.05	Multas / Dif. E Erro Operacional
8.1.7.69.05	Despesas Indedutíveis
8.1.7.69.09	Outros Tributos
8.1.7.77	Multas Aplicadas Pelo BC
8.1.9.99.00.00002	Perdas

### 4.4. Análise dos riscos

Para cada registro no sistema informatizado para acompanhamento e controle do risco operacional, são identificados os processos associados, a gravidade e a probabilidade de reincidência, sendo mensurado, quando possível, o valor das perdas. Também são identificadas as principais causas e fontes de risco, bem como os indicadores para acompanhamento estruturado, que visam identificar:

- Recorrências
- Localização (processo e unidade organizacional)
- Responsabilidade (responsável pelo plano de ação)
- Causas
- Efetividade dos Planos de Ação

### 4.5. Avaliação dos riscos

Para os apontamentos, sua resolução é mandatória, dentro dos prazos acordados com as auditorias e órgãos reguladores. No caso das ocorrências, em função da gravidade e da probabilidade de reincidência, é avaliada a urgência e prioridade da solução.

Para a avaliação são utilizadas a Tabela de Avaliação do Risco e as Matrizes de Riscos e Controles do processo em questão.

### 4.6. Tratamento do risco

Após avaliação e priorização da solução, são definidos Planos de Ação com identificação da Área Responsável e prazos. Toda ocorrência ou apontamento obrigatoriamente possuem **pelo menos um** Plano de Ação, que são registrados em sistema informatizado para acompanhamento e controle, conforme **item 4.5.1**.

#### 4.6.1. Procedimentos para Registro da Ocorrência/Apontamento e respectivos Planos de Ação

## Procedimentos de Gerenciamento do Risco Operacional

### Menu – Apontamento

Campo	Conteúdo
Selecionar a Estrutura	Processo
Nome do Trabalho (Origem)	Bacen, CVM, Anbima, BSM, Cetip
Identificação da Irregularidade	
Prioridade	Nível de Criticidade
Responsável pelo Processo	Diretor/Superintendente/Gerente da Área Impactada
Atribuído	Agente de Compliance do Processo da Área Impactada
Recomendação do Regulador ou Fiscalizador	[texto]
Data de Previsão de Regularização	[data válida]
Data Efetiva de Conclusão da Regularização	[data válida]

### Menu – Ocorrência

- Data da Ocorrência
- Data da Identificação
- Identificação da Ocorrência
- Atribuído – Agente de Compliance do Processo – área impactada
- Responsável (Diretor/Superintendente/Gerente) pelo Processo – área Impactada

### Menu - Plano de Ação

- Identificar Plano de Ação
- Tipo de Ação (item 3.6)
- Status da Ação
- Responsável (Diretor/Superintendente/Gerente) do executor pelo plano de ação –

#### Área Responsável

- Atribuído – executor do plano de ação - Área Responsável
- Início Previsto
- Início Efetivo
- Conclusão Prevista do Plano de Ação
- Conclusão Efetiva do Plano de Ação
- Eficiência – Ponto de Melhoria
- Descrição da Ação

### Menu - Arquivo

- Guarda das evidências

## 4.7. Monitoramento e Análise Crítica

O processo de monitoramento e análise crítica visa a garantir que os controles internos estão implantados e que são adequados para as atividades da instituição. O monitoramento também avalia os níveis de exposição ao risco definidos pela administração. Para o monitoramento são realizados:

- Follow-ups periódicos (acompanhamento da execução dos Planos de Ação pelas Áreas Responsáveis).
- Análises de tendências (“heat-map” das ocorrências e apontamentos das Áreas Impactadas).
- Gráficos de indicadores.

As alterações relativas às unidades de negócios e ao ambiente no qual se inserem são identificadas para que sejam efetuadas as adaptações necessárias e seja identificado se as medidas adotadas alcançaram os resultados esperados.

## Procedimentos de Gerenciamento do Risco Operacional

### 4.8. Comunicação e Consulta

As informações internas e externas relacionadas ao risco operacional são comunicadas de forma sistemática nos níveis vertical (Comitê GRC, grupos de trabalho e diretorias) e horizontal (colaboradores e participantes de processos compartilhados), considerando-se graus diferentes de detalhamento da informação, que variam em função da abrangência de atuação. São utilizados de forma periódica os seguintes instrumentos de comunicação corporativa:

- Boletins Normativos.
- Reuniões do Comitê GRC.

### 5. Matriz RACI

A **matriz RACI** apresenta a relação entre papéis desempenhados e atividades e/ou artefatos a serem entregues. RACI é o acrônimo (em inglês) para:

**Responsible** (responsável): É efetivamente quem trabalha na atividade.

**Accountable** (aprovador): É o papel do responsável pelo aceite formal da tarefa ou produto entregue. Este pode delegar a função para outros profissionais, entretanto ele é quem se responsabiliza pelo recebimento do trabalho.

**Consulted** (consultado): é o responsável por fornecer informações ou pareceres sobre a tarefa ou produto a ser entregue.

**Informed** (informado): é quem necessita ser mantido informado sobre o andamento da atividade.

MATRIZ RACI (legenda)		Comitê GRC	Compliance Corporativo	Auditoria Externa	Auditoria Interna	Diretorias	Gestores	Agentes de Compliance
	<b>Responsible</b> (responsável)							
	<b>Accountable</b> (aprovador)							
	<b>Consulted</b> (consultado)							
	<b>Informed</b> (informado)							
Ref.	Procedimento	Intervenientes						
4.1	Mapa de Processo	A	R			C	C	C
4.2	Identificação dos Riscos Operacionais	I	R	R	R	I	R	R
4.3	Análise dos Riscos	I	R	C	C	I	C	C
4.4	Avaliação dos Riscos	I	R	C	C	I	C	C
4.5	Tratamento dos Riscos	I	A	A	A	A	R	R
4.6	Monitoramento e análise crítica	I	R	I	I	I	C	C

### 6. Referência cruzada com outros Instrumentos Normativos Internos

- GRC-02 - Estruturas de Governança do Grupo Paulista
- GRC-03 – Política Geral de Gerenciamento e Controle de Riscos
- GRC-04 – Política de Gerenciamento do Risco Operacional
- SCI-01 – Sistema de Controles Internos do Grupo Paulista
- SCI-03.A - Manual de Operação do Sistema OpAdvanced
- SCI-03.B – Dicionário de Riscos
- SCI-03.C – Mapa de processos do Grupo Paulista
- SCI-05 – Procedimentos dos Programas de Compliance



## Procedimentos de Gerenciamento do Risco Operacional

### 7. Alinhamento com Órgãos Reguladores e Legislações

**Resolução CMN 2554/1998:** Dispõe sobre a implantação e implementação de sistema de controles internos.

**Circular BCB 3380/2006:** Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional.

**Circular BCB 3467/2009:** Estabelece critérios para elaboração dos relatórios de avaliação da qualidade e adequação do sistema de controles internos e de descumprimento de dispositivos legais e regulamentares e dá outras providências.

**Instrução CVM 505/2011:** Estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.

### 8. Informações de Controle

Vigência: Até 11.nov.2017

#### Registro das alterações:

Versão	Item alterado	Descrição resumida da alteração	Motivo	Dt.Publicação
01	Não se aplica	Não se aplica	1ª. versão	31.dez.2013
02	4.1 4.3.1	Inclusão do conceito: área impactada e área responsável Inclusão dos procedimentos de monitoramento das perdas operacionais.	Aprimoramento	27.nov.2014
03	2	Atualização do Público-Alvo	Atualização	11.nov.2016

#### Responsáveis pelo Instrumento Normativo:

Etapa	Responsável	Contato / Ramal	Unid.Organizacional
Elaboração	Marcus Vinicius Sannino	<a href="mailto:marcus.sanino@bancopaulista.com.br">marcus.sanino@bancopaulista.com.br</a>	Compliance Corporativo
Revisão	Nelson Heleno	<a href="mailto:nelson.heleno@bancopaulista.com.br">nelson.heleno@bancopaulista.com.br</a>	Compliance Corporativo
	Nelson Geraldo	<a href="mailto:nelson.geraldo@bancopaulista.com.br">nelson.geraldo@bancopaulista.com.br</a>	Compliance Corporativo
	Denilson Santos	<a href="mailto:denilson.santos@bancopaulista.com.br">denilson.santos@bancopaulista.com.br</a>	Compliance Corporativo
Aprovação	Eduardo Kuniyoshi	<a href="mailto:eduardo.kuniyoshi@bancopaulista.com.br">eduardo.kuniyoshi@bancopaulista.com.br</a>	Compliance Corporativo

**Compliance Corporativo**