

MARIANA FIORIN FERNANDEZ

**SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO  
OPERACIONAL**

Trabalho de formatura apresentado à  
Escola Politécnica da Universidade de São  
Paulo para obtenção do diploma de  
Engenheiro de Produção.

SÃO PAULO

2011

MARIANA FIORIN FERNANDEZ

**SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO  
OPERACIONAL**

Trabalho de Formatura apresentado à  
Escola Politécnica da Universidade de São  
Paulo para obtenção do diploma de  
Engenheiro de Produção.

Orientador:

Mauro de Mesquita Spinola

SÃO PAULO

2011

## **FICHA CATALOGRÁFICA**

**Fernandez, Mariana Fiorin**

**Sistema de informação para gestão de risco operacional /  
M.F. Fernandez. -- São Paulo, 2011.  
112 p.**

**Trabalho de Formatura - Escola Politécnica da Universidade  
de São Paulo. Departamento de Engenharia de Produção.**

**1. Sistema de informação 2. Gestão de risco operacional  
I. Universidade de São Paulo. Escola Politécnica. Departamento  
de Engenharia de Produção II. t.**

## **DEDICATÓRIA**

Dedico esse presente trabalho à minha família: meus pais, minha irmã, meus primos e amigos, que sempre me auxiliaram a superar todas as dificuldades e desafios e me propiciaram amor incondicional. Em especial ao meu pai, meu exemplo, que me incentivou a seguir essa carreira e me auxiliou no desenvolvimento desse trabalho, e à minha mãe, que sempre esteve ao meu lado, e me aturou nos bons e maus momentos.

## **AGRADECIMENTOS**

Agradeço primeiramente aos meus pais, que me propiciaram a melhor educação que alguém poderia ter.

Ao meu pai, sem o qual eu não teria seguido a carreira de engenharia.

À minha mãe, que me apoiou em todos os momentos difíceis, começando pelo meu nascimento prematuro.

À minha irmã coruja, sem a qual eu não seria a mesma.

Ao meu professor orientador, Mauro Spinola, pelo apoio e instruções durante o ano inteiro, que contribuíram para que o trabalho evoluísse.

Ao meu amigo Bruno Lunardi, sem o qual eu não teria aprendido tão rapidamente a utilizar o Microsoft Access.

Aos meus colegas de trabalho, Marcelo Oseas, Vanessa Cardoso Amorim e Christiane Sanchez, que compartilharam seus conhecimentos e experiências e me incentivaram durante todo o tempo de estágio.

De toda maneira, gostaria de agradecer a todos que me auxiliaram, não apenas no desenvolvimento do presente trabalho, como também para que o meu último ano não se tornasse estressante.

## **RESUMO**

O risco operacional constitui hoje um assunto de grande importância para o sistema financeiro. Seu bom gerenciamento possibilita a sobrevivência das instituições financeiras e restabelece a confiança dos investidores. O objetivo deste trabalho é apresentar o desenvolvimento de um sistema de informação, para a gestão de risco operacional numa instituição financeira. Na empresa estudada, o mapeamento desse tipo de risco era realizado com apoio de uma ferramenta que apresentava diversas limitações e não se adequava às necessidades dos usuários. Para atingir o objetivo proposto, foram elaborados, juntamente com os responsáveis pelo mapeamento de risco, os requisitos funcionais e não funcionais para o desenvolvimento do novo programa. O sistema foi modelado, implementado e disponibilizado em duas etapas: primeiramente numa versão para testes e em seguida numa versão de produção, após a adaptação dos usuários à nova metodologia. Mesmo com algumas limitações do programa e do conhecimento técnico dos programadores, o sistema foi bem avaliado pelos usuários e contribuiu para um melhor gerenciamento dos riscos operacionais da empresa.

Palavras-chave: risco operacional, gestão de risco operacional, Sistema de Informação.

## **ABSTRACT**

Operational risk is, presently, a subject of great importance to the financial system. Proper management enables the survival of financial institutions and restores investors' confidence. The objective of this paper is to present the development of an information system for managing operational risk, in a financial institution. In the company observed, the mapping of this type of risk was done using a tool that had several limitations and did not fit users' needs. To achieve this goal, the functional and nonfunctional requirements for the development of the new program were gathered, with the help of those responsible for risk mapping. The system was modeled, implemented and made available in two phases: first in a trial version and then in production as the users adapted to the new methodology. Despite some limitations of the program and lack of expertise of programmers, the system was well evaluated by users and contributed to a better management of the company's operational risks.

**Keywords:** operational risk, operational risk management, information system.

## LISTA DE ILUSTRAÇÕES

Figura 1 - Comitê Operacional de Risco.....	31
Figura 2 - Níveis de risco operacional.....	34
Figura 3 - Etapas da Metodologia de Identificação de Risco Operacional .....	36
Figura 4 - Listagem de causas por subprocesso no programa antigo .....	37
Figura 5 - Listagem de causas por subprocesso no programa atual .....	38
Figura 6 - Cadastro de causas no programa antigo.....	38
Figura 7 - Cadastro de ambiente de controle no programa antigo .....	38
Figura 8 - Vínculo entre ambiente de controle e causas do risco no programa antigo .....	39
Figura 9 - Estrutura de Riscos da empresa.....	42
Figura 10 - Diagrama de Casos de Uso .....	45
Figura 11 - Tabela Mapeamento de Risco e relacionamentos.....	55
Figura 12 - Tabela Área e relacionamentos.....	57
Figura 13 - Tabela Mapeamento de Causas e relacionamentos.....	58
Figura 14 - Tabela Ambiente de Controle: Causas Mitigadas e relacionamentos.....	59
Figura 15 - Tabela Avaliação de Risco e relacionamentos.....	60
Figura 16 - Tabela Planos de Ação: Causas Mitigadas e relacionamentos .....	61
Figura 17 - Tabelas do sistema e seus relacionamentos .....	63
Figura 18 - Menu Principal.....	66
Figura 19 - Cadastro de Mapeamento de Risco .....	68
Figura 20 - Seleção da Área.....	69
Figura 21 - Cadastro de Risco .....	70
Figura 22 - Árvore de Decisão .....	70
Figura 23 - Editar risco .....	71
Figura 24 - Regra de Alteração entre Status.....	71
Figura 25 - Cancelamento de Mapeamento de Risco .....	72
Figura 26 - Justificativa cancelamento do mapeamento.....	72
Figura 27 - Salvar mapeamento.....	73



Figura 28 - Seleção do mapeamento.....	73
Figura 29 - Mapeamento de Causas.....	74
Figura 30 - Cadastro de causa detalhada .....	75
Figura 31 - Edição de causa detalhada .....	75
Figura 32 - Cadastro do ambiente de controle .....	76
Figura 33 - Seleção do componente do ambiente de controle .....	77
Figura 34 - Vínculos entre ambientes de controle e causas - Adicionar mitigador.....	78
Figura 35 - Vincular ambiente de controle .....	79
Figura 36 - Vínculos entre ambientes de controle e causas.....	80
Figura 37 - desvincular ambiente de controle .....	81
Figura 38 - Cadastro de plano de ação .....	82
Figura 39 - Seleção do plano de ação .....	84
Figura 40 - Cadastro de plano de ação .....	85
Figura 41 - Alteração no plano de ação.....	86
Figura 42 - Imprimir alterações do plano de ação .....	86
Figura 43 - Vínculos entre planos de ação e causas .....	87
Figura 44 - Vincular plano de ação .....	88
Figura 45 - Desvincular plano de ação.....	88
Figura 46 - Relatório de Riscos e Causas .....	91
Figura 47 - Relatório Apresentação .....	92
Figura 48 - Tabelas Resumo: Status dos ambientes de controle .....	93
Figura 49 - Tabelas Resumo: Características dos ambientes de controle.....	94
Figura 50 - Tabelas Resumo: Tipos de planos de ação.....	94
Figura 51 - Tabelas Resumo: Nível do Risco por Cenário.....	95
Figura 52 - Login no Acesso via Citrix.....	99
Figura 53 - Conexão no Acesso via Citrix.....	99

## **LISTA DE QUADROS**

Quadro 1 - Basileia I: Fator de ponderação de ativos .....	19
Quadro 2 - Alguns Normativos de Basileia I .....	25
Quadro 3 - Casos de Uso do novo sistema.....	44

## **LISTA DE EQUAÇÕES**

Equação 1 - Cálculo do $P_{OPR}$ na Abordagem do Indicador Básico .....	26
Equação 2 - Cálculo do $P_{OPR}$ na Abordagem Padronizada Alternativa.....	27
Equação 3 - Cálculo do $P_{OPR}$ na Abordagem Padronizada Alternativa Simplificada .....	27

## **LISTA DE ABREVIATURAS E SIGLAS**

BCBS	Basel Committee on Banking Supervision
BIS	The Bank for International Settlements
COSO	Committee of Sponsoring Organizations of the Treadway
Commission	
GRO	Gestão de Risco Operacional
RO	Risco Operacional
UML	Unified Modeling Language

## SUMÁRIO

<b>I</b>	<b>INTRODUÇÃO.....</b>	<b>15</b>
I.1	DEFINIÇÕES DE RISCO E RISCO OPERACIONAL .....	16
I.2	GERENCIAMENTO DE RISCOS .....	17
I.3	COMITÊ DE BASILEIA .....	18
I.4	BASILEIA I.....	18
I.5	EXEMPLOS DE PERDAS .....	20
I.6	BASILEIA II .....	22
I.7	BASILEIA III .....	27
<b>II</b>	<b>RISCO OPERACIONAL NA EMPRESA .....</b>	<b>30</b>
II.1	METODOLOGIA DE RISCO OPERACIONAL UTILIZADA .....	33
II.2	SISTEMA DE INFORMAÇÃO UTILIZADO .....	36
<b>III</b>	<b>REQUISITOS DE UM NOVO SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL.....</b>	<b>41</b>
III.1	TIPOS DE REQUISITOS.....	41
III.2	REQUISITOS FUNCIONAIS.....	42
III.3	REQUISITOS NÃO FUNCIONAIS .....	50
III.4	BENEFÍCIOS E LIMITAÇÕES.....	51
<b>IV</b>	<b>DESENVOLVIMENTO .....</b>	<b>55</b>
<b>V</b>	<b>IMPLANTAÇÃO DO SISTEMA.....</b>	<b>64</b>
<b>VI</b>	<b>NAVEGAÇÃO NO PROGRAMA .....</b>	<b>66</b>
VI.1	MENU PRINCIPAL .....	66
VI.2	MAPEAMENTO DE RISCOS E CAUSAS.....	68
VI.3	AMBIENTE DE CONTROLE E SEGUROS.....	76
VI.4	PLANOS DE AÇÃO .....	82
VI.5	MATRIZ DE RISCOS .....	89
VI.6	RELATÓRIOS.....	91

VI.7	ALTERAÇÕES NA FERRAMENTA .....	96
<b>VII</b>	<b>TREINAMENTO.....</b>	<b>97</b>
	MANUAL DO USUÁRIO.....	97
<b>VIII</b>	<b>PROBLEMAS ENCONTRADOS.....</b>	<b>101</b>
<b>IX</b>	<b>CONCLUSÃO .....</b>	<b>105</b>
<b>X</b>	<b>REFERÊNCIAS .....</b>	<b>109</b>

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### I INTRODUÇÃO

O sistema financeiro é essencial para o funcionamento e bom desempenho da economia. Por isso, é um dos setores mais regulados do mundo, e exige que as instituições gerenciem seus riscos.

Há alguns anos, o risco operacional (RO) não era visto como relevante, como os riscos de mercado e crédito. Porém, muitos eventos ocorridos a partir da década de 90 evidenciaram sua importância, culminando na elaboração do Novo Acordo de Capital, que introduziu o gerenciamento de risco operacional e o capital mínimo necessário para cobri-lo.

Na empresa estudada neste trabalho, o mapeamento e o gerenciamento de RO eram realizados através de um sistema, que apresentava diversas limitações, como falta de extração de dados e lentidão, e, assim, não atendia aos requisitos dos funcionários da área.

Por esses motivos, foi decidido que um novo programa para a gestão de RO seria criado internamente. Coube à autora desenvolver uma versão para esse programa, que se tornou o objeto deste Trabalho de Formatura.

A empresa para a qual foi criado o programa é um dos maiores bancos de capital privado do Brasil. Atua em diversos segmentos, como financiamento ao consumo, *corporate banking*, mercado de capitais, corretora, tesouraria, área internacional e gerenciamento de recursos de terceiros.

O trabalho está estruturado em nove capítulos.

No primeiro capítulo, analisa-se o significado e importância de risco e risco operacional, seu contexto internacional e os Acordos de Basileia, para que o assunto seja compreendido anteriormente à demonstração do sistema desenvolvido.

O segundo capítulo trata sobre a estrutura de risco operacional na empresa estudada, e como funciona o trabalho de gestão do mesmo.

No terceiro capítulo são apresentados os requisitos funcionais e não funcionais do sistema, levantados com base em modelos de casos de uso.

O quarto capítulo exhibe a estrutura do sistema, suas principais tabelas e relacionamentos entre si.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

O quinto capítulo trata da implantação do programa criado e os principais cuidados tomados.

O capítulo seis mostra o funcionamento do sistema, com exemplos das principais telas e formulários para facilitar o entendimento.

O capítulo sete trata do treinamento que os funcionários de mapeamento de risco realizaram para se tornarem aptos a utilizar o sistema.

O penúltimo capítulo elenca diversos problemas ocorridos após a disponibilização do sistema, com a elaboração de algumas opções para solucionar cada um. E, por fim, o Capítulo nove sumariza as principais conclusões do trabalho.

### I.1 DEFINIÇÕES DE RISCO E RISCO OPERACIONAL

Não há uma definição única para risco. Risco pode ser definido, de forma abrangente, como o potencial de eventos ou tendências continuadas causarem perdas ou flutuações em receitas futuras (MARSHALL, 2002).

De acordo com a Resolução CNS196/96, risco é a possibilidade de danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente. Já Bernstein (1998), o termo risco deriva de *riscu*, que significa ousar.

Qualquer tipo de negócio possui risco. As instituições financeiras estão sujeitas aos seguintes riscos: risco de crédito, risco país e de transferência, risco de mercado, risco de taxa de juros, risco de liquidez, risco legal, risco reputacional e risco operacional. Esses riscos devem ser identificados, monitorados e controlados (BIS, 1997).

Risco operacional, de acordo com o BACEN (2006), é definido como o risco de “perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos”.

Instituições financeiras e grandes bancos muitas vezes possuem suas próprias definições de RO (CHERNOBAI; RACHEV; FABOZZI, 2007). O Deutsche Bank (2010) definiu da seguinte maneira:

O Risco Operacional é definido como a potencial ocorrência de falhas relacionadas a pessoas, a especificações contratuais e documentações, à tecnologia, à infraestrutura e desastres, a projetos, a influências externas e relações com clientes.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Os riscos são inerentes ao negócio de qualquer instituição e a melhor maneira de lidar com eles é através de uma boa estrutura de gerenciamento de riscos, onde deve ser decidido o apetite a risco da empresa, definido como do nível de risco que a instituição está disposta a assumir: ou seja, quais riscos mitigar, evitar e aceitar.

### I.2 GERENCIAMENTO DE RISCOS

As organizações enfrentam diversos riscos, que se não forem devidamente identificados e mensurados, podem levá-las a imensos prejuízos. Por esse motivo, é importante que elas possuam áreas exclusivamente responsáveis pelo gerenciamento de riscos, com funcionários capacitados e treinados.

De acordo com Vaughan (1997), gerenciamento de risco é uma abordagem científica para lidar com os riscos puros, de maneira a antecipar possíveis perdas acidentais e implementar procedimentos que minimizem a ocorrência da perda ou o impacto financeiro que as perdas possam causar.

O gerenciamento de riscos corporativos tem como objetivo (COSO, 2007):

- Alinhar o apetite a risco e a estratégia;
- Otimizar as decisões de resposta a risco, que incluem prevenção, compartilhamento, redução e aceitação de riscos;
- Reduzir perdas não esperadas e prejuízos operacionais, através da identificação, avaliação e respostas aos riscos;
- Identificar e administrar os riscos inerentes aos empreendimentos, além de entender os impactos inter-relacionados;
- Fornecer soluções integradas aos diversos riscos;
- Aproveitar as oportunidades;
- Alocar eficientemente o capital investido.

Um bom gerenciamento de riscos corporativos auxilia a empresa no alcance dos seus objetivos (COSO, 2007).

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### I.3 COMITÊ DE BASILEIA

Em maio de 1930 foi fundado o Banco de Compensações Internacionais (*The Bank for International Settlements* - BIS) após o Acordo de Haia, no âmbito do Plano Young, que lidava com as reparações de guerra impostas à Alemanha pelo Tratado de Versalhes. É a organização financeira internacional mais antiga do mundo e tem como objetivo a supervisão bancária e a cooperação monetária e financeira entre os bancos centrais e instituições financeiras, além de realizar a função de banco central para os bancos centrais (BIS, 2011).

Em 1974, após diversos acontecimentos, como distúrbios da moeda internacional e mercados financeiros (como a quebra do banco *Bankhaus Herstatt*, na Alemanha), os presidentes dos bancos centrais dos países pertencentes ao Grupo dos Dez (G-10) e dirigentes do BIS, criaram o Comitê de Supervisão Bancária da Basileia (BCBS - *Basel Committee on Banking Supervision*), com responsabilidade de supervisionar e orientar as instituições financeiras dos países membros do G-10 (BCBS, 2009), visando a melhorar a qualidade e fortalecer a segurança do sistema bancário internacional. Embora o Comitê não possua formalmente autoridade para fazer com que suas recomendações sejam cumpridas, a maioria dos países membros costuma implementar suas políticas, contribuindo para um mercado financeiro internacional mais equilibrado (Banco do Brasil, 2011).

### I.4 BASILEIA I

Em 1988, foi publicado o Acordo de Capital da Basileia (*International Convergence of Capital Measurement and Capital Standards*), ou Basileia I, que definiu mecanismos para mensuração do risco de crédito e estabeleceu a exigência de padrões mínimos de requerimento de capital para fazer frente à exposição dos bancos. O foco do acordo foi o risco de crédito, considerado como o mais relevante para o sistema bancário (CHERNOBAI; RACHEV; FABOZZI, 2007; SOUZA, 2006).

De acordo com Basileia I, as instituições deveriam alocar capital em valor igual a, pelo menos, 8% do valor dos ativos ponderados pelo risco. Assim, os bancos deveriam manter capital suficiente para cada um dos instrumentos de sua carteira de ativos, de acordo com a exposição desses ativos ao risco de crédito, classificados em quatro faixas de percentuais de ponderação. Um ativo com fator de ponderação 20%, por exemplo, corresponde a uma

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

alocação de 1,6%, considerando o fator de alocação mínima de 8%, multiplicado por 20% do valor do ativo (HELOM, 2010). O **Erro! Fonte de referência não encontrada.** exibe os fatores de ponderação dos riscos conforme Basileia I.

O acordo tinha como objetivo o fortalecimento das transações bancárias e estabilidade do sistema financeiro, contando com o apoio do FMI e outras organizações para supervisionar a adoção das políticas.

**Quadro 1 - Basileia I: Fator de ponderação de ativos**

Fator	Ativos ponderados
0%	• Caixa
	• Operações com governos e bancos centrais em moeda local
	• Operações com governos membros da Organização para Cooperação e Desenvolvimento Econômico (OECD) e bancos centrais
0, 10, 20 ou 50% (a critério)	• Operações com entidades nacionais do setor público, excluindo governo central
20%	• Créditos com bancos de desenvolvimento multilaterais ou operações garantidas por esses bancos
	• Operações com bancos incorporados à OECD ou garantidas por esses bancos
	• Operações com bancos sediados em países fora da OECD, em operações com prazo de até um ano
50%	• Financiamentos imobiliários garantidos por hipoteca residencial
100%	• Operações no setor privado
	• Operações com governos não membros da OECD
	• Operações com bancos sediados em países fora da OECD com prazo superior a um ano
	• Operações com empresas comerciais do setor público
	• Ativo permanente e demais ativos
	• Bens imobiliários e outros investimentos

Fonte: Elaboração própria a partir de BCBS (1988).

Foi definido o conceito de capital, dividindo-o em duas partes: o capital básico (*core capital*) e o capital suplementar (*supplementary capital*). O primeiro, também conhecido como Nível I, é composto por capital acionário mais reservas em dinheiro publicadas em balanço (*disclosed reserves*). O segundo, também chamado de Nível II, inclui reservas em

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

dinheiro não publicadas em balanços (*undisclosed reserves*), reservas provenientes de reavaliação do valor contábil dos ativos do banco (*asset revaluation reserves*), provisão para perdas (*general provisions/general loan-loss reserves*), dívida conversível em ação (*hybrid debt/equity capital instruments*) e dívida subordinada (*subordinated debt*) (BCBS, 1988; SIVINSKI, 2010).

No Brasil, Basileia I teve início apenas em agosto de 1994, com a publicação da Resolução CMN 2.099, que definiu que as instituições brasileiras deveriam alocar capital de também no mínimo 8%. Porém, esse valor foi acrescido para 10%, através da Resolução 2.399 em Junho de 1997, e depois para 11%, através da Circular 2.784 em Novembro de 1997, que permanece atualmente (Frebaban, 2010).

O acordo sofreu diversas críticas, como, por exemplo, sua limitação de abrangência, por tratar apenas de risco de crédito, e seu método simples, onde o risco total seria apenas a soma dos riscos atribuídos para cada categoria, que considera poucos valores (0, 10, 20, 50 e 100%), perante a diversidade de operações realizadas pelos bancos (ONO, 2002). Surge, então, a necessidade de um aprimoramento do documento. Entre as melhorias, destacou-se a alocação de capital para cobertura de Riscos de Mercado, com a publicação, em 1996, da Emenda de Risco de Mercado.

Mesmo com essas alterações, o acordo apresentava diversas falhas e não se encaixava ao mercado financeiro internacional da época.

### 1.5 EXEMPLOS DE PERDAS

Neste item são citados alguns exemplos de perdas envolvendo risco operacional que ficaram famosos nacional e internacionalmente a partir de 1990.

O primeiro é o do Banco Barings, que em fevereiro de 1995, declarou falência. O banco era o mais antigo banco de investimentos do Reino Unido, fundado em 1762. Após levar lucros ao banco, Nick Leeson, visto como o operador mais promissor da instituição, foi designado operador de mercados futuros na bolsa de valores de Cingapura, a SIMEX (*Singapore International Monetary Exchange*). Ele não possuía qualquer supervisão e começou a tomar posições muito arriscadas nos derivativos. Quando o mercado tornou-se volátil, as perdas começaram a se acumular, forçando-o a aumentar suas apostas em uma tentativa de recuperá-las, pois acreditava que não estava errado, e sim, o mercado (DUARTE

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Jr., 2000). Ele criou uma conta especial secreta para manter o controle de suas perdas: a conta 88888, originalmente criada para encobrir um erro cometido por um funcionário.

Por dois anos, enganou auditores e a própria bolsa. Finalmente, o índice Nikkei caiu drasticamente após o terremoto Kobe em janeiro de 1995, e as perdas ultrapassaram US\$ 1 bilhão (CHERNOBAI; RACHEV; FABOZZI, 2007). O banco foi incapaz de sustentar a perda e anunciou falência. O caso inclusive virou o filme “A Fraude” (*Rogue Trader*) em 1999.

O primeiro grande caso de fraude contábil no Brasil ocorreu no Banco Nacional em 1996. A instituição possuía mais de 600 contas secretas, que contabilizavam empréstimos fictícios e escondiam um rombo que não parava de crescer. As operações foram realizadas por dez anos até serem descobertas pelo Banco Central. Parte da instituição foi vendida para o Unibanco e outra parte foi entregue ao Banco Central, que descobriu que a mesma estava quebrada desde 1986 (COSTA, 2008).

Em 2008, o banco Société Générale teve perdas de quase 5 bilhões de euros quando o funcionário Jérôme Kerviel realizou transações sem a autorização da empresa, criando negociações fictícias, no que ficou caracterizado como uma das maiores fraudes da história do sistema bancário.

Em 2009, o Bradesco foi condenado, em primeira instância, a pagar uma indenização de aproximadamente 1,3 milhões de reais para um ex-funcionário que alega ter sido vítima de homofobia. No mesmo ano, outro exemplo famoso de fraude financeira foi o Esquema Ponzi, realizado pelo ex-presidente da bolsa eletrônica Nasdaq, Bernard Madoff, adaptando o esquema de fraude ocorrido em 1920. Um grupo de investidores foi formado com base em uma pirâmide. Os mais antigos são remunerados com os recursos dos novos investidores que vão entrando, a quem são oferecidos grandes rentabilidades num curto prazo e que na maioria dos casos ignora o esquema fraudulento. Estima-se que as perdas totalizaram 50 bilhões de dólares, sendo esta a maior fraude de todos os tempos (LIBERATO, 2009). Em 2010, o mesmo esquema foi aplicado em Minas Gerais, pelo empresário Thales Emanuelle Maioline, que culminou em perdas de 86 milhões de reais e aproximadamente 280 ações judiciais.

Já no final de 2010, devido a fraudes contábeis realizadas pela Administração, o caso do Banco Panamericano também obteve notoriedade, com perdas de 4,3 bilhões de reais.

Esses eventos recentes têm mostrado a importância sobre a detecção e boa gestão de riscos operacionais, assunto não comentado no primeiro acordo de Basileia.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### **I.6 BASILEIA II**

Em 2004, foi assinado o Novo Acordo de Capital (Basileia II), com o objetivo de melhorar a segurança e confiabilidade no sistema financeiro internacional. O Acordo, muito mais complexo que o anterior, além de introduzir novos métodos para calcular o risco de crédito, leva em conta o risco operacional, controles internos e transparência da supervisão bancária de instituições financeiras, levando a uma gestão de risco mais refinada. Ele se fixa em três pilares:

1. Alocação de capital para cobrir Risco de Mercado, Risco de Crédito e Risco Operacional, através da determinação dos requisitos mínimos de capital para a cobertura dos riscos.

2. Processo de Revisão e Supervisão. O objetivo desse pilar é garantir que as instituições possuam processos internos sólidos de maneira a avaliar a adequação do capital, com base em uma avaliação completa dos seus riscos (ONO, 2002, p. 33, apud BCBS 2001). É composto por quatro princípios (CHERNOBAI; RACHEV; FABOZZI, 2007):

Princípio i: estabelecimento de processos para avaliar a adequação de capital em relação ao perfil de risco, e de uma estratégia para manter os níveis de capital.

Princípio ii: revisão e avaliação do gerenciamento e estratégias dos bancos com relação a adequação de capital, assim como suas habilidades para monitorar e garantir sua conformidade com os índices de capital regulatório. Os supervisores devem tomar ações apropriadas se não estiverem satisfeitos com os resultados deste processo.

Princípio iii: os supervisores devem exigir que os bancos operem acima do índice de capital mínimo e que mantenham esse nível.

Princípio iv: os supervisores devem prevenir que o capital caia abaixo do nível mínimo requerido e garantir ações rápidas de reforço caso o capital não seja mantido ou restabelecido.

3. Disciplina de Mercado e Transparência Administrativa, através da divulgação de informações qualitativas e quantitativas sobre os riscos ao mercado e ao público em geral, assegurando maior transparência sobre a situação financeira e a solvabilidade das instituições, promovendo confiança e estabilidade do setor. No caso do RO, alguns exemplos são: descrição da estrutura de capital, estratégias de gerenciamento de risco, políticas para mitigação de risco, abordagem de cálculo de capital utilizada, descrição do capital Nível I e II

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

e indicações caso o requisito de capital mínimo tenha sido excedido (CHERNOBAI; RACHEV; FABOZZI, 2007).

Basileia II não fornece uma metodologia precisa para implementar o gerenciamento de RO, e também não fornece um benchmarking para comparar as diferentes implementações pelas organizações. Mas algumas pesquisas recentes mostram uma tendência por parte das empresas em adotar a metodologia proposta pelo *Committee of Sponsoring Organizations of the Treadway Commission*, popularmente conhecido como COSO (CYRIAC, 2008).

O Banco Central é o responsável por verificar a implementação de Basileia II nas instituições financeiras, divulgando, desde 2004, regras e prazos para as adequações aos pilares.

### I.6.1 Pilar I: Alocação de Capital

A alocação mínima de capital permanece em 8%, mas Basileia II propõe um método detalhado para medir a exposição ao risco de mercado, crédito e operacional (CYRIAC, 2008).

**Risco de Crédito:** é definido como “a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas na renegociação e aos custos de recuperação” (BACEN, 2009). O Comitê de Basileia propõe dois métodos para se calcular o montante necessário para a sua cobertura: a abordagem padronizada, já abordada em Basileia I, e a baseada em classificações internas (*Internal Ratings Based – IRB*). A segunda abordagem é dividida em IRB básica e avançada, e permite a utilização de metodologias internas para o cálculo, e, por isso, requer autorização de órgãos reguladores.

**Risco de Mercado:** é definido como “a possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira” (BACEN, 2007). O Comitê incorporou à Basileia I o conteúdo da emenda de Risco de Mercado, divulgada em 1996. Possui duas abordagens, o modelo padronizado, que apresenta metodologias de cálculos específicos para cada categoria de risco (Ações, Câmbio, Commodities e Taxas de Juros) e o modelo avançado, baseado na metodologia estatística Value-at-Risk (VaR).

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Risco Operacional:** O cálculo da parcela do capital requerido pode ser feito através de quatro abordagens: Abordagem do Indicador Básico (BIA), Abordagem Padronizada Alternativa (TSA), Abordagem Padronizada Alternativa Simplificada (ASA) e Abordagem Avançada (AMA), que são explicadas mais detalhadamente.

Instituições que possuem maior exposição aos riscos devem utilizar uma metodologia mais sofisticada que a abordagem básica. É permitida a utilização de uma combinação do AMA com as outras abordagens. Porém, uma vez que a empresa adotou a abordagem mais avançada, não é permitido voltar para as mais simplificadas (CHERNOBAI; RACHEV; FABOZZI, 2007).

Assim, Basileia II possibilita as empresas criarem suas próprias metodologias para o cálculo do capital requerido para se fazer a cobertura dos riscos operacionais, de crédito e de mercado, que podem então ser aproveitadas para outros riscos, como também para reduzir a quantidade de capital necessária, com o uso de uma metodologia adequada, que “proporciona maior conhecimento do perfil de risco da instituição e melhor adequação à qualidade dos controles” (Banco do Brasil, 2011).

Essas abordagens deveriam ser implementadas gradualmente, cujo cronograma varia para os riscos envolvidos (crédito, mercado ou operacional) e foi estabelecido pelo Comunicado BACEN 12.746, e editado posteriormente nos Comunicados nº 16.137 e 19.028.

### I.6.2 Normativos

O BACEN, alinhado com os procedimentos dos órgãos reguladores dos países desenvolvidos, publicou uma série de normatizações prudenciais, dentre as quais destacamos as principais:



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Quadro 2 - Alguns Normativos de Basileia I**

<b>Resolução CMN 2.099</b> (17 de agosto de 1994)	<b>Resolução CMN 2.682</b> (21 de dezembro de 1999)	<b>Resolução CMN 2.837</b> (30 de maio de 2001)	<b>Comunicado BACEN nº 12.746</b> (09 de dezembro de 2004)
Estabeleceu a exigência de capital para cobertura de risco de crédito e a instituição dos limites mínimos de capital e de patrimônio líquido para as instituições financeiras.	Instituiu a classificação das operações de crédito em nove níveis de risco (AA, A, B, C, D, E, F, G, H) e a constituição de provisão para créditos de liquidação duvidosa.	Definiu o Patrimônio de Referência das instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN.	Estabeleceu o cronograma e os procedimentos a serem adotados na implementação da Basileia II – levando-se em consideração o nível de risco associado às operações
<b>Resolução CMN 3.464</b> (26 de junho de 2007)	<b>Resolução CMN 3.444</b> (28 de fevereiro de 2007)	<b>Resolução CMN 3.490/07</b> (29 de agosto de 2007)	<b>Comunicado nº 16.137</b> (27 de setembro de 2007)
Determinou a implementação da estrutura de gerenciamento de Risco de Mercado, com destaque para a definição de política institucional, processos, procedimentos e sistemas de suporte, além da indicação do diretor responsável pela gestão.	Revisou a definição do conceito de Patrimônio de Referência (PR), revogando a Resolução 2.837, de 30 de maio de 2001.	Alterou os critérios para a apuração do Patrimônio de Referência Exigido (PRE), incorporando parcelas de risco de mercado não contidas anteriormente, trazendo modificações significativas na apuração de capital para risco de crédito e incorporando o risco operacional.	Estabeleceu novo cronograma, ajustando o Comunicado nº 12.746, de 09/12/04. Conforme este documento, a implementação das exigências para utilização de modelos avançados de mensuração de capital deverá ocorrer até o final de 2012, com destaque para a alocação de capital para risco operacional e mudanças na alocação de capital para risco de crédito (Pilar I).

**Fonte: Adaptado de (Banco do Brasil, 2011)**

Além dos normativos citados acima, é interessante detalhar os documentos publicados em Basileia II que se referem ao risco operacional, assunto tratado neste trabalho.

### ***1.6.2.1 Resolução CMN 3.380 (29 de junho de 2006)***

Dispõe sobre a implementação de uma estrutura de gerenciamento do risco operacional, que deve ser compatível com a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas da instituição, como também capacitada para identificar, avaliar, monitorar, controlar e mitigar os riscos da empresa, além de identificar e monitorar os riscos de empresas terceirizadas, relevantes para o funcionamento da instituição. A Resolução determina também a indicação de diretor responsável pelo gerenciamento do Risco Operacional.

### ***1.6.2.2 Circular nº 3.383 (30 de abril de 2008)***

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Estabelece os procedimentos para o cálculo da parcela de Patrimônio de Referência Exigido (PRE) referente ao risco operacional ( $P_{OPR}$ ), que deve ser realizado semestralmente pelas empresas. Dois indicadores são utilizados no cálculo:

- Indicador de Exposição ao Risco Operacional: “corresponde, para cada período anual, à soma dos valores semestrais das receitas de intermediação financeira e das receitas com prestação de serviços, deduzidas as despesas de intermediação financeira”.
- Indicador Alternativo de Exposição ao Risco Operacional (IAE): “corresponde, para cada período anual, à média aritmética dos saldos semestrais das operações de crédito, de arrendamento mercantil e de outras operações com características de concessão de crédito e dos títulos e valores mobiliários não classificados na carteira de negociação, multiplicada pelo fator 0,035.”

Os seguintes modelos podem ser utilizados pelas empresas, ao seu critério:

I – Abordagem do Indicador Básico – BIA: é a abordagem mais simples, que utiliza um percentual fixo de 15% e o parâmetro Z, multiplicador cujos valores são definidos no artigo 8º da Circular, para calcular o  $P_{OPR}$ .

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^3 \max[0, 15.IEt; 0]}{n}, \text{ onde}$$

**Equação 1 - Cálculo do  $P_{OPR}$  na Abordagem do Indicador Básico**

n = número de vezes, nos três últimos períodos anuais, em que o valor do IE é maior que zero.

II – Abordagem Padronizada Alternativa - TSA: semelhante ao BIA, mas define o fator de ponderação  $\beta$ , que varia de 12% a 18%, dependendo da linha de negócio da empresa.

A abordagem padronizada pode ser usada somente se o banco demonstrar um gerenciamento eficaz e controle de risco operacional. Também precisa demonstrar que tem as seguintes implementações (CYRIAC, 2008):

- Controle de risco independente e função de auditoria.
- Sistemas de divulgação de risco eficazes.
- Funções de GRO com responsabilidades claramente atribuídas a ele.
- Conselho de diretores e gerentes seniores ativamente envolvidos na supervisão do programa de GRO.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Sistema de GRO robusto e aplicado com integridade.
- Recursos suficientes para a utilização da abordagem nas linhas de negócio principais, bem como nas áreas de controle e auditoria (CYRIAC, 2008).

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^3 \max [(\sum_{i=1}^2 IAEi, t. \beta i) + (\sum_{i=3}^8 IEi, t. \beta i); 0]}{3}$$

**Equação 2 - Cálculo do  $P_{OPR}$  na Abordagem Padronizada Alternativa**

III – Abordagem Padronizada Alternativa Simplificada - ASA: semelhante ao método TSA, porém utilizada para as linhas de negócio Varejo e Comercial.

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^2 \max \{ [IAEt, 0, 15) + (IEt, 0, 18) \}; 0 \}}{3}$$

**Equação 3 - Cálculo do  $P_{OPR}$  na Abordagem Padronizada Alternativa Simplificada**

IV – Abordagem Avançada – AMA: “engloba todas as técnicas de medição que levam a uma medição precisa da exposição de cada linha de negócios de uma instituição financeira para cada categoria de evento de perda operacional” (CHAPELLE et al., 2004, tradução nossa). É o método mais complexo, que deve ser desenvolvido internamente à empresa e aprovado pelo Banco Central.

Caso a metodologia utilizada pela empresa seja considerada inadequada, o Banco Central poderá exigir a utilização da Abordagem do Indicador Básico.

### ***I.6.2.3 Carta-Circular nº 3.315 (30 de abril de 2008)***

Esclarece, com exemplos, os procedimentos para o cálculo do Patrimônio de Referência Exigido (PRE) referente a Risco Operacional ( $P_{OPR}$ ), de que trata a Circular nº 3.383, com base nas três metodologias: Abordagem do Indicador Básico, Abordagem Padronizada Alternativa e Abordagem Padronizada Alternativa Simplificada.

## **I.7 BASILEIA III**

Considerando a crise financeira internacional, iniciada em 2008, o Comitê de Basileia criou em dezembro de 2009, o acordo Basileia III, que visa “aperfeiçoar a capacidade das

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

instituições financeiras de absorver choques provenientes do sistema financeiro ou dos demais setores da economia, propiciando a manutenção da estabilidade financeira e a promoção do crescimento econômico sustentável” (BACEN, 2011a). O objetivo é reduzir a probabilidade de futuras crises bancárias e seus potenciais efeitos negativos sobre os demais setores da economia. O termo Basileia III, no entanto, não é utilizado pelo comitê, e as regras são vistas por muitos mais como um refinamento de Basileia II do que uma reforma. Em 17 de fevereiro de 2011, o Banco Central divulgou o Comunicado 20.605, que fixa orientações preliminares e o cronograma para adoção das regras de Basileia III no Brasil.

Para evitar que haja outras crises, algumas recomendações foram criadas, como:

- O conceito de Patrimônio de Referência (PR) será alterado para atender às exigências das regras prudenciais. Permanecerá composto pelos capitais Nível I e II. O primeiro passará a ser constituído de duas parcelas, o Capital Principal (*Common Equity Tier 1*) e o Capital Adicional (*Additional Tier 1*), com capacidade efetiva de absorver perdas durante o funcionamento da instituição financeira. O Capital Principal será composto fundamentalmente pelo capital social e o Adicional será composto por instrumentos híbridos de capital e dívida autorizados. O Nível II será constituído de elementos capazes de absorver perdas em caso de ser constatada a inviabilidade do funcionamento da instituição (BACEN, 2011a).

- Os bancos devem ter, até 2015, um capital social equivalente a 4,5% dos seus ativos e não mais 2%, como atualmente. Capital social é “constituído por cotas ou por ações ordinárias e ações preferenciais não resgatáveis e sem mecanismos de cumulatividade de dividendos, e por lucros retidos, deduzidos os valores referentes aos ajustes regulamentares” (BACEN, 2011a).

- Até 2019, deverá ser criada uma proteção adicional, chamado Capital de Conservação, de 2,5% dos ativos, que pode ser utilizado para absorver perdas em períodos de stress econômico e financeiro. É composto por elementos aceitos no Capital Principal (BACEN, 2011a).

- Deverá ainda ser criado o Capital Contracíclico, de 2,5% até 2019, também composto por elementos aceitos no Capital Principal, que seria formado para contemplar os riscos decorrentes de alterações no ambiente macroeconômico (BACEN, 2011a).

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Deverá ser implementado, a partir de 1º de janeiro de 2013, o Índice de Alavancagem, calculado pela divisão do valor do Nível I do PR pelo valor da exposição total. A partir de 2018, será exigido um valor mínimo para o índice, previsto em 3% (BACEN, 2011a).
- Deverão ser definidos até dezembro de 2013: o Índice de Liquidez de Curto Prazo (LCR) e o Índice de Liquidez de Longo Prazo (NSFR), para estabelecer requerimentos mínimos quantitativos para a liquidez das instituições financeiras. O LCR possibilita que as instituições possuam recursos de alta liquidez para resistir durante um período de stress financeiro de um mês e o NSFR “busca incentivar as instituições a financiarem suas atividades com fontes mais estáveis de captação”. Os índices deverão possuir valores superiores a 1% a partir de 2015 e 2018, respectivamente (BACEN, 2011a).
- Dezembro de 2013: será definido o cálculo do índice de liquidez (LCR) e até dezembro de 2014 o BC divulga metodologia para outra medida de liquidez (NSFR). Até dezembro de 2016, a composição do NSFR. E até julho de 2017, a definição final da composição e do índice de alavancagem (BACEN, 2011a).

As recomendações de Basileia III são complementares às de Basileia II e devem ser juntamente consideradas com as informações do Comunicado nº 12.746, alterado pelos Comunicados 16.137 e 19.028.

O Comitê de Basileia recomendou a aplicação gradual das regras ao longo de oito anos, o que é visto por muitos como uma deficiência, que consideram que as empresas demorariam para implementar as regras. Outros concordam com a medida, já que muitos bancos ainda estão se recuperando da crise. Há ainda preocupações de que as mudanças afetem a capacidade de crédito dos bancos.

De acordo com o BACEN, a regulamentação prudencial brasileira é mais conservadora do que o padrão internacional, o que contribuiu que as empresas brasileiras superassem a crise financeira de 2008 mais rapidamente. Portanto, embora haja a necessidade de adaptação para as novas exigências, os bancos no Brasil necessitarão de menor esforço que os internacionais para se adequar, considerando que algumas regras prudenciais já foram adotadas internamente. Assim, o Bacen pretende antecipar algumas recomendações do acordo de Basileia III (BACEN, 2011b).

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### **II RISCO OPERACIONAL NA EMPRESA**

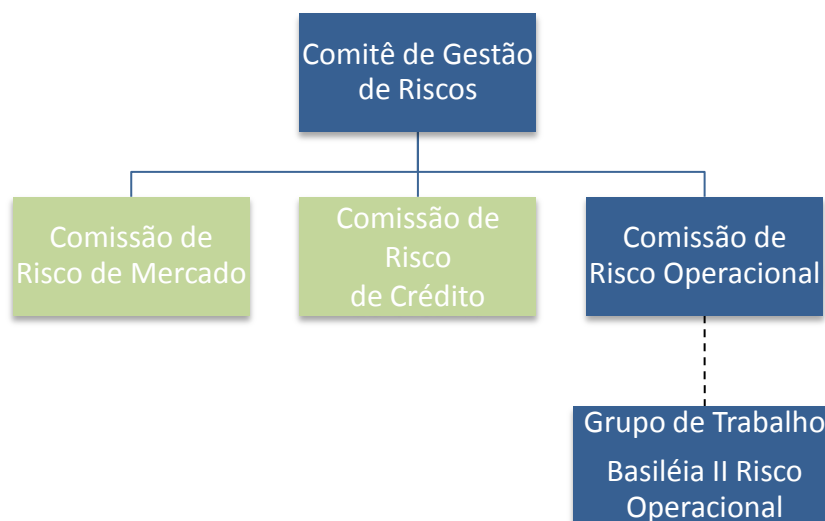
A empresa estudada define o risco operacional de acordo com o BCBS, ou seja, como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. Para se mitigar um risco ao máximo, deve-se buscar, por exemplo, reduzir o impacto que ele causa, a frequência em que ocorre, o custo do controle existente para mitigá-lo (ou aumentar sua eficiência) e o próprio evento.

De acordo com a Resolução CMN 3.380, citada anteriormente no item I.6.2.1, entre os eventos de risco operacional, incluem-se:

1. Fraudes internas;
2. Fraudes externas;
3. Demandas trabalhistas e segurança deficiente do local de trabalho;
4. Práticas inadequadas relativas a clientes, produtos e serviços;
5. Danos a ativos físicos próprios ou em uso pela instituição;
6. Aqueles que acarretem a interrupção das atividades da instituição;
7. Falhas em sistemas de tecnologia da informação;
8. Falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição;
9. Risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como sanções legais e administrativas.

A empresa possui um Comitê Operacional de Risco, em alinhamento com as diretrizes do Banco Central, responsável por definir a política de gerenciamento e controle dos riscos inerentes aos negócios, com o objetivo de mensurar, gerir, controlar e mitigar a exposição aos riscos de mercado, crédito e operacional. O Comitê ainda tem o papel de definir os objetivos globais para controle dos riscos, devendo ratificar as decisões das comissões de risco e encaminhar propostas ao Conselho de Administração. Subordinados a esse comitê, estão as Comissões de Risco de Crédito, Operacional e de Mercado.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL



**Figura 1 - Comitê Operacional de Risco**

A Comissão de Risco Operacional define as diretrizes para uma boa gestão de risco operacional, com o objetivo de identificar e conhecer todos os riscos operacionais existentes, assim como avaliar a melhor maneira de controlá-los e mitigá-los, através da melhoria de processos, controles internos e planos de ação. Possui a responsabilidade de revisar a Política de Gerenciamento de RO, informar a Diretoria e o Conselho de Administração sobre o cumprimento de suas recomendações, nomear os responsáveis para o gerenciamento de RO e estabelecer as regras para seu próprio funcionamento. Para manter-se alinhada com as diretrizes do Comitê de Basileia e do Banco Central, a Comissão de risco operacional se reúne normalmente uma vez a cada três meses, exceto quando há necessidade de uma frequência maior de reuniões. A Comissão tem a função de supervisão, revisando e aprovando as políticas de gerenciamento de risco operacional, como também acompanhando os planos de ação para eventos de risco operacional.

Além da Comissão, existe também o Grupo de Trabalho Basileia II para risco operacional, que se reúne mensalmente para discutir assuntos relacionados à gestão e modelagem de RO. O Grupo deve estruturar a captura de dados de perdas operacionais, atender exigências regulatórias para implantação de modelos avançados e acompanhar o desenvolvimento de modelos de alocação. As áreas de Gestão e Modelagem de RO são responsáveis pela preparação do material das reuniões, e as áreas envolvidas no processo de captura e reporte de eventos devem enviar pelo menos um representante, que deve divulgar o que foi discutido para os outros funcionários da área.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A área de Gerenciamento de Risco Operacional tem como objetivo identificar, categorizar e avaliar os riscos que possam impedir o cumprimento dos objetivos dos negócios, assim como os controles existentes para mitigá-los. Para isso, a instituição deve possuir uma infra-estrutura de recursos materiais e humanos capaz de monitorar os riscos, controles e perdas operacionais, como também possuir uma cultura de risco operacional que seja disseminada aos funcionários da empresa, garantindo entendimento e monitoramento constante, além de dar conhecimento à Alta Administração dos principais riscos existentes. O Plano de Comunicação deve ser estabelecido para assegurar que todas as áreas compreendam o papel, objetivos e responsabilidades da área de Gerenciamento de RO.

Caso seja necessário, os colaboradores envolvidos podem receber treinamento, para assegurar que a cultura seja disseminada, atingindo as diversas áreas e departamentos, possibilitando identificar eventos relacionados a risco operacional. A empresa, através da área de Recursos Humanos, deve fornecer o treinamento mais compatível com as necessidades dos funcionários, além dos recursos para um bom treinamento, mantendo sempre tudo em arquivo.

O Banco Central exige que as empresas que utilizam a Abordagem de Mensuração Avançada para apuração do risco operacional (AMA), possuam um sistema de reporte de eventos de RO. Ele é importante para as empresas manterem o registro em uma base de dados todas as perdas decorrentes de riscos operacionais que se materializaram, independentemente de ocorrência de impacto financeiro, com a descrição resumida e detalhada do evento e suas causas, para auxiliar no cálculo do montante necessário para se realizar cobertura frente ao risco operacional, de acordo com a política de Basileia II, além de proporcionar informações para identificar as possíveis causas de outros riscos. A área de Gestão de Riscos se responsabiliza por analisar os dados cadastrados no sistema, e caso alguma informação não esteja de acordo com os padrões estabelecidos, a pessoa que realizou o registro deve ser contatada para que o erro não ocorra novamente.

De acordo com as determinações do Banco Central, as instituições financeiras devem possuir metodologia própria para calcular o capital necessário para realizar a cobertura dos riscos operacionais, como também criar cenários para os eventos que venham a ocorrer.

Outras áreas também possuem responsabilidades. A área de Controles Internos deve verificar a efetividade dos controles internos existentes (BACEN, 1998), assim como a implementação dos planos de ação. As áreas de Tecnologia de Informações e Segurança da



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Informação devem prestar o suporte tecnológico necessário para o desenvolvimento dos trabalhos.

A avaliação de riscos operacionais contribui para auxiliar o seu gerenciamento de risco operacional, através do entendimento e conhecimento pelo gestor dos riscos existentes nos processos sob sua gestão, e também contribui para dar ciência à alta administração dos riscos relevantes da empresa.

### II.1 METODOLOGIA DE RISCO OPERACIONAL UTILIZADA

A metodologia de Gestão de Risco Operacional na empresa segue os seguintes passos:

*Identificação dos macroprocessos*, processos e subprocessos relacionados ao risco da área mapeada.

*Identificação dos Eventos de Risco Operacional*. A descrição do risco associado ao processo deve ser detalhada, com a identificação das principais causas e com a classificação das categorias de risco (nível 1 e 2), que segue o Dicionário de Eventos de Risco Operacional, metodologia desenvolvida pela empresa. Ademais, deve ser identificado o Status do risco (caso este seja cancelado, é necessária uma justificativa), os possíveis efeitos de sua materialização e caso haja sobreposição com outros tipos de risco, como Risco de Crédito, Mercado, Legal, Imagem ou Estratégico.

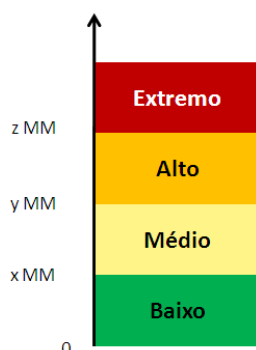
*Identificação e Avaliação dos Controles Existentes*. As atividades de controle e os instrumentos mitigadores existentes para reduzir ou evitar a materialização do risco devem ser descritos, como seus objetivos, causas mitigadas, área responsável por sua implementação, periodicidade de execução e características do controle, que pode ser preventivo, detectivo, manual, parcialmente automatizado ou automatizado. A avaliação dos controles é realizada pela área de Controles Internos, com o objetivo de analisar se o controle mitiga adequadamente o risco. De acordo com a avaliação, é estabelecida uma classificação e nota da efetividade do controle; caso seja insatisfatório, medidas devem ser tomadas.

*Ocorrência de Eventos de RO*. Antes de avaliar os riscos de acordo com a metodologia interna, a área de Gestão de RO verifica se há lançamentos de perda operacional na base de dados de eventos de risco operacional, para uma avaliação mais correta.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

*Avaliação dos Riscos*, realizado por questionários respondidos pela área de Gestão de RO, juntamente com o gestor da área analisada. Na avaliação quantitativa (Impacto no Negócio), o gestor e o analista devem estimar a probabilidade e a severidade quantitativas do risco, ou seja, a intensidade com que a ocorrência do risco pode afetar financeiramente o objetivo do processo. O impacto financeiro é quantificado em termos monetários e base mensal e de acordo com esse valor, chega-se a uma avaliação. A avaliação qualitativa (Possibilidade de Ocorrência) é a expectativa de ocorrência do risco, considerando a efetividade do ambiente de controle existente. São atribuídos pesos às questões do questionário, e de acordo com o resultado das respostas chega-se a um valor da avaliação. Caso o trabalho seja revisão de mapeamento, deverão ser consideradas ainda o percentual de Possibilidade Anterior, planos de ação implementados e ocorrência de eventos de RO e de pontos de auditoria. A partir das avaliações qualitativas e quantitativas, é definida a exposição final do risco, que será explicado no capítulo V.

De acordo com esse valor e métrica definida pela Comissão de Risco Operacional, o risco é classificado em Baixo, Médio, Alto ou Extremo.



**Figura 2 - Níveis de risco operacional**

*Tratamento dos Riscos e Planos de Ação.* Depois de identificados, avaliados e mensurados, deve-se definir qual o tratamento que será dado aos riscos. Como na prática é impossível eliminar totalmente os riscos, a melhor alternativa de tratamento deve ser escolhida, levando-se em consideração os objetivos estratégicos da empresa, assim como sua posição frente aos riscos. As alternativas de tratamento estão descritas abaixo:

Evitar – Esta opção será possível caso o processo que gera o evento de risco operacional seja eliminado, ou o que se deseja é sair do negócio a que se aplica o risco, quando, por exemplo, a empresa decide se desfazer de uma unidade de negócios.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Reduzir – Quando o que se deseja é minimizar o nível de risco operacional, seja reduzindo o impacto no negócio e/ou a probabilidade de ocorrência.

Transferir – Ações tomadas para minimizar o nível de risco operacional através da transferência, compartilhando o gerenciamento a outros processos, áreas ou terceiros. Em alguns casos, mesmo com o gerenciamento de risco operacional efetivo, a instituição ainda está exposta a eventos que não pode controlar, nem evitar, como, por exemplo, com catástrofes naturais. Uma das medidas a serem tomadas é a transferência do risco através da contratação de seguro, de acordo com as condições definidas por Basileia II. A utilização de seguros é importante para riscos catastróficos, de baixa probabilidade e alta severidade, e para riscos de alta frequência que propiciam perdas relevantes; ou seja, é uma ótima opção para riscos cujos custos de transferência sejam menores que os de retenção.

Aceitar – Nesse caso, nenhuma ação é tomada, assumindo o risco operacional exatamente como está atualmente. Essa opção só deve ser tomada quando o nível do risco for Baixo, com pequena probabilidade de ocorrência e baixo impacto para o negócio e qualquer ação a ser tomada seja mais custosa para a empresa que arcar com os custos do risco, caso este se materialize.

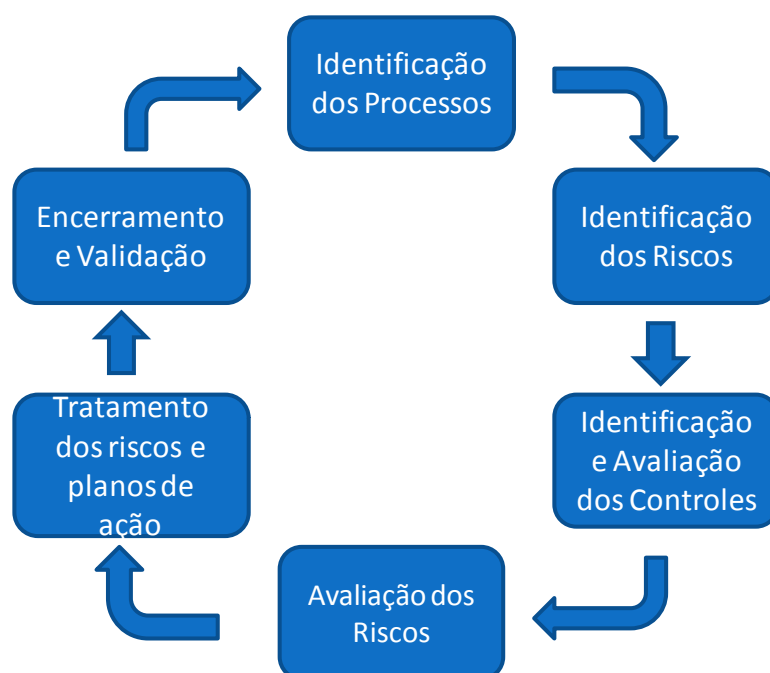
Caso a estratégia seja “Aceitar”, deve-se justificar a escolha de tal tratamento. Caso seja “Evitar”, “Reduzir” ou “Transferir”, devem ser definidas as ações a serem tomadas. Neste caso, o plano de ação deve ser descrito claro e sucintamente, juntamente com seus benefícios, causas a serem minimizadas e criação de novos controles ou automatização dos controles existentes. Além disso, deve ser definido o estágio de implementação (Em edição, Ativo, Cancelado ou Concluído), assim como as datas de Início Planejado, Início Efetivo, Conclusão Planejada e Conclusão Efetiva e o percentual de redução do risco devido à implementação dos planos de ação, avaliado pela área de Gestão de RO. A área de Controles Internos é responsável por acompanhar, junto à área gestora do processo, a implantação dos planos de ação recomendados.

*Encerramento e Validação.* Após todas as etapas anteriores estarem concluídas, deve ser feito um encerramento, com apresentações dos trabalhos de mapeamento de riscos e controles para os gestores da área mapeada e gerência de riscos. E por último, ocorre a validação pela Comissão de Risco Operacional, que analisa se a política adotada, para os riscos aceitos, riscos com alta exposição, planos de ação prorrogados e cancelados, pontos sem consenso entre a área gestora e a Gerência de Riscos, fora a mais adequada. As decisões

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

tomadas pela Comissão de Risco Operacional são registradas em ata e divulgadas aos membros e participantes convidados e estão acima de quaisquer decisões tomadas pelas áreas envolvidas.

O esquema a seguir resume as etapas da Metodologia de Identificação de Risco Operacional:



**Figura 3 - Etapas da Metodologia de Identificação de Risco Operacional**

## II.2 SISTEMA DE INFORMAÇÃO UTILIZADO

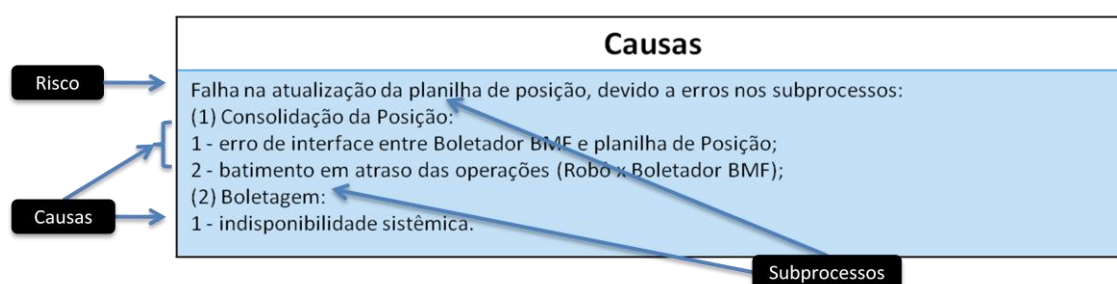
Para realizar o Mapeamento de Riscos, era utilizado um sistema de informação disponibilizado via intranet. Por ser uma ferramenta desenvolvida por outra empresa, que também é responsável pela manutenção do programa, há pouca personalização do produto e quaisquer alterações a serem realizadas de acordo com a vontade do cliente, dependem de disponibilidade e capacidade da empresa fornecedora, que ainda não entende a metodologia de risco operacional. Por ser utilizada em rede, a ferramenta fica por muitas vezes lenta, com o excesso de carregamento de informações ou com atualizações realizadas semanalmente nos computadores da empresa. Por essas razões, apresenta limitações que impedem que os analistas da área de Risco Operacional a utilizem durante entrevistas com os gestores das

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

áreas do banco. Assim, eles fazem uso de planilhas em Excel, onde anotam todas as informações relevantes à área analisada, como Riscos, Controles e Planos de ação para cada Subprocesso. Depois disso, transferem esses dados para o sistema de mapeamento na Intranet, realizando, portanto, o mesmo trabalho duas vezes.

Algumas limitações são explicadas mais detalhadamente. Cada registro deve ser criado para uma área específica e para uma dada filial da empresa, o que impede a visualização de um determinado risco para o conglomerado da empresa. Ademais, a edição de diversos campos importantes, como *Nome da Empresa*, *Nome da Área*, *Macroprocesso*, *Processo* e *Subprocesso* no sistema é feita livremente, o que permite variações do tipo “Diretoria Corretora” / “Dir. Corretora” e “Administração de Recursos” / “Adm. de Recursos”.

A forma como as causas e subprocessos são listados no sistema, conforme a ilustração abaixo, com os subprocessos listados abaixo de cada risco, e as causas listadas abaixo de cada subprocesso, é de difícil visualização e pouca praticidade, pois pode deixar a lista relativamente longa, se houver muitos subprocessos e causas mapeados.



**Figura 4 - Listagem de causas por subprocesso no programa antigo**

A seguinte visualização, da Figura 5 - Listagem de causas por subprocesso no programa atual, com os riscos, subprocessos, causas tratados de maneira independente, lado a lado, é mais adequada.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Risco	Subprocesso	Causa Detalhada
Falha na atualização da planilha de posição	Consolidação da Posição	Erro de interface entre Boletador BMF e planilha de Posição
		Batimento em atraso das operações (Robô x Boletador BMF)
	Boletagem	Indisponibilidade sistêmica

**Figura 5 - Listagem de causas por subprocesso no programa atual**

O cadastro de causas no sistema também possui limitações: deve ser realizado em campos de livre digitação, com uma causa após a outra. Essa maneira acarreta dificuldade de visualização, além de perda de tempo para escrever todas as causas.

Causa do risco
Falha na estruturação de operações de fusões e aquisições decorrente de: - utilização de informações para estudo da empresa e análise setorial de fontes não oficiais/não confiáveis; - erro no cálculo de precificação do ativo; - não solicitar parecer de auditoria externa para análise de "Due Diligence"

**Figura 6 - Cadastro de causas no programa antigo**

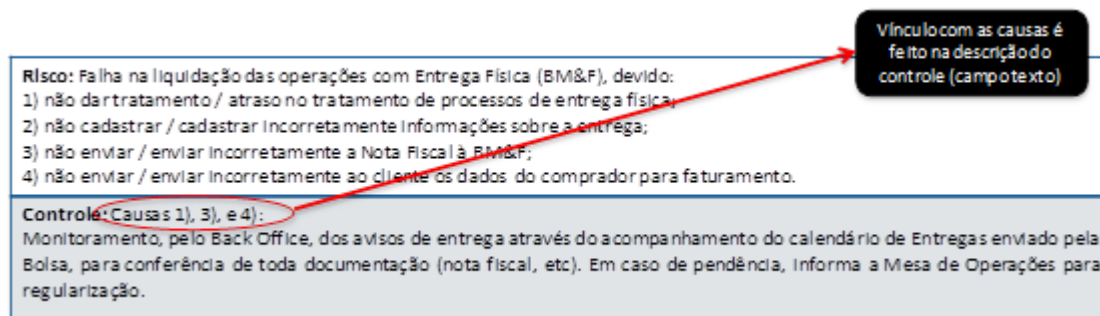
A figura abaixo ilustra o registro de ambiente de controle, realizado em campo texto para cada risco. Nesse caso, como um mesmo controle mitiga dois riscos diferentes, ele deve ser cadastrado duas vezes. Não há padronização em relação aos controles. Cada analista descreve-o, da melhor forma possível. O mesmo ocorre para o cadastro de plano de ação.

<b>Risco:</b> Liberação de ordem de pagamento sem autorização	<b>Risco:</b> Falha na liquidação financeira das operações dos clientes
<b>Controle:</b> Conciliação automática dos lançamentos através da importação dos arquivos ao sistema Sinacor ou integração ao sistema SAP-RV. Em caso de divergências, providenciam as regularizações.	<b>Controle:</b> Todas as causas Conciliação automática dos lançamentos através da importação dos arquivos ao sistema Sinacor ou integração ao sistema SAP-RV. Em caso de divergências, providenciam as regularizações.

**Figura 7 - Cadastro de ambiente de controle no programa antigo**

O vínculo dos ambientes de controle (ou planos de ação) com as causas do risco é feito na descrição do controle, também em campo texto. A única forma de mensurar que o controle mitiga determinada causa, era mencionar no próprio texto da descrição do controle. Qualquer análise fica impossibilitada, como por exemplo, o número de causas ele mitiga.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL



**Figura 8 - Vínculo entre ambiente de controle e causas do risco no programa antigo**

Há dificuldade para navegar entre os diversos módulos. Devido à utilização de campos texto, não é possível reaproveitar a descrição dos riscos e controles. Somente para plano de ação existe uma funcionalidade, que permite vincular um único plano de ação para diversos riscos.

Outro problema é a extração de dados, como a dificuldade e limitação de gerar consultas e relatórios, que poderiam ser encaminhados para os diversos envolvidos e interessados no processo, como os próprios funcionários de Gestão de Risco Operacional, como também os de Controles Internos, que utilizam das informações sobre os controles para realizar testes e avaliar seu funcionamento. Os relatórios, de acordo com os usuários, são confusos e cansativos, de layout não amigável.

O sistema possui alguns campos que são de preenchimento obrigatório, porém não são usados pela área de Gestão de Risco Operacional. Além disso, os módulos de reporte de perdas e pontos de auditoria não possuem integração com o mapeamento de riscos: Não é possível visualizar a existência de perdas e pontos de auditoria em aberto no momento de efetuar a avaliação dos riscos, características muito importantes para auxiliar no cálculo do nível de exposição ao risco (baixo, médio, alto ou extremo).

Certas peculiaridades ainda não são analisadas na ferramenta. Como exemplo, pode ser citada a vinculação de um controle inadequado a um risco, cuja análise deve ser realizada pelo analista, quando poderia ser pelo próprio programa.

Por último, não existe integração com a estrutura da empresa, que muda consideravelmente a cada mês. Isso impacta negativamente em todos os registros vinculados a uma determinada área, quando esta é reestruturada, ou a um gestor, quando este sai da empresa ou muda de área.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Devido a essas limitações, foi decidido que um programa em Access deveria ser elaborado internamente pelos funcionários de Gestão de RO. Além de não conter os problemas acima mencionados, ele seria mais adequado para as necessidades dos usuários de Mapeamento de Risco, levando em consideração como o mapeamento é efetivamente realizado dentro da área.

Para atingir esse objetivo, foram realizadas as seguintes atividades:

- Levantamento dos requisitos do novo sistema, com base em informações levantadas juntos aos operadores;
- Desenvolvimento do programa;
- Implantação de versão para testes, para os usuários se familiarizarem com o sistema e tirarem eventuais dúvidas;
- Realização de ajustes e correções. Essa etapa é explicada detalhadamente no item VI.7;
- Implantação da versão de produção ou final, onde os usuários realizam os cadastros dos mapeamentos;
- Análise dos resultados obtidos.

A elaboração dos requisitos do programa é explicada no próximo capítulo. Os capítulos seguintes apresentam a solução desenvolvida, a sua implantação e a análise dos resultados.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### **III REQUISITOS DE UM NOVO SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL**

Este capítulo apresenta os requisitos para um novo sistema de gestão de risco operacional para a empresa.

Primeiramente, antes de elaborar e analisar os requisitos desse projeto, foi realizada uma pesquisa para avaliar a sua viabilidade. Para realizar essa tarefa, o ponto de partida foi o levantamento da opinião dos usuários do sistema atual, para descobrir se o novo sistema seria mais vantajoso que o anterior, e se, além disso, ajudaria a contribuir com os objetivos da organização.

Entrevistas foram realizadas com os usuários, que elencaram as diversas limitações do programa antigo, como já explicado anteriormente, e se posicionaram a favor da criação de um novo. Foi decidido, portanto, que o novo sistema seria desenvolvido internamente pela empresa, apesar da limitação por parte dos funcionários com o conhecimento sobre o assunto, e utilizado por período indeterminado pela empresa, podendo ser usado como modelo num projeto de aquisição.

Neste capítulo são identificados os requisitos do sistema, utilizando a modelagem orientada a objetos, mais especificamente com base no método proposto por Wilson de Padua Paula Filho, no seu livro *Engenharia de Software*.

Por fim, são elencados os benefícios e as limitações provenientes do desenvolvimento do novo sistema.

#### **III.1 TIPOS DE REQUISITOS**

Os requisitos podem ser classificados em dois tipos: funcionais e não funcionais. Os primeiros “descrevem as funcionalidades que se espera que o software forneça quando estiver pronto, como entradas, saídas exceções etc” (KOSCIANSKI; SOARES, 2006, p.179) e são mais bem descritos em um modelo de casos de uso. Os últimos “descrevem restrições ao software de forma geral. Não são, portanto, relativos diretamente às funções desempenhadas pelo produto” (KOSCIANSKI; SOARES, 2006, p.179). Estão relacionados com padrões de

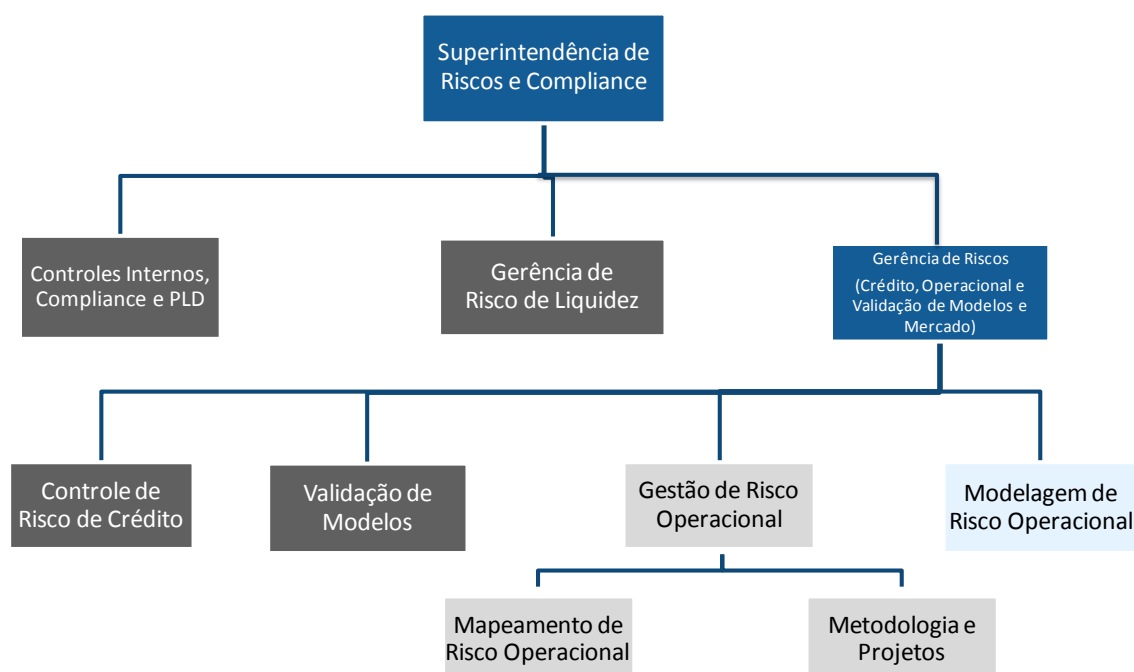
## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

qualidade como desempenho, confidencialidade e qualidade e influenciam diretamente a satisfação do usuário.

### III.2 REQUISITOS FUNCIONAIS

#### III.2.1 Modelo de casos de uso de negócio e sistema

Para entendermos adequadamente o sistema a ser desenvolvido, deve-se estar claro, primeiramente, o negócio em que ele está inserido. A figura abaixo mostra a estrutura em que a área de Gestão de Risco Operacional, dividida em Mapeamento de Risco Operacional e Metodologia e Projetos, está inserida na empresa. O sistema recém desenvolvido é usado por ambas as unidades de Gestão de RO para o cadastro e gerenciamento dos mapeamentos de riscos.



**Figura 9 - Estrutura de Riscos da empresa**

Para determinar os aspectos relevantes do contexto em que um produto irá operar, utiliza-se um modelo da UML (*Unified Modeling Language*): o Modelo de Casos de Uso, composto por atores, casos de uso e o sistema a ser criado.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Caso de uso de sistema é um documento narrativo que descreve a sequência de eventos de um ator que usa um sistema para completar um processo (JACOBSON et al.,1992). Rosenberg e Scott (1999, p.38, tradução nossa) definem caso de uso como uma “sequência de ações que um ator (geralmente uma pessoa ou uma entidade externa, como um outro sistema) executa dentro de um sistema para atingir um objetivo específico”. Cada caso de uso gera benefícios para os usuários do sistema e a totalidade deles mostra o que o sistema deve fazer, ou seja, sua funcionalidade. Já atores, de acordo com Paula Filho (1999, p. 96), são “representações dos usuários e outros sistemas que interagem com o produto”.

O modelo tem por objetivo descrever os requisitos funcionais do sistema e definir os atores que irão se comunicar com o sistema (NIEMANN, 2004), fornecendo uma descrição clara e sucinta do que ele deve fazer.

Para identificar os atores do sistema, algumas perguntas podem ser feitas, como, por exemplo (WTHREEX, 2011, PAULA FILHO, 1999):

- Quem usa a informação do sistema;
- Quem se beneficia do sistema;
- Quem fornece ou remove informações do sistema
- Quem realiza a manutenção;
- Qual papel desempenhado por cada usuário;
- Com quais sistemas deve interagir.

Com base nesses critérios, foram identificados os seguintes atores:

- O próprio usuário do sistema, ou seja, o funcionário de Mapeamento de Risco;
- Funcionário de Gestão de Risco Operacional, responsável não apenas pelo gerenciamento dos riscos, como também pelo desenvolvimento e manutenção do sistema;
- Gestor da área sendo mapeada, que participa de entrevistas com o funcionário de Mapeamento de Risco, em busca da identificação de todos os riscos da área;
- Funcionário de Controles Internos, responsável por verificar o funcionamento dos planos de ação e ambientes de controle que estão em andamento.

Os casos de uso identificados para o novo sistema estão explicitados no Quadro 3, juntamente com uma descrição sucinta de cada um.

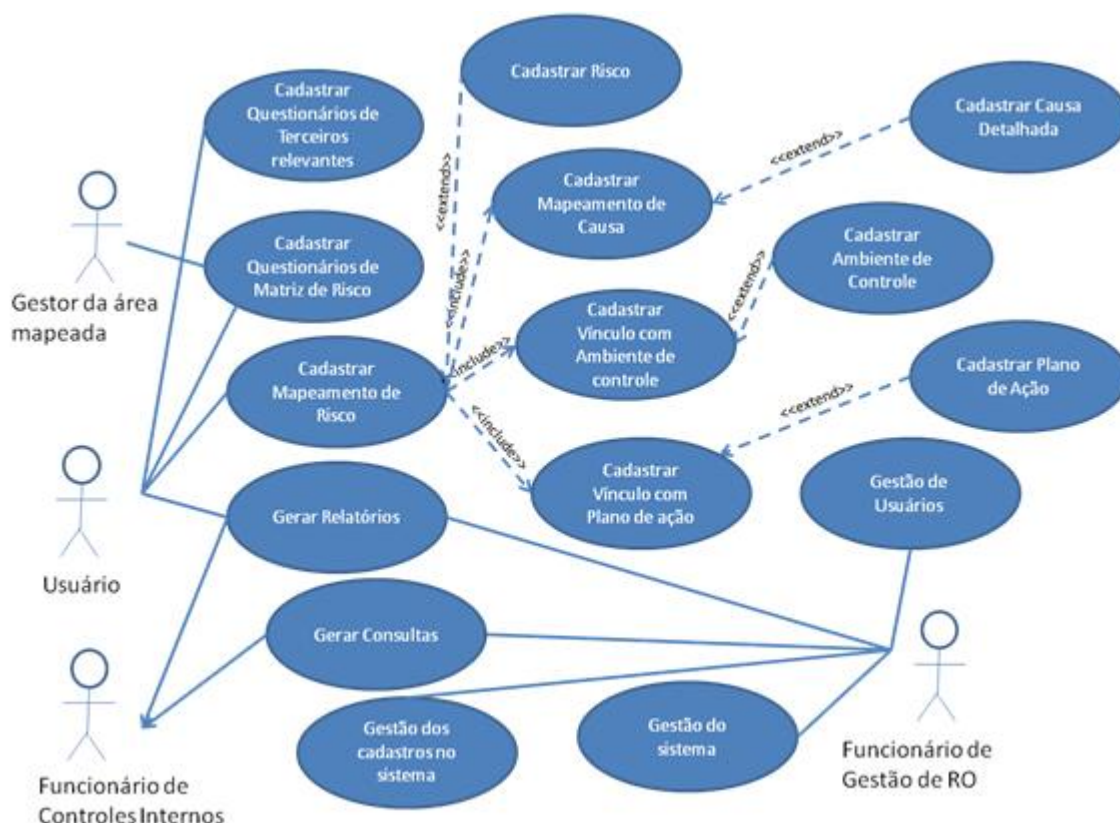
## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Quadro 3 - Casos de Uso do novo sistema**

Item	Caso de Uso	Descrição
1	Gestão de Usuários	Controle de usuários que terão acesso ao sistema
2	Gestão do sistema	Processamento de inclusão, exclusão e alteração de qualquer funcionalidade do sistema, assim como manutenção
3	Gestão dos cadastros	Processamento de inclusão, exclusão e alteração de cadastros
4	Gerar Relatórios	Emissão de relatórios com as informações das bases de dados do sistema
5	Gerar Consultas	Emissão de relatórios com as informações das bases de dados do sistema
6	Cadastrar/Editar Mapeamento de Risco	Inclusão, exclusão e alteração de cadastros de mapeamento de risco
7	Cadastrar/Editar Mapeamento de Causa	Inclusão, exclusão e alteração de cadastros de mapeamento de causa
8	Cadastrar/Editar vínculo com Ambiente de Controle	Inclusão, exclusão e alteração de vínculos com ambiente de controle
9	Cadastrar/Editar vínculo com Plano de Ação	Inclusão, exclusão e alteração de vínculos com planos de ação
10	Cadastrar/Editar Questionário de Terceiros relevantes	Inclusão, exclusão e alteração de questionário de terceiros relevantes
11	Cadastrar/Editar Questionário de Matriz de Risco	Inclusão, exclusão e alteração de questionário de matriz de risco
12	Cadastrar/Editar Ambiente de Controle	Inclusão, exclusão e alteração de cadastros de ambiente de controle
13	Cadastrar/Editar Plano de Ação	Inclusão, exclusão e alteração de cadastros de plano de ação
14	Cadastrar/Editar Causa Detalhada	Inclusão, exclusão e alteração de cadastros de causa detalhada
15	Cadastrar/Editar Risco	Inclusão, exclusão e alteração de cadastros de risco

Para um melhor entendimento do funcionamento do sistema, abaixo se encontra o diagrama de casos de uso mais importante, o diagrama de contexto, que “mostra as interfaces do produto com seu ambiente de aplicação, inclusive os diversos tipos de usuários e outros sistemas com os quais o produto deve interagir” (PAULA FILHO, 2003, p. 100). Os atores são simbolizados por bonecos e representam os usuários, sistemas externos e outros componentes de um sistema, enquanto os casos de uso, simbolizados por uma elipse, representam as possíveis formas de interação do produto com os atores (PAULA FILHO, 2003, p. 100).

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL



**Figura 10 - Diagrama de Casos de Uso**

Os relacionamentos representados na figura são a ligação sem direção, a ligação de inclusão e a de extensão. A primeira é a mais usual, quando a iniciativa da comunicação parte do ator (PAULA FILHO, 2003, p.99). O relacionamento de extensão representa uma situação opcional ou de exceção que geralmente ocorre durante a execução de um caso de uso, enquanto o relacionamento de inclusão representa uma atividade complexa, comum a diversos casos de uso. (PAULA FILHO, 2003, p.106).

### III.2.2 Fluxo de Eventos

Para detalhar melhor o Modelo Caso de Uso do Sistema e seus respectivos casos de uso, são descritos os fluxos de eventos, que representam o que o sistema faz. As descrições, porém, não são muito detalhadas, pois isso já fugiria do objetivo do modelo, que utiliza de descrições sucintas.

#### III.2.2.1 Fluxos de Eventos Básicos

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

O fluxo básico “é o caminho principal que o usuário vai seguir, do começo ao fim, nas circunstâncias normais” (ROSENBERG; SCOTT, 1999, p. 47, tradução nossa).

### Fluxo 1 - Cadastrar Mapeamento de Risco

1. O usuário acessa a tela de mapeamento de risco;
2. O sistema exibe uma tela com os campos a serem preenchidos, divididos em Gestor de Risco, Macroprocesso, Processo, Área, Categoria Nível 2 do Risco e o Risco;
3. O sistema preenche automaticamente a data de cadastro do risco com a data atual;
4. O usuário preenche as informações do risco;
5. O usuário clica no botão “salvar”;
6. O cadastro do mapeamento de risco é salvo no sistema com um código gerado automaticamente.

### Fluxo 2 - Cadastrar Mapeamento de Causas

1. O usuário clica no botão Mapeamento de Causa, presente na tela Mapeamento de Risco e o sistema abre a tela de Mapeamento de Causa;
2. O sistema exibe a tela com campos já preenchidos, ao salvar o cadastro em Mapeamento de Risco, como Gestor de Risco, Macroprocesso, Processo, Área, Categoria Nível 2 do Risco e o Risco;
3. Há ainda campos a serem preenchidos, como Subprocesso, Causa Padronizada e Causa Detalhada.
4. Após preenchê-los, o usuário clica em Adicionar causa, e a causa aparece na consulta.
5. Caso o usuário queira adicionar mais causas, repete os passos 3 e 4.
6. Caso o usuário deseje excluir uma causa, clica na causa desejada na consulta, e clica em apagar causa selecionada.
6. O sistema preenche automaticamente a data de cadastro da causa com a data atual;
7. O usuário clica no botão “salvar”;
8. O cadastro do mapeamento de causas é salvo no sistema com um código gerado automaticamente.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### Fluxo 3 - Vincular Ambiente de Controle ao risco

1. O usuário clica no botão Ambiente de Controle, presente na tela Mapeamento de Risco, e o sistema abre a tela de vínculos entre ambiente de controle e causas;
2. O sistema exhibe as causas que foram mapeadas para o risco em questão, e o usuário clica no botão “Adicionar mitigador”;
3. O sistema abre uma tela auxiliar, chamada Seleção do mitigador, com uma consulta que exhibe todos os controles cadastrados no sistema. Para refinar a busca, pode-se preencher os filtros, divididos por Categoria, Tipo, Área ou palavra-chave da descrição;
4. O usuário clica no controle desejado e clica em “Vincular mitigador” (caso o controle desejado não exista, o usuário pode clicar em “Cadastrar mitigador”; caso o controle deva ser editado, o usuário pode clicar em “Editar mitigador”;
5. O usuário clica no botão “fechar”;
6. Na tela de ambiente de controle, o controle é adicionado na tela.
7. Para cada causa mapeada que o controle mitigar, o usuário clica na Caixa de Seleção específica;
8. Caso o usuário deseje adicionar outro ambiente de controle, refaz os passos 3 a 7.
9. O usuário clica no botão “salvar”;
10. O cadastro do vínculo do ambiente de controle é salvo no sistema com um código gerado automaticamente.
11. O usuário clica no botão “fechar”;
12. O sistema volta à tela Mapeamento de Risco.

### Fluxo 4 - Cadastrar Questionários de Matriz de Risco

1. O usuário, durante entrevista com o gestor da área a ser mapeada, clica em “Matriz de Risco: Questionário” e o sistema abre o formulário “Avaliação de Riscos: Principal”.
2. No formulário, o usuário escolhe o questionário que deseja cadastrar.
3. Preenche as informações do questionário e clica em salvar.
4. O cadastro do questionário é salvo no sistema com um código gerado automaticamente.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### Fluxo 5 - Definir o tratamento do Risco

1. Depois de preenchidos os questionários qualitativos e quantitativos, o usuário clica em “Resumo”, no formulário “Avaliação de Riscos: Principal”.
2. De acordo com as informações dos questionários, o sistema calcula a exposição final do risco.
3. O usuário define o tratamento a ser dado para o risco e clica em salvar.
4. Caso o tratamento seja diferente de aceitar o risco, planos de ação devem ser vinculados, seguindo o mesmo padrão para ambientes de controle.
5. O usuário clica em salvar e o cadastro da avaliação é salvo no sistema.

### **III.2.3 Fluxos de Eventos Alternativos**

O fluxo alternativo “pode representar um caminho não usual, uma exceção ou uma condição de erro [...] e é mais difícil de identificar que o fluxo básico” (ROSENBERG; SCOTT, 1999, p.48, tradução nossa).

#### Fluxo 1 - Cadastrar Risco

1. Na tela de Mapeamento de Risco o usuário clica em Cadastrar/Editar Risco;
2. O sistema abre a tela de Cadastro de Risco com os campos a serem preenchidos, divididos em Categoria Nível 1 e Nível 2 e Descrição do Risco;
3. O usuário clica no botão “salvar”;
4. O cadastro do risco é salvo no sistema com um código gerado automaticamente.
5. O usuário clica no botão “fechar” e está de volta à tela de Mapeamento de Risco, podendo escolher o Risco cadastrado no respectivo combo;

#### Fluxo 2 - Cadastrar Causa Detalhada

1. Na tela de Mapeamento de Causa o usuário clica em Cadastrar Causa Detalhada;
2. O sistema abre a tela de Cadastro de Causa com os campos a serem preenchidos, divididos em Categoria Nível 2, Causa Padronizada e Causa Detalhada;



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

3. O usuário define se a atividade dessa causa é executada por Áreas Internas da empresa, e/ou por empresas terceirizadas, devendo, nesse caso, escolher a empresa (o cadastro é realizado apenas pela área de Gestão de Risco Operacional);
4. O usuário clica no botão “salvar”;
5. O cadastro da causa é salvo no sistema com um código gerado automaticamente.
6. O usuário clica no botão “fechar” e está de volta à tela de Mapeamento de Causa, podendo escolher a causa detalhada cadastrada, no respectivo combo;

### Fluxo 3 - Cadastrar Ambiente de Controle

1. O usuário clica no botão Ambiente de Controle: Novo Cadastro, presente na tela principal, ou no botão Cadastrar mitigador, presente na tela Seleção do mitigador e o sistema abre a tela de cadastro de ambiente de controle;
2. O sistema exibe os campos a preencher, divididos em Categoria (se o ambiente é Atividade de Controle, Instrumento Mitigador, Contingência ou Seguro), Tipo, Nome, Área, Descrição, Atuação (Preventiva ou Detectiva), Automatização, Periodicidade de execução, Aplicabilidade;
3. O usuário clica no botão “salvar”;
4. O cadastro do ambiente de controle é salvo no sistema com um código gerado automaticamente.

### Fluxo 4 - Cadastro de Questionário de Terceiros Relevantes

1. O usuário clica no botão Terceiros Relevantes: Novo Questionário, presente na tela principal, ou no botão “Novo Questionário”, presente na tela Edição de Questionário sobre Terceiros e o sistema abre a tela de cadastro;
2. A tela exibe os campos a serem preenchidos, divididos em Nome do Terceiro (mostra apenas as empresas já cadastradas no sistema), Atividades, Macroprocesso, Processo, Área, campos do questionário e a Relevância do Terceiro;
3. O usuário clica no botão “salvar”;
4. O cadastro do questionário é salvo no sistema com um código gerado automaticamente.
5. O usuário clica no botão “fechar”;

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

6. O sistema volta à tela Seleção do mitigador.

### Fluxo 5 - Emitir Relatório

1. Caso o usuário queira gerar relatório para enviar para a área de Controles Internos, por exemplo, ele clica no botão do Relatório desejado;
2. A tela exibe filtros para refinarem a busca: por área (Empresa, Vice-Presidência, Diretoria,...), macroprocesso e processo, e Status do risco (Ativo, Em edição, Cancelado);
3. Ao preencher os filtros desejados, o usuário clica em “Gerar Relatório”.
4. O sistema abre o Relatório, que exibe todos os riscos existentes e outras informações de acordo com o tipo do relatório selecionado para os filtros selecionados;
5. O usuário clica em Imprimir relatório e o envia para a área de Controles Internos.

## III.3 REQUISITOS NÃO FUNCIONAIS

Os requisitos não funcionais identificados para o sistema estão elencados a seguir:

*Agilidade na navegação.* A ferramenta deve usada durante as entrevistas entre a área de Mapeamento de Risco e os gestores das áreas mapeadas, o que exige rapidez e agilidade do sistema para que todas as informações relevantes levantadas durante o mapeamento sejam armazenadas, podendo ser consultadas e alteradas no futuro.

*Flexibilidade nas consultas e relatórios.* A área de Gestão de RO deve analisar se algum registro foi incluído, alterado ou excluído erroneamente por algum usuário, para poder orientar a maneira correta de se fazer, e a área de Controles Internos, após receberem os dados dos controles, realiza teste para verificar a efetividade dos controles. Por isso, as áreas devem receber as informações necessárias para realizarem seus trabalhos, e a adição ou exclusão de dados nas consultas e relatórios devem ser rapidamente implantadas.

*Implantação rápida de alterações.* A metodologia utilizada está em desenvolvimento pela área de Risco Operacional e deve ser aprovada pela Comissão de Risco Operacional da empresa e o Banco Central, e por esse motivo está sujeita a alterações, que devem ser rapidamente aplicadas na ferramenta.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

*Interface intuitiva*, para que o usuário aprenda facilmente a funcionalidade do programa e saiba onde estão todos os botões e ações que deve fazer, para não perder tempo procurando.

*Base única de informações*. Todos os cadastros realizados na ferramenta devem ser armazenados em um único lugar, o que facilita a supervisão das informações e da utilização do sistema, assim como o gerenciamento dos riscos.

*Guarda e resgates de mapeamentos passados*. Ao realizar um novo trabalho de mapeamento em uma área, os funcionários devem analisar os mapeamentos anteriores, para fazerem as alterações necessárias. Assim, será possível fazer uma comparação no tempo, verificando se algum risco deixou de existir ou surgiu, se um ambiente de controle não existe mais, etc.

### III.4 BENEFÍCIOS E LIMITAÇÕES

O levantamento dos benefícios é importante para identificar o valor do sistema e se o investimento realizado nele será vantajoso (PAULA FILHO, 2003). A ferramenta desenvolvida pelos funcionários de RO apresenta diversos benefícios, principalmente quando comparada com o programa anteriormente utilizado, como:

*Integração com outras áreas*, como Modelagem de RO, responsável por disponibilizar valores das perdas por processo, por área e por risco, dados a serem utilizados para calcular a exposição dos riscos; Auditoria, responsável por disponibilizar se há pontos de auditoria por processo, por área e por risco, para também calcular a exposição dos riscos; Controles Internos, que deve receber informações sobre os controles, avaliados pelos gestores das áreas mapeadas durante as entrevistas com os funcionários de Mapeamento RO e, após testes dos controles nas próprias áreas, disponibilizar a avaliação mais adequada dos controles, para alterar os dados na ferramenta; Engenharia de Processos, que fornece todos os processos por área da empresa, já que os mapeamentos de cada risco são realizados por processo e não mais por área (como é feito atualmente), dando uma visão mais detalhada e abrangente de todos os riscos existentes; Recursos Humanos, que torna acessível a estrutura organizacional, já que para todos os cadastros a serem registrados na ferramenta a área deve ser fornecida.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

*Melhor divulgação da base de dados*, através de consultas e relatórios, que facilitam o trabalho dos funcionários de Gestão de RO de supervisionar todos os registros gravados na ferramenta, verificando que os usuários estão realizando um bom mapeamento. Além do mais, as consultas e relatórios poderão ser enviados para a área de Controles Internos, que, como já mencionado, necessitam dos dados sobre os controles, para os gestores das áreas mapeadas, que necessitam validar o trabalho realizado, e ainda para os diretores e Alta Administração da empresa, para se tornarem cientes do assunto.

*Maior personalização e flexibilidade de alterações* do sistema para a empresa, pois a ferramenta é desenvolvida por funcionários da área de risco, que entendem da metodologia de risco operacional baseada nos Acordos de Basiléia e também do Mapeamento de Risco, por estarem em contato direto com os funcionários do mapeamento. Assim, qualquer alteração a ser realizada no sistema, seja por mudança na metodologia, seja por sugestão ou reclamação da área de Mapeamento de Risco, é rapidamente realizada pela equipe.

*Maior padronização* da estrutura de gestão de risco operacional, através da imposição de limites de escolhas para a área analisada, processo, risco e causa, nos cadastros de mapeamento de risco, anteriormente realizados no sistema anterior em campos texto. Para a escolha da área em que está sendo realizado o estudo do mapeamento, o usuário percorre campos, preenchendo desde a filial da empresa, vice-presidência, até níveis mais abaixo da estrutura, que termina em coordenação, e o sistema indica o nome da área, código do organograma (fornecido pela área de RH, para facilitar o manuseio das informações) e responsável da área.

Para a escolha do processo o usuário poderá escolher apenas os macroprocessos e processos disponíveis de acordo com a listagem elaborada pela área Gestão de RO. A existência de padrões diferentes nas empresas do grupo dificulta a análise e a comparação entre os riscos por processo e o mesmo padrão de nomenclatura deve então ser utilizado em todas as empresas, possibilitando a criação de uma estrutura mais organizada e eficiente, além da redução do número de riscos, e, portanto, melhor comparação entre eles, devido ao foco em processo.

A descrição do risco é feita livremente pelo usuário, mas o cadastro de um mapeamento de risco é realizada baseado nas classificações de Nível 1 e 2 do risco em questão, que segue metodologia de Dicionário de Eventos de RO, criada pela empresa. A identificação das causas de cada risco ocorre de forma semelhante, com classificações de cada causa detalhada em Causa Padronizada e Categoria Nível 2, seguindo o Dicionário de Causas

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

padronizada da Gestão de RO. Essa padronização possibilita uma unificação de nomenclatura na instituição, podendo-se comparar, para os riscos identificados, por exemplo, quais as causas mais freqüentes, ou inexistentes em atividades semelhantes.

Com o trabalho de padronização de riscos e causas e unificação na visão de processos, haverá a redução de registros não apenas de causas, como também de riscos, facilitando o trabalho de gestão da área, com uma linguagem padronizada na Organização, governança mais eficiente, além de atendimento aos requisitos de Basiléia II: Estrutura padronizada de Controle de Risco Operacional.

*Menor subjetividade nas avaliações.* Com a redução de campos de livre digitação na ferramenta, orientação da área de Gestão de RO e dos desenvolvedores da ferramenta, e elaboração de travas no sistema com o objetivo de reduzir e até evitar erros dos usuários, o trabalho de mapeamento de risco minimizará a subjetividade nas avaliações, facilitando e aprimorando o trabalho de gerenciamento de riscos operacionais.

*Melhor gestão dos riscos.* A ferramenta será uma base única de informações e por isso facilitará o trabalho de gerenciamento e supervisão da área de Gestão de Risco Operacional e o de mapeamento dos analistas, além de proporcionar maior conhecimento dos riscos existentes para a Alta Administração, através das saídas do sistema, como relatórios e consultas.

*Minimização de tempo em levantamento dos riscos.* Devido à padronização no cadastro de mapeamento de risco, que leva à redução do número de riscos cadastrados no sistema, como comentando anteriormente, juntamente com a facilidade de uso e layout da ferramenta, o levantamento dos riscos será facilitado, e assim, o tempo para se mapear os riscos da área será reduzido. Com essa economia de tempo, os funcionários de mapeamento terão maior disponibilidade para realizar outras tarefas.

Além dos benefícios, é importante também identificar as limitações do sistema, para evitar “falsas expectativas por parte do cliente e dos usuários” (PAULA FILHO, 2003, p. 95). Por ser de desenvolvimento interno, os desenvolvedores não são especializados em tecnologia da informação, e, por isso, o sistema possui diversas limitações, como falhas em praticidade e inteligência de programação.

Com as informações do cadastro dos planos de ação, como as datas planejadas e efetivas de início e término, que serão geradas nas consultas em Acompanhamento dos Planos de Ação, os gestores devem ser notificados dias antes que seus planos de ação estão vencendo, para informarem o andamento do projeto. Caso os planos tenham sido cancelados

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

ou prorrogados, devem justificar para a área de Gestão de RO. Porém, a ferramenta em Access não faz o envio da notificação automática para o gestor, e o funcionário de gestão de RO o realiza manualmente, por envio de e-mail.

Além de Risco Operacional, outras áreas, como Auditoria, Controles Internos, Segurança da Informação, Administração de Contingência e Processo também estão diretamente envolvidas com RO, e seria, portanto, interessante que a ferramenta fosse utilizada por todas elas. Entretanto, foi desenvolvida apenas para a área de RO, impedindo, assim, a administração de riscos em um único lugar.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### IV DESENVOLVIMENTO

Neste capítulo é apresentada a solução técnica adotada para o sistema de gestão de risco operacional da empresa.

São mostradas a seguir as principais tabelas do sistema e o relacionamento entre elas e a descrição de seus campos, para facilitar o entendimento do programa.

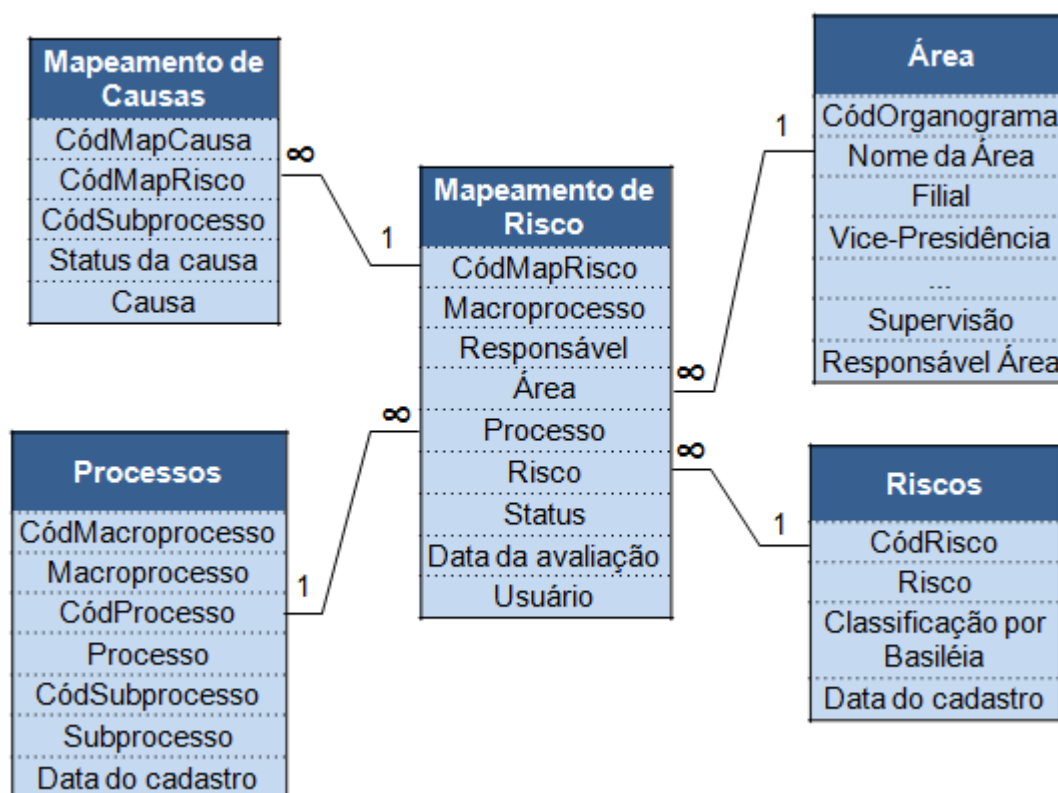


Figura 11 - Tabela Mapeamento de Risco e relacionamentos

#### MAPEAMENTO DE RISCO

Principal tabela da ferramenta, Mapeamento de Risco se relaciona com quase todas as outras tabelas direta ou indiretamente. A Figura 11 exibe a tabela e seus relacionamentos diretos. Seu campo chave é o ‘CódMapRisco’, campo numérico que gera um registro único para cada risco mapeado que será usado como referência nas demais tabelas. Responsável é um campo texto, que contém o nome do gestor responsável pelo risco mapeado. ‘Macroprocesso’ e ‘Processo’ são campos numéricos que geram registros únicos para cada macroprocesso e processo da empresa, e estão relacionados com a tabela Processos. ‘Área’

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

possui o código estrutural do organograma da empresa, utilizado como referência em diversas tabelas e está ligado à tabela Área. ‘Risco’ contém o código de cada risco que existe e se relaciona com a tabela Riscos. ‘Status’ representa o status do mapeamento do risco, que pode ser ativo, cancelado ou em edição. E, por último, ‘Data da avaliação’ e ‘Usuário’ armazenam informações da data em que foi realizado o cadastro e o usuário que o efetuou.

### **RISCOS**

Contém os riscos cadastrados e editados pelos usuários no formulário “Cadastro de Riscos”. ‘CódRisco’ é o campo chave, com o código de cada tipo de risco existente. ‘Risco’ contém o nome (descrição) do risco; ‘Classificação de Basiléia’ contém a classificação do risco pelo dicionário de eventos de Basiléia II, e se relaciona com a tabela ‘Dicionário de Eventos’. Por último, ‘Data do cadastro’ contém a data da inclusão do risco no banco de dados.

### **PROCESSOS**

Tabela auxiliar gerenciada pela área de Metodologia e Projetos, contém a lista padronizada dos Macroprocessos, Processos e Subprocessos das empresas. Os campos ‘CódMacroprocesso’, ‘CódProcesso’ e ‘CódSubprocesso’ são campos numéricos que contém um registro único para cada macroprocesso, processo e subprocesso da empresa, respectivamente. ‘Macroprocesso’, ‘Processo’ e ‘Subprocesso’ contém o nome de cada um. ‘Data do cadastro’ contém a data da inclusão dos campos no banco de dados.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

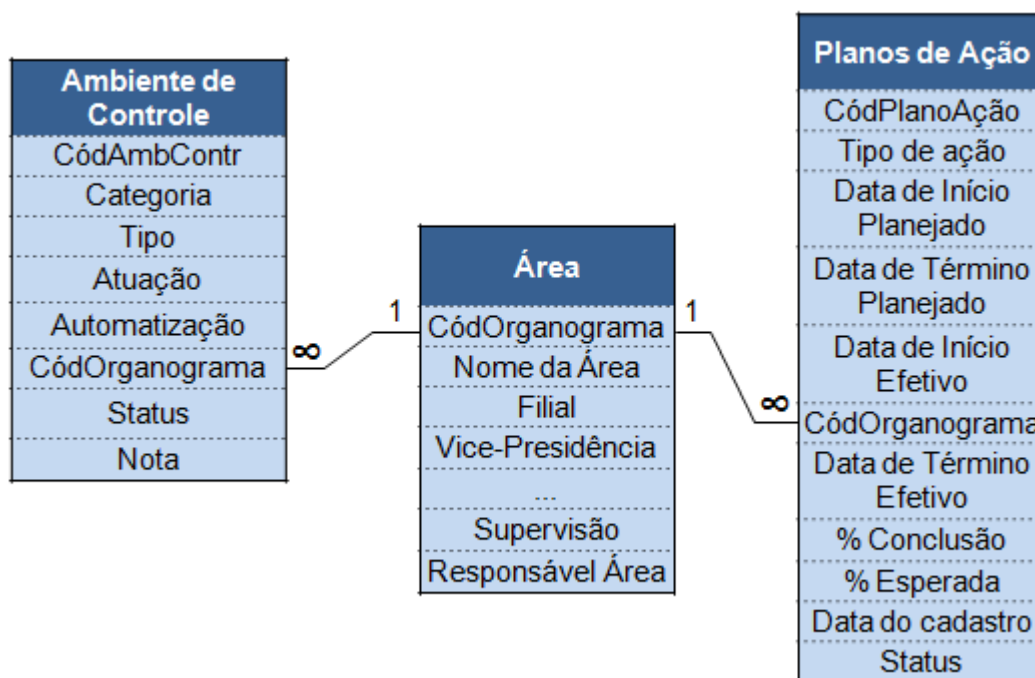
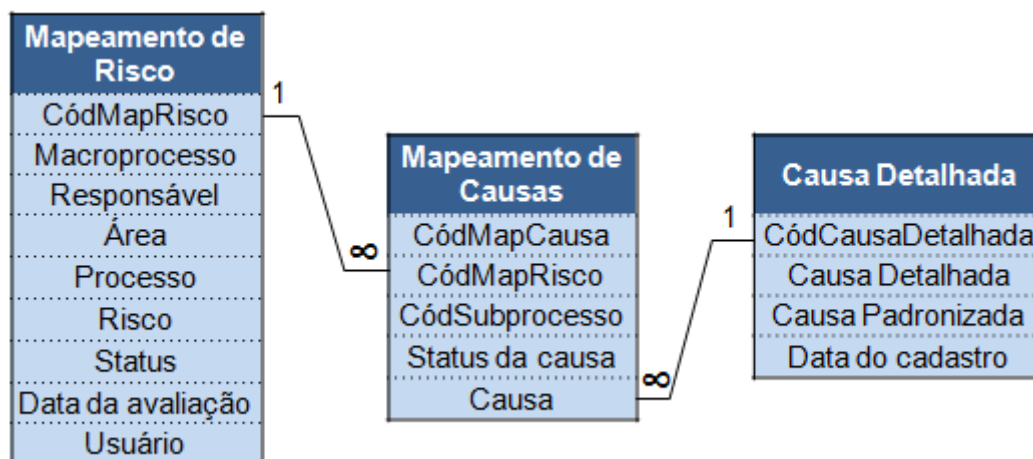


Figura 12 - Tabela Área e relacionamentos

### ÁREAS

Tabela auxiliar da ferramenta, seus registros são administrados pela área de Metodologia e Projetos e atualizados mensalmente, de acordo com as informações enviadas pela área de Recursos Humanos, contendo alterações das áreas da empresa, com as saídas e entradas de funcionários. Seu campo chave é o 'CódOrganograma', campo numérico que gera um registro único para cada área da empresa e que se relaciona às tabelas 'Mapeamento de Risco', como mostrando anteriormente, 'Ambiente de Controle', 'Plano de Ação' e 'Terceiros: Avaliação'. Esta última não é relevante para o trabalho e por isso não está presente na Figura 12. 'Nome da Área' é um campo texto que contém o nome da área. 'Filial' é um campo numérico com a identificação da filial da empresa. 'Responsável Área' indica o nome do funcionário que responde pela área. Os outros campos se relacionam à estrutura organizacional, que vai da vice-presidência à supervisão.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL



**Figura 13 - Tabela Mapeamento de Causas e relacionamentos**

### MAPEAMENTO DE CAUSAS

A tabela Mapeamento de Causas contém os registros de todas as causas vinculadas e desvinculadas a um mapeamento de risco. Seu campo chave é 'CódMapCausa', que gera um código único para cada causa mapeada. O campo 'CódMapRisco' contém o código do mapeamento de risco a que a causa está vinculada e se relacionam à tabela Mapeamento de Risco. 'CódSubprocesso' contém o código do subprocesso a que a causa está vinculada e se relaciona à tabela Processos. 'Status da causa' é um campo texto que representa o status, que pode ser oficial ou cancelada. E 'Causa' é um código numérico que contém o código da causa detalhada.

### CAUSAS DETALHADAS

A tabela contém os registros das causas detalhadas cadastradas e editadas no formulário "Cadastro de Causas Detalhadas". O campo chave é 'CódCausaDetalhada', que gera um código único para cada causa detalhada cadastrada. 'Causa detalhada' é o campo texto que contém a descrição da causa detalhada. 'Causa padronizada' é um campo numérico que contém a classificação por causas padronizada e se relaciona à tabela Causa Padronizada. 'Data do cadastro' armazena informações da data em que foi realizado o cadastro no banco de dados.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

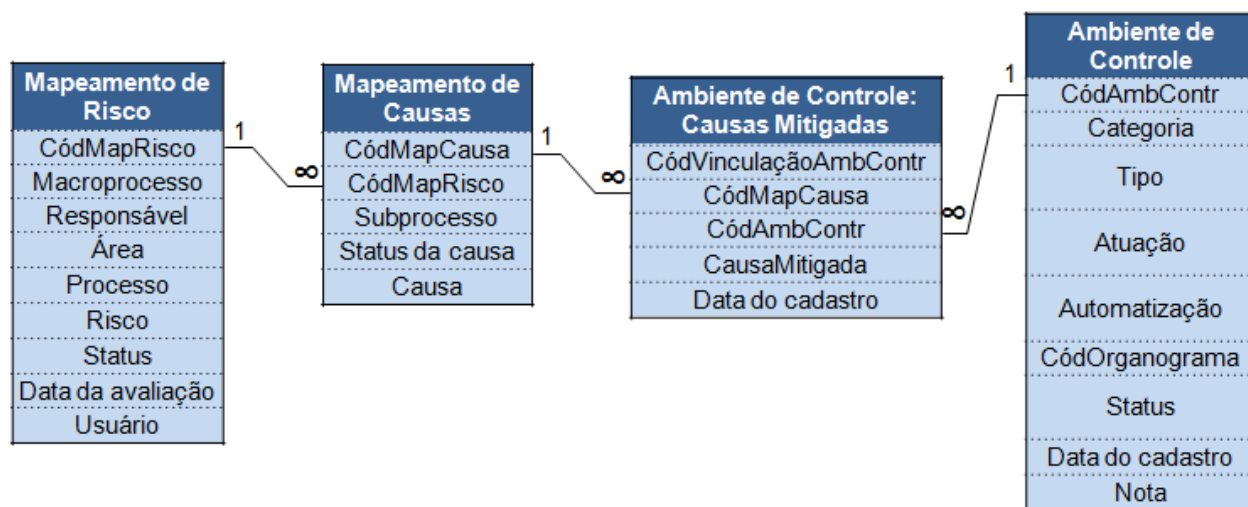


Figura 14 - Tabela Ambiente de Controle: Causas Mitigadas e relacionamentos

### AMBIENTES DE CONTROLE: CAUSAS MITIGADAS

Mostra os ambientes de controles vinculados a um mapeamento de risco e os relacionamentos com as causas mapeadas. Seu campo chave é ‘CódVinculaçãoAmbContr’, que gera um código único para cada controle vinculado. ‘CódMapCausa’ contém o código da causa a que o controle está vinculado e que está relacionada à tabela “Mapeamento de Causas”. ‘CódAmbContr’ é um campo numérico que contém o registro único do ambiente de controle vinculado, relacionado à tabela Ambiente de Controle. ‘CausaMitigada’ contém o valor 1, caso a causa seja mitigada pelo controle, ou o valor 0, caso a causa já tenha sido desvinculada. ‘Data do cadastro’ armazena informações da data em que foi realizada a vinculação no banco de dados.

### AMBIENTE DE CONTROLE

A tabela possui todos os ambientes de controle cadastrados no formulário “Cadastro de ambientes de controle” e suas respectivas características. O campo chave é ‘CódAmbContr’, que gera um código único para cada ambiente de controle registrado. ‘Categoria’ é um campo numérico que pode ser Atividade de Controle, Instrumento Mitigador Contingência ou Seguro. ‘Tipo’ é um campo numérico que representa o tipo do ambiente de controle. ‘Atuação’ é um campo numérico que representa a atuação do ambiente: detectivo ou preventivo. ‘Automatização’ é um campo numérico que possui os seguintes valores: Automatizado, Parcialmente automatizado ou Manual. O campo ‘CódOrganograma’ contém o

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

registro da área a que o controle está vinculado e se relaciona com a tabela Áreas. ‘Status’ contém o status do ambiente, que pode ser ativo, cancelado ou em edição. ‘Data do cadastro’ possui a data em que o plano foi registrado na base de dados. Por último, ‘Nota’ possui valores entre 0 e 10, que dependem das características do controle.

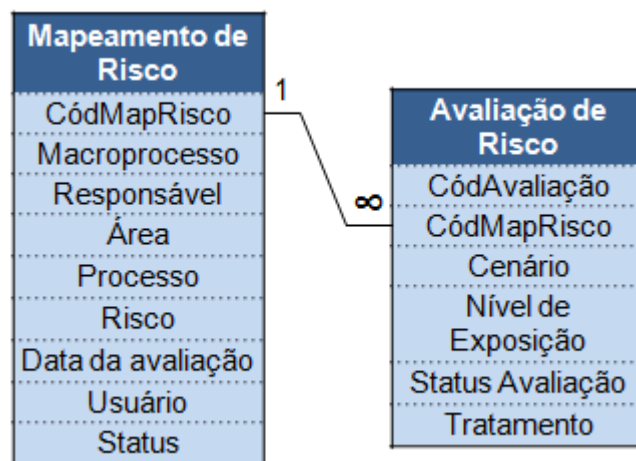
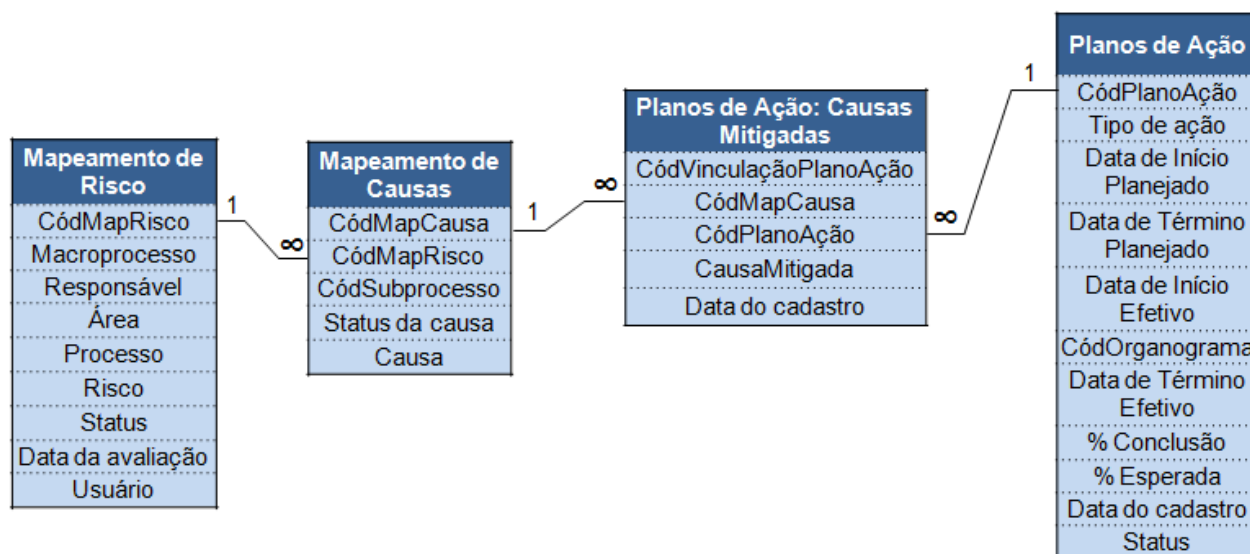


Figura 15 - Tabela Avaliação de Risco e relacionamentos

### AVALIAÇÃO DO RISCO

A tabela contém os registros das avaliações dos mapeamentos de risco para cada cenário (Esperado e Stress) e suas respectivas informações, como Exposição do Risco e Tratamento. O campo chave é ‘CódAvaliação’, que gera um código único para cada avaliação de risco que for vinculada ao mapeamento. ‘CódMapRisco’ contém o código do mapeamento de risco a que a avaliação está vinculada. ‘Cenário’ é um campo texto que representa a visão em que a avaliação do risco foi realizada: cenário esperado ou stress. ‘Nível de Exposição’ é um campo texto que contém a exposição do risco, que pode ser baixo, médio, alto ou extremo. ‘Status da avaliação’ é um campo texto com o status, que pode ser em edição, caso a avaliação esteja em andamento, ou concluída, caso esteja terminada. ‘Tratamento’ é um campo texto que representa o tratamento a ser dado ao risco, que pode ser Aceitar, Reduzir, Transferir ou Evitar.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL



**Figura 16 - Tabela Planos de Ação: Causas Mitigadas e relacionamentos**

### PLANOS DE AÇÃO: CAUSAS MITIGADAS

A tabela contém os planos de ação vinculados a um mapeamento de risco e os relacionamentos com as causas mapeadas. Seu campo chave é ‘CódVinculaçãoPlanoAção’, que gera um código único para cada plano vinculado. ‘CódMapCausa’ contém o código da causa a que o plano está vinculado e que está relacionada à tabela Mapeamento de Causas. ‘CódPlanoAção’ é um campo numérico que contém o registro único do plano de ação vinculado, relacionado à tabela Plano de Ação. ‘CausaMitigada’ contém o valor 1, caso a causa seja mitigada pelo plano, ou o valor 0, caso a causa não seja. ‘Data do cadastro’ armazena informações da data em que foi realizada a vinculação no banco de dados.

### PLANOS DE AÇÃO

A tabela possui todos os planos de ação cadastrados no formulário “Cadastro de plano de ação” e suas respectivas características. O campo chave é ‘CódPlanoAção’, que gera um código único para cada plano de ação registrado. ‘Tipo de ação’ é um campo numérico que representa o tipo do plano. ‘Data de Início Planejado’ é um campo data/hora, que contém a data em que se pretende iniciar a implantação do plano de ação. ‘Data de Término Planejado’ é um campo data/hora, que contém a data em que se pretende concluir a implantação do plano de ação. ‘Data de Início Efetivo’ é um campo data/hora, que contém a data em que o plano foi efetivamente iniciado. ‘Data de Término Efetivo’ é um campo data/hora, que contém a data

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

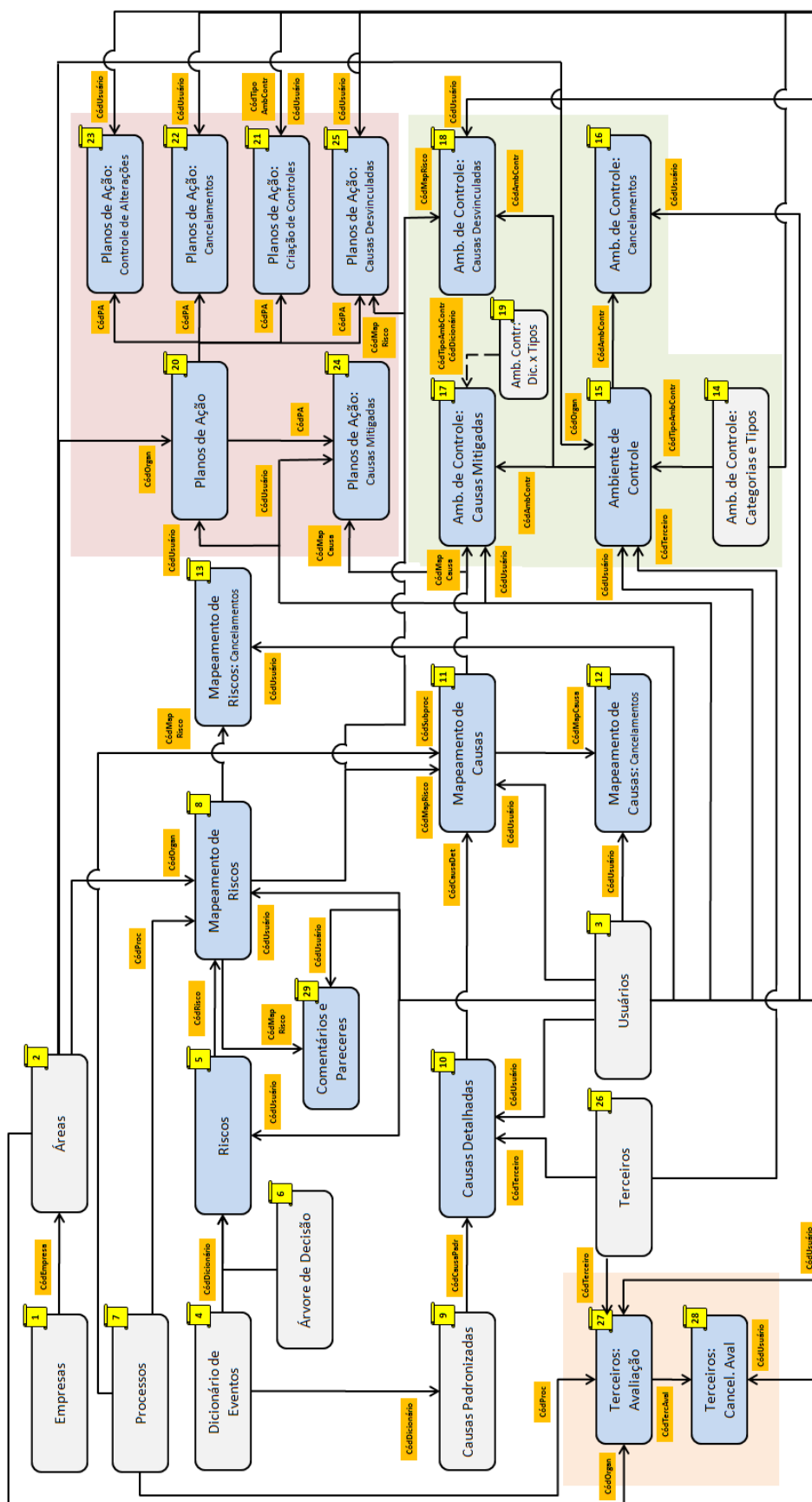
em que o plano foi efetivamente concluído. O campo ‘CódOrganograma’ contém o registro da área a que o plano está vinculado e se relaciona com a tabela Áreas. ‘% Conclusão’ contém a porcentagem de andamento do plano que foi realizada até o momento. O campo ‘% Conclusão Esperada’ possui o valor percentual do andamento do plano que deveria ter sido realizada até o momento. ‘Status’ contém o status do plano, que pode ser ativo, cancelado ou em edição. ‘Data do cadastro’ possui a data em que o plano foi registrado na base de dados.

Como as tabelas são dependentes umas das outras, a criação de cada campo deve ser bem estudada para não prejudicar o funcionamento do programa, que por este motivo, foi desenvolvido em etapas, como será explicado no próximo capítulo.

A Figura 18 mostra o relacionamento entre todas as tabelas da ferramenta, e por quais campos ele ocorre. As tabelas representadas por azul escuro são provenientes dos cadastros realizados pelos usuários no sistema, enquanto as representadas em azul claro são de responsabilidade da área de ‘Metodologia e Projetos’: os usuários não possuem acesso para alterá-las.

Fica clara a importância da tabela Mapeamento de Riscos, que por ser a principal do programa, é a que possui o maior número de vínculos diretos com outras tabelas. Através dos campos ‘CódOrganograma’, ‘CódProcesso’, ‘CódRisco’ e ‘CódUsuário’, ela se relaciona com as tabelas “Áreas”, “Processos”, “Riscos” e “Usuários”, enquanto com o campo ‘CódMapRisco’ se relaciona com as tabelas “Comentários e Pareceres”, “Mapeamento de Riscos: Cancelamentos” e “Ambiente de Controle: Causas Desvinculadas”.

Considerando que algumas tabelas da figura não são muito relevantes e não foram sequer mencionadas no trabalho, a figura possui mais um caráter de visualização e entendimento dos relacionamentos entre as tabelas do programa.



**Figura 17 - Tabelas do sistema e seus relacionamentos**

**Figura 18 - Tabelas do sistema e seus relacionamentos**

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### V IMPLANTAÇÃO DO SISTEMA

Antes de iniciar o desenvolvimento do novo programa, foi realizada uma análise dos pontos vulneráveis e falhas do sistema que ainda era utilizado pela área e que deveriam ser corrigidos, levando em consideração a metodologia de mapeamento de RO utilizada pela empresa e as necessidades dos usuários, para se chegar à funcionalidade de cada formulário. A área de ‘Metodologia e Projetos’, responsável pelo desenvolvimento do programa, era composta por quatro pessoas. Todas participaram da etapa de planejamento do funcionamento do programa, mas apenas duas ficaram a cargo da programação. O sistema foi dividido em módulos:

- Mapeamento de Riscos e Causas
- Ambiente de Controle
- Planos de Ação e Terceiros Relevantes
- Avaliação de Riscos
- Relatórios

Um módulo só poderia ser iniciado quando o anterior já estivesse sido concluído e homologado. Essa decisão foi de extrema importância, já que a ordem dos módulos não foi escolhida por acaso: cada módulo depende do anterior. Os relatórios, por exemplo, necessitam das informações de todos os outros módulos.

Além disso, cada etapa foi devidamente documentada, contendo o funcionamento de cada formulário e os problemas encontrados, para facilitar a construção dos módulos seguintes e o trabalho de um novo programador, que viesse a ser contratado pela área.

A autora deste trabalho foi contratada para a vaga de um dos (dois) programadores e o primeiro módulo do programa já estava concluído. Por sua falta de conhecimento em Access e programação em Visual Basic, além de Basileia e RO, foi necessário primeiramente um estudo teórico em literatura especializada, como livros, artigos, políticas e normas disponibilizados na internet ou na própria empresa. O antigo programador permaneceu por alguns dias trabalhando em conjunto com a autora, para explicar o que havia sido feito até então e tirar eventuais dúvidas que surgissem na construção dos primeiros formulários, facilitando o entendimento e a familiarização com a linguagem do programa.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A partir de então, pode contribuir com a análise e estudo do funcionamento dos outros módulos e a construção no Access dos respectivos formulários, tabelas, consultas e relatórios. A autora ficou responsável pelo desenvolvimento da maior parte do restante do programa e o outro programador pela homologação do que ia sendo construído, já que possuía muitas responsabilidades além do programa. O oposto diversas vezes ocorreu: caso ele desenvolvesse algo no programa, a autora deveria realizar os testes.

Durante todo o processo de implantação, o programa anterior continuou a ser utilizado, para que o trabalho de mapeamento de risco não fosse interrompido. Após as etapas de homologação do novo sistema e sua respectiva disponibilização, ele foi descontinuado.

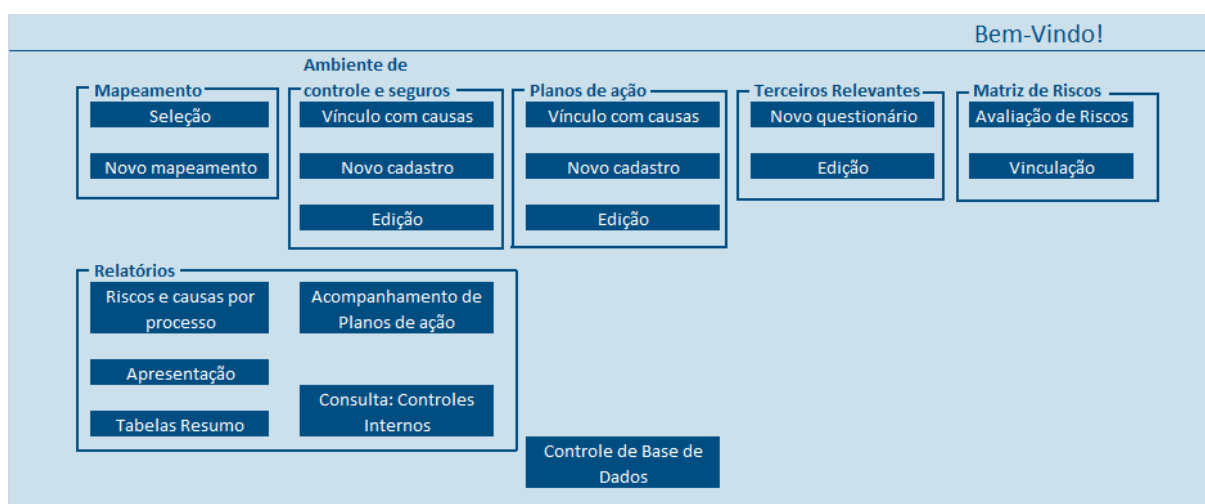
## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### VI NAVEGAÇÃO NO PROGRAMA

Neste capítulo é mostrado o funcionamento do protótipo, com seus principais formulários e relatórios, criados para facilitar o trabalho de mapeamento dos riscos dos funcionários de Gestão de Risco Operacional.

#### VI.1 MENU PRINCIPAL

O Menu Principal apresenta as principais funções da ferramenta: Mapeamento de Riscos e Causas, Ambiente de controle e seguros, Planos de ação, Terceiro Relevantes, Matriz de Riscos e Relatórios. Abaixo são descritas as sessões apresentadas no Menu Principal.



**Figura 19 - Menu Principal**

#### MAPEAMENTO DE RISCOS E CAUSAS

- “Seleção”, o usuário, através dos filtros de Área, Macroprocesso e Processo, tem a opção de visualizar e editar determinado risco.
- “Novo mapeamento” possibilita o usuário cadastrar ou editar um novo risco e suas causas, o acesso aos vínculos com componentes de ambiente de controle e planos de ação (este apenas para visualização), além da inclusão de comentário ou parecer.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### AMBIENTE DE CONTROLE E SEGUROS

É possível realizar um novo cadastro, edição de componentes do ambiente de controle e a vinculação com as causas dos riscos previamente mapeados.

### PLANOS DE AÇÃO

É possível realizar um novo cadastro, edição de planos de ação e a visualização dos vínculos com as causas dos riscos previamente mapeados.

### TERCEIROS RELEVANTES

Pode-se cadastrar ou editar o Questionário sobre Empresas Terceirizadas.

### MATRIZ DE RISCOS

- “Vinculação” tem por finalidade determinar o responsável pelas avaliações;
- “Avaliação de Riscos”, onde são preenchidos os Questionários Qualitativos e Quantitativos de Probabilidade e Severidade.

### RELATÓRIOS

Estão disponíveis para impressão, os seguintes relatórios:

- Riscos e causas por processo;
- Apresentação, que exhibe os riscos e causas por processo, além dos correspondentes ambientes de controle, avaliação de risco e planos de ação vinculados.

Estão disponíveis para visualização:

- Tabelas resumo, com as informações mais relevantes dos mapeamentos de riscos, ambientes de controle, planos de ação e nível de risco, apresentadas em tabelas dinâmicas;
- Acompanhamento de planos de ação, onde é verificado o andamento dos planos, para que as devidas cobranças por e-mail da área de Gestão de RO sejam enviadas aos gestores responsáveis.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Consulta de CI, que será encaminhada para a área de Controles Internos, responsável por testar a efetividade dos ambientes de controles.

### VI.2 MAPEAMENTO DE RISCOS E CAUSAS

#### VI.2.1 A partir de um novo cadastro

Para cadastrar um novo mapeamento, os seguintes passos devem ser seguidos:

**Mapeamento do Risco**

Gestor(es) do risco

Incluído em 01/08/2011 Alterado em 01/08/2011 Status Em edição ▼

☒ Mapeamento proveniente da base de perdas

**Processo**

Macroprocesso  Processo  Alterar estrutura do processo

**Área**

Código de organograma  Nome da Área  Responsável pela área  Escolher área

**Risco**

Categoria Nível 2 de risco  Cadastrar novo risco

Descrição do risco  Editar risco

**Vínculos**

Causas mapeadas 0 Ambientes de controle e seguros 0 Planos de ação 0 Incluir comentário ou parecer

Salvar Sair

**Figura 20 - Cadastro de Mapeamento de Risco**

- Definir gestor(es) do risco
- Escolher Macroprocesso
- Escolher Processo
- Escolher área

Ao clicar, o formulário Seleção da Área é aberto.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Figura 21 - Seleção da Área

Os filtros de Área respeitam a estrutura hierárquica emitida pela área de Recursos Humanos. Ao associar a área ao cadastro, o nível hierárquico ótimo a ser definido deve ser verificado.

- Escolher a Categoria Nível 2
- Escolher a Descrição do Risco.
  - Cadastrar Risco

Caso o risco desejado não esteja presente na lista, o usuário deve cadastrá-lo, clicando em “Cadastrar novo risco”. O formulário “Cadastro de Riscos” é aberto, e para preencher as Categorias Nível 1 e 2 do risco, o usuário clica em “Árvore de decisão para classificação de Eventos de Risco Operacional”.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A interface do formulário 'Cadastro de Risco' possui um cabeçalho azul com o título 'Cadastro de Risco' em branco. Abaixo, há três campos de texto: 'Descrição do Risco' (grande), 'Incluído em' (com o valor '26/04/2011') e 'Alterado em' (com o valor '26/04/2011'). Uma seção centralizada, delimitada por uma caixa azul, contém o título 'Classificação pelo Dicionário de Eventos de Risco Operacional' e dois campos para 'Categoria Nível 1' e 'Categoria Nível 2'. À direita desta seção, há uma caixa amarela com o texto 'Árvore de Decisão para classificação de Eventos de Risco Operacional'. Na base, há dois botões cinza: 'Salvar' e 'Sair'.

Figura 22 - Cadastro de Risco

O formulário Árvore de Decisão é aberto, com uma pergunta inicial na tela, que reflete as informações do normativo da empresa. Ao responder em Sim ou Não, uma segunda pergunta surge na tela (que depende da resposta anterior) e o processo continua, até as Categorias Nível 1 e 2 serem automaticamente preenchidas. Nesse caso, clica-se em Incluir, e o sistema volta para Cadastro de Riscos, com as Categorias com os valores selecionados, e o usuário preenche a Descrição do Risco.

A interface do formulário 'Árvore de Decisão para Classificação de Eventos de Risco Operacional' possui um cabeçalho azul com o título 'Árvore de Decisão para Classificação de Eventos de Risco Operacional' em branco. Abaixo, há um campo de texto grande para 'Pergunta inicial'. À direita, há quatro botões empilhados: 'Sim', 'Não', 'Voltar' e 'Reiniciar'. Abaixo do campo de texto, há dois campos para 'Categoria Nível 1' e 'Categoria Nível 2'. À direita, há um botão 'Incluir'.

Figura 23 - Árvore de Decisão

- Editar Risco

Caso o risco esteja presente na lista, mas o analista deseje alterar a sua descrição, ele deve clicar em “Editar risco”.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Cadastro de Risco

---

Descrição do Risco <div style="border: 1px solid black; padding: 2px;">Fraude na cotação de operações</div>	Incluído em <div style="border: 1px solid black; padding: 2px;">26/04/2011</div>	Alterado em <div style="border: 1px solid black; padding: 2px;">26/04/2011</div>
--	---	---

Classificação pelo Dicionário de Eventos de Risco Operacional
 

Categoria Nível 1  

1. Fraude interna

 Categoria Nível 2  

1.1 Atividade não autorizada

Risco registrado nos seguintes mapeamentos
 

Macroprocesso	Nome da Área	Processo
Macroprocesso 2	Área X	Processo 2.3

Salvar

Sair

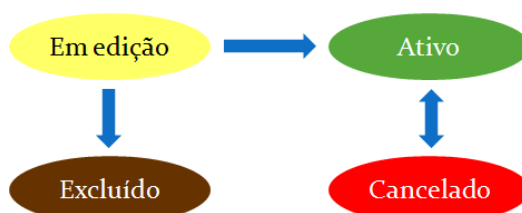
**Figura 24 - Editar risco**

Após alterar a descrição do risco, o usuário deve salvar o registro, que é imediatamente atualizado em “Mapeamento de Risco”.

- Definir o Status

Todos os formulários de cadastramento possuem informações mínimas para cadastro, de forma a possibilitar que as mesmas sejam recuperadas pelo usuário. Para o cadastro de um mapeamento de risco com o Status “Em edição” (valor inicial), os campos de ‘Processo’ (Macroprocesso e Processo), ‘Área’ (Código de organograma, Nome da área e Responsável pela área) e ‘Risco’ (Categoria nível 2, Descrição do risco) devem ser preenchidos, ou o sistema não permite o salvamento do registro.

Para alterar o Status do mapeamento, o sistema realiza algumas checagens, não permitindo a troca, caso algo não esteja conforme. As possibilidades de alterações entre status respeitam a seguinte regra:



**Figura 25 - Regra de Alteração entre Status**

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

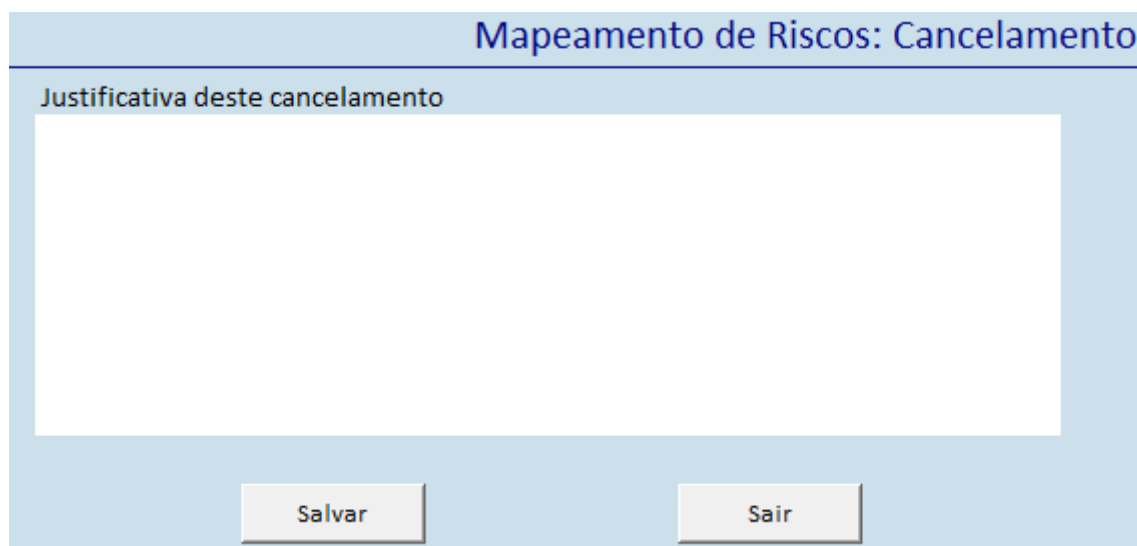
### Troca de “Em edição” para “Ativo”

Para realizar a alteração, os campos de ‘Processo’, ‘Área’ e ‘Risco’ devem ser preenchidos, além de ‘Gestor(es) do risco’.

### Troca de “Ativo” para “Cancelado”

Ao alterar de “Ativo” para “Cancelado”, o sistema exibe uma mensagem de confirmação, para evitar um cancelamento desnecessário.

Caso o usuário confirme que deseja cancelar o mapeamento, o formulário Mapeamento de Risco: Cancelamentos é aberto e a justificativa deve ser preenchida.



O formulário, intitulado "Mapeamento de Riscos: Cancelamento", possui um campo de texto grande para a "Justificativa deste cancelamento". Na base do formulário, há dois botões: "Salvar" e "Sair".

Figura 26 - Cancelamento de Mapeamento de Risco

### Troca de “Cancelado” para “Ativo”

Ao reativar um risco cancelado, o sistema exibe a seguinte mensagem, que apresenta a justificativa do cancelamento do mapeamento.

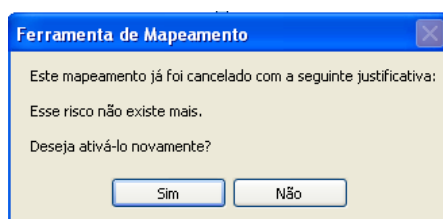


Figura 27 - Justificativa cancelamento do mapeamento



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A regra de alterações entre Status é aplicável a todos os formulários que possuem esse campo. Casos que apresentarem exceções serão detalhados em seus itens específicos

- Clicar em Salvar

Quando o mapeamento do risco for salvo, a mensagem abaixo é exibida.

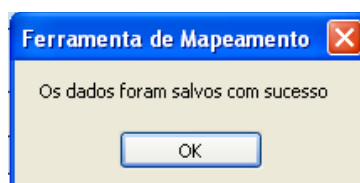


Figura 28 - Salvar mapeamento

### VI.2.2 A partir de um mapeamento existente

#### VI.2.2.1 Seleção do mapeamento

Selecionar Mapeamento

Empresa	Nome da Área	Macroprocesso	Processo	Status	Categoria Nível 2	Risco
Área 1	Macroprocesso 1	Processo 1.1	Ativo	3.1. Relações traba	Risco 1	
Área 1	Macroprocesso 1	Processo 1.2	Ativo	7.1. Captura, execu	Risco 2	
Área 1	Macroprocesso 1	Processo 1.3	Ativo	1.1. Atividade não-	Risco 3	
Área 1	Macroprocesso 1	Processo 1.4	Ativo	6.1. Falhas de Siste	Risco 4	
Área 1	Macroprocesso 2	Processo 2.1	Cancelado	4.4. Falhas em pro	Risco 5	
Área 2	Macroprocesso 2	Processo 2.2	Ativo	7.5. Parceiros com	Risco 6	
Área 2	Macroprocesso 2	Processo 2.3	Ativo	3.2. Segurança do e	Risco 7	
Área 2	Macroprocesso 2	Processo 2.4	Em edição	6.3. Violação do sis	Risco 8	
Área 2	Macroprocesso 3	Processo 3.1	Ativo	2.1. Estelionato, ro	Risco 9	
Área 3	Macroprocesso 3	Processo 3.2	Ativo	1.3. Apropriação in	Risco 10	
Área 3	Macroprocesso 4	Processo 4.1	Ativo	7.5. Parceiros com	Risco 11	
Área 3	Macroprocesso 4	Processo 4.2	Ativo	4.5. Atividade cons	Risco 12	
Área 4	Macroprocesso 4	Processo 4.3	Cancelado	1.3. Apropriação in	Risco 13	
Área 4	Macroprocesso 5	Processo 5.1	Ativo	5.1. Desastres e ev	Risco 14	
Área 5	Macroprocesso 6	Processo 6.1	Ativo	6.2. Interrupção da	Risco 15	

\*Clicar duas vezes para editar o risco selecionado

Empresa

Vice-Presidência

Diretoria I

Diretoria II

Superintendência

Gerência I

Gerência II

Gerência III

Supervisão

Coordenação

Macroprocesso

Processo

Dados cadastrais

Status

Data do cadastro inicial

Data do cadastro final

Limpar filtros

Sair

Figura 29 - Seleção do mapeamento

O formulário em questão exibe todos os riscos cadastrados no sistema, classificados de acordo com o 'Nome da Área', 'Macroprocesso', 'Processo', 'Status', 'Categoria Nível 2' e 'Descrição do Risco'. Para facilitar a visualização, o usuário pode utilizar os filtros de estrutura organizacional, macroprocesso, processo, status e data de cadastro.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Ao clicar duas vezes em um registro, o formulário Mapeamento de Risco é aberto, exibindo as informações do mapeamento escolhido.

### VI.2.3 Mapeamento de causas

**Mapeamento de Causas**

Gestor(es) do risco Gestor	Incluído em 1/8/2011	Alterado em 1/8/2011	Status Ativo ▼
-------------------------------	-------------------------	-------------------------	-------------------

Área		
Código de organograma 010.030	Nome da Área Área 4	Responsável pela área Responsável

Risco	
Categoria Nível 2 de risco 1.1 Atividade não autorizada	
Descrição do risco Fraude na formalização de contratos	

Processo		
Macroprocesso Macroprocesso 2	Processo Processo 2.3	Subprocesso ▼

Causas				
Causa Padronizada ▼				<div style="text-align: center;">Adicionar causa</div> <div style="text-align: center;">Apagar causa selecionada</div> <div style="text-align: center;">Cadastrar nova causa selecionada</div> <div style="text-align: center;">Editar causa detalhada</div>
Causa detalhada ▼				
Causas mapeadas				
Terceiro	Relevância	Subprocesso	Causa Padronizada	Causa Detalhada
Áreas Internas	Não aplicável	Subprocesso 2.3.1	Causa Padronizada 1	Causa Detalhada 1.1
Terceiro 1	Relevante	Subprocesso 2.3.2	Causa Padronizada 2	Causa Detalhada 2.1

Salvar

Sair

**Figura 30 - Mapeamento de Causas**

Para adicionar uma causa, cinco passos devem ser seguidos:

- Escolher Subprocesso
- Escolher Causa padronizada
- Escolher Causa detalhada
  - Cadastrar causa detalhada

Caso a causa detalhada não se encontre no campo, o usuário deve clicar em “Cadastrar nova causa detalhada” e o formulário é aberto, com a Categoria Nível 2 do risco preenchida.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Cadastro de causas detalhadas**

Causa detalhada  Incluído em 16/05/2011 Alterado em 16/05/2011

Classificação padrão de causas

Categoria Nível 2  
1.3 Apropriação indébita, roubo, furto

Causa Padronizada

Atividade executada por  
☒ Áreas internas  
☒ Empresas terceirizadas

Terceiros

Terceiro 1  Terceiro 2  Terceiro 3

Figura 31 - Cadastro de causa detalhada

O usuário escolhe a Causa Padronizada e preenche a Causa Detalhada, que é um campo livre. Por fim, deve ser selecionado quem executa a atividade: Áreas Internas da empresa, e/ou Empresas terceirizadas.

- Editar causa detalhada

Caso o usuário deseje editar uma causa detalhada existente, ele deve selecioná-la e clicar em “Editar causa detalhada”. O analista altera a descrição da causa detalhada e/ou o executor da atividade.

**Cadastro de causas detalhadas**

Causa detalhada  
Pagamento em desacordo à política vigente

Incluído em 16/05/2011 Alterado em 16/05/2011

Classificação padrão de causas

Categoria Nível 2  
1.3 Apropriação indébita, roubo, furto

Causa Padronizada  
Liberação fraudulenta de valor

Atividade executada por  
☒ Áreas internas  
☒ Empresas terceirizadas

Terceiros

Terceiro 1  Terceiro 2  Terceiro 3

Causa detalhada registrada nos seguintes mapeamentos

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Risco
Macroprocesso 1	Área 5	Processo 1.3	1.1 Atividade não au	Divulgação de inform
Macroprocesso 3	Área 2	Processo 3.2	1.3 Apropriação indé	Pagamento fraudule

Figura 32 - Edição de causa detalhada

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Clicar em Adicionar causa

A causa é, então, imediatamente adicionada na lista de Causas mapeadas, classificada por Terceiro, Relevância (definida no questionário de terceiro relevantes), Subprocesso e Causa Padronizada.

Para apagar uma causa, basta selecioná-la na lista de Causas mapeadas e clicar em “Apagar causa detalhada”. Caso possua vínculo com controles ou planos de ação, ela não poderá ser excluída, a menos que seja providenciada a desvinculação (se aplicável).

- Clicar em Salvar

## VI.3 AMBIENTE DE CONTROLE E SEGUROS

### VI.3.1 Novo Cadastro

**Cadastro do Ambiente de controle**

Categoria: ☒ Atividade de controle ☐ Instrumento mitigador ☐ Contingência ☐ Seguro

Tipo de controle: Acesso físico

**Informações gerais**

Nome:  Incluído em: 03/05/2011 Alterado em: 03/05/2011 Status: Em edição

Nota:

**Área responsável**

Código do organograma:  Nome da área:  Responsável pela área:  Escolher área:

☐ Controle executado por empresa terceirizada Terceiro:

**Características**

Descrição: Restrição de acesso de  ao(à)(s)  , por meio de  , com o objetivo de  .

Atuação: ☒ Preventiva ☐ Detectiva

Automatização: ☒ Manual ☐ Parcialmente automatizado ☐ Automático

Possibilidade de automatização:

Aplicabilidade:  Periodicidade de execução:

**Afirmações de auditoria**

☐ Integridade ☐ Validade ☐ CUT-OFF ☐ Registro ☐ Valoração ☐ Apresentação ☐ Salvaguarda de Ativos ou Registro de Passivos

**Figura 33 - Cadastro do ambiente de controle**

Para cadastrar um novo ambiente de controle, deve-se seguir 7 etapas:

- Escolher Categoria e Tipo
- Escolher área
- Preencher a Descrição do ambiente de controle

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Definir a Atuação e o Nível de Automatização

O ambiente de controle pode atuar sobre as causas que mitiga de forma ‘Preventiva’, caso seja implementado com a finalidade de impedir possíveis ocorrências de riscos, ou ‘Detectiva’, caso seja implementado com a finalidade de detectar possíveis falhas antecipando a ocorrência do risco. Já o “Nível de Automatização” pode ser ‘Manual’, ‘Parcialmente automatizado’ ou ‘Automatizado’.

De acordo com as características do ambiente de controle, chega-se a um valor para a sua Nota, que irá impactar na avaliação da classificação de probabilidade qualitativa do risco

- Definir a Empresa terceirizada, caso o controle seja executado por uma empresa terceirizada
- Definir o Status

O funcionamento da troca de Status funciona analogamente ao de Mapeamento de Risco.

- Clicar em Salvar

### VI.3.2 Edição

O formulário “Seleção do componente” exibe todos os controles cadastrados no sistema, classificados de acordo com a ‘Categoria’, ‘Tipo’, ‘Nome da Área’, ‘Status’, ‘Nome’ e ‘Descrição’. Para facilitar a visualização, o usuário pode utilizar os filtros de categoria, tipo, área e Palavra-Chave da Descrição. Ao clicar no ambiente desejado, é mostrado o número de causas mitigadas por esse controle, assim como os mapeamentos aos que está vinculado.

#### Seleção do componente

Filtro por

Categoria ▼

Tipo ▼

Área ▼

Palavra-chave

Categoria	Tipo	Nome	Status	Descrição
Atividade de Controle	Alçadas	Alçadas para pagamento	Ativo	Validação por alçada
Atividade de Controle	Autorização	Autorização do(a)(s)	Ativo	Autorizada, realizada
Atividade de Controle	Conciliação	Conciliação do(a)(s)	Cancelado	Conciliação, realizada
Atividade de Controle	Validação	Validação do(a)(s)	Ativo	Validação, realizada
Contingência	Guarda e/	Guarda/Backup de a	Ativo	Guarda/Backup de a
Instrumento mitigador	Aviso	Aviso do(a)(s) aberto	Em edição	Aviso do(a)(s) aberto
Instrumento mitigador	Treinamento	Treinamento contínuo	Ativo	Treinamento, aplicação
Seguro	Seguro	Seguro contra danos	Ativo	

Limpar filtros

Editar mitigador

Número de causas mitigadas pelo controle 3

Controle vinculado aos seguintes mapeamentos

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Risco
Macroprocesso 1	Área 5	Processo 1.3	1.1 Atividade não autorizada	Divulgação de informação sem a
Macroprocesso 3	Área 2	Processo 3.2	1.3 Apropriação indébita, roubo	Pagamento fraudulento

**Figura 34 - Seleção do componente do ambiente de controle**

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Para editá-lo, basta clicar em “Editar mitigador” e o formulário “Cadastro do ambiente de controle e seguros” é aberto, com todas as informações do ambiente preenchidas.

Qualquer alteração deve ser devidamente estudada, pois impactará em todos os riscos com os quais o controle está associado.

### VI.3.3 Vínculo com causas

O objetivo desse formulário é estabelecer o relacionamento dos componentes do ambiente de controle com as respectivas causas do mapeamento de riscos.

Para facilitar a explicação será mostrado o caso de um risco recém mapeado, com apenas causas e nenhum controle vinculados.

**Vínculos entre ambientes de controle e causas**

**Filtros**  

Área

Macroprocesso

Processo

Limpar filtros

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Riscos	Status
Macroprocesso 1	Área 1	Processo 1.1	1.1 Atividade não au	Desvio no p	Ativo <span style="float: right;">▲</span>
Macroprocesso 1	Área 2	Processo 1.2	5.1 Desastres e even	Falhas na d	Ativo <span style="float: right;">■</span>
Macroprocesso 2	Área 3	Processo 2.1	3.1 Relações trabalh	Falha na bo	Ativo <span style="float: right;">▼</span>

**Controles e instrumentos mitigadores**  
Avaliação   
  
Forma de atuação  

Simultânea ▼

Subprocessos e Causas detalhadas		
SB 1.1.1	SB 1.1.2	SB 1.1.3
Causa detalhada 1	Causa detalhada 2	Causa detalhada 3

notas  
% mitigação  
Nota de mitigação  
  

Adicionar mitigador

**Figura 35 - Vínculos entre ambientes de controle e causas - Adicionar mitigador**

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Para adicionar um ambiente, deve-se clicar em “Adicionar mitigador” e a tela “Seleção do componente” é aberta. Caso o analista deseje adicionar um ambiente de controle que não se encontra na lista, ele pode criar um novo ou editar um existente, através dos botões “Cadastrar novo mitigador” e “Editar mitigador”, respectivamente.

**Seleção do componente**

Filtro por

Categoria

Tipo

Área

Palavra-chave

Limpar filtros

Categoria	Tipo	Nome	Status	Descrição
Atividade de Controle	Alçadas	Alçadas para pagamento	Ativo	Validação por alçada
Atividade de Controle	Autorização	Autorização do(a)(s)	Ativo	Autorizada, realizada
Atividade de Controle	Conciliação	Conciliação do(a)(s)	Cancelado	Conciliação, realizada
Atividade de Controle	Validação	Validação do(a)(s)	Ativo	Validação, realizada
Contingência	Guarda e/	Guarda/Backup de a	Ativo	Guarda/Backup de a
Instrumento mitigador	Aviso	Aviso do(a)(s) aberto	Em edição	Aviso do(a)(s) aberto
Instrumento mitigador	Treinamento	Treinamento contínuo	Ativo	Treinamento, aplicação
Seguro	Seguro	Seguro contra danos	Ativo	

Cadastrar novo mitigador    Editar mitigador    **Vincular mitigador**

Número de causas mitigadas pelo controle

Controle vinculado aos seguintes mapeamentos

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Risco
Macroprocesso 1	Área 5	Processo 1.3	1.1 Atividade não autorizada	Divulgação de informação sem a
Macroprocesso 3	Área 2	Processo 3.2	1.3 Apropriação indébita, roubo	Pagamento fraudulento

Sair

**Figura 36 - Vincular ambiente de controle**

Após encontrar o ambiente desejado, o usuário deve selecioná-lo e então clicar em “Vincular mitigador”, como mostra a Figura 36, e o ambiente será adicionado no formulário anterior.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Vínculos entre ambientes de controle e causas**

**Filtros**  
 Área  Macroprocesso  Processo  Limpar filtros

**Riscos**

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Riscos	Status
Macroprocesso 1	Área 1	Processo 1.1	1.1 Atividade não au	Desvio no p	Ativo <span style="float: right;">▲</span>
Macroprocesso 1	Área 2	Processo 1.2	5.1 Desastres e even	Falhas na d	Ativo
Macroprocesso 2	Área 3	Processo 2.1	3.1 Relações trabalh	Falha na bo	Ativo <span style="float: right;">▼</span>

**Controles e instrumentos mitigadores**  
 Avaliação   
 Forma de atuação

**Subprocessos e Causas detalhadas**

	SB 1.1.1	SB 1.1.2	SB 1.1.3
Causa detalhada	Causa detalhada	Causa detalhada	Causa detalhada
	1	2	3

	SB 1.1.1	SB 1.1.2	SB 1.1.3
Controle 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Controle 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Nota de mitigação

Adicionar mitigador
Recalcular notas
Salvar
Sair

**Figura 37 - Vínculos entre ambientes de controle e causas**

O relacionamento entre os ambientes de controle e as causas é realizado através da vinculação entre eles, ao clicar na caixa de seleção localizada entre os mesmos. Além dos vínculos, o analista deve preencher a aplicabilidade dos controles, ao lado da descrição do ambiente (destacada na Figura 37 com a cor verde) e a Forma de atuação, que pode ser:

- Simultânea - quando os componentes do ambiente de controle são executados ao mesmo tempo;
- Complementar - Quando os componentes do ambiente de controle não são capazes de prevenir ou detectar isoladamente a ocorrência de um evento.

Para controles que atuam de forma complementar, a soma das aplicabilidades deve ser sempre igual a 100%. Os vínculos dos ambientes de controle com as causas, sua forma de atuação e seu nível de automatização determinam a nota que é atribuída para a avaliação da mitigação de causas de um risco, que impacta no questionário qualitativo.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

No exemplo, o primeiro controle mitiga as causas 1 e 3, enquanto o segundo mitiga as causas 1 e 2, e os controles atuam sobre o risco de forma simultânea: ambos atuam 100% sobre as causas, gerando uma avaliação da mitigação de causas com o valor de 8,2.

Caso o analista deseje desvincular um dos componentes do ambiente de controle, ele deve desmarcar as caixas de seleção do controle que estão selecionadas e clicar em Salvar. O formulário “Ambiente de Controle: Desvinculados” é aberto, exigindo a justificativa. Ao voltar para o formulário anterior, o ambiente já não é mais exibido na tela.

O formulário, intitulado "Ambiente de Controle: Desvinculados", possui um fundo azul claro. No topo, há uma barra de título com o mesmo nome. Abaixo, há dois campos de entrada lado a lado: "Risco" e "Descrição do Risco". Logo abaixo, há um campo rotulado "Ambiente de controle" que contém o texto "Controle 2". Abaixo disso, há um campo rotulado "Justificativa" que é uma caixa de texto grande e vazia. Na base do formulário, há dois botões: "Salvar" à esquerda e "Sair" à direita.

**Figura 38 - desvincular ambiente de controle**

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### VI.4 PLANOS DE AÇÃO

#### VI.4.1 Novo Cadastro

Cadastro de plano de ação

**Informações gerais**

Nome do plano de ação  Incluído em 26/04/2011 Alterado em 26/04/2011 Status Em edição ▼

Código do organograma  Nome da área  Responsável pela área  Escolher área

☒ Solicitado pela Comissão de Riscos Operacionais Data da solicitação

**Características**

Tipo de ação

Descrição da ação

Benefícios da implantação

**Acompanhamento**

Início planejado  Conclusão planejada

Início real  Conclusão real

% Conclusão  % Conclusão esperada

**Lista de alterações - Cronograma e Andamento**

Data	Usuário	Campo alterado	Comentário
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Imprimir lista de alterações

**A implantação deste plano de ação criará os seguintes controles**

Categoria ▼ Tipo ▼ Adicionar controle

Controles mapeados

Categoria	Tipo
<input type="text"/>	<input type="text"/>

Apagar controle

Salvar
Sair

**Figura 39 - Cadastro de plano de ação**

Para cadastrar um novo plano, os seguintes passos devem ser seguidos:

- Preencher o Nome do plano de ação
- Escolher a área: análogo aos formulários anteriores.
- Definir o Tipo de ação: Tecnologia, Recursos Humanos, Processos, Infraestrutura e Ativos ou Outros.
- Preencher Descrição da ação.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

- Preencher Benefícios da implantação
- Implantação de novos controles

Caso a implantação deste plano de ação contribua com a criação de novos controles, eles devem ser adicionados no cadastro. Para tal, é necessário escolher a categoria e o tipo de controle a ser criado, e clicar em Adicionar controle. Para apagar, basta selecionar o item exibido na lista “Controles mapeados” e clicar em “Apagar controle”.

- Definir o Acompanhamento

Os campos de datas planejadas e reais e “% Conclusão” devem ser preenchidos pelo usuário. O “% Conclusão esperada” é então calculada, e, com base nesses dados, verifica-se se o ambiente está dentro do prazo ou atrasado.

O envio de e-mails para o acompanhamento dos planos de ação para os gestores das áreas é de responsabilidade da célula “Metodologia e Projetos”, e por isso os cadastros devem ser continuamente atualizados pelos analistas de “Mapeamento de RO”.

- Solicitação pela Comissão de Riscos Operacionais

Caso o plano de ação tenha sido solicitado pela Comissão de RO, a opção deve ser marcada e a data da solicitação preenchida.

- Definir o Status

A alteração de Status segue a mesma inteligência de “Mapeamento de Risco” e “Cadastro do Ambiente de Controle e seguros”. Caso o plano de ação possua vínculos com o mapeamento de riscos, ele não poderá ser cancelado.

- Clicar em Salvar

### VI.4.2 Edição

O formulário “Seleção do plano de ação” exhibe todos os planos cadastrados no sistema, classificados de acordo com o ‘Tipo de ação’, ‘Nome da Área’, ‘Status’, ‘Nome’ e ‘Descrição’. Para facilitar a visualização, o usuário pode utilizar os filtros de tipo, área e Palavra-Chave da Descrição. Ao clicar no registro desejado, é mostrado o número de causas mitigadas por ele, assim como os mapeamentos aos que está vinculado.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Seleção do plano de ação**

**Filtro por**

Tipo de ação

Área

Palavra-chave

Tipo de ação	Nome	Status	Descrição
Processos	Abertura das inform	Ativo	Abertura das inform
Processos	Aditivo contratual	Ativo	Autorizada, realizad
Processos	Aquisição de uma fe	Cancelado	Conciliação, realizad
Recursos Humanos	Reestruturação da ár	Ativo	Reestruturação da ár
Recursos Humanos	Contratação de colab	Ativo	Contratação de um c
Tecnologia	Arquivos de Carga	Em edição	Os arquivos de carga
Infraestrutura e Ativos	Atividades	Ativo	Atividades realizada
Tecnologia	Aquisição de softwa	Ativo	Aquisição de softwa

Número de causas mitigadas pelo controle

Controle vinculado aos seguintes mapeamentos

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Risco
Macroprocesso 1	Área 5	Processo 1.3	1.1 Atividade não autorizada	Divulgação de informação sem a
Macroprocesso 3	Área 2	Processo 3.2	1.3 Apropriação indébita, roub	Pagamento fraudulento

**Figura 40 - Seleção do plano de ação**

Para editá-lo, basta clicar em “Editar plano de ação” e o formulário “Cadastro de plano de ação” é aberto.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Cadastro de plano de ação**

**Informações gerais**

Nome do plano de ação	Incluído em	Alterado em	Status
Sistema de pagamentos	06/01/2010	06/05/2011	Em edição ▼
Código do organograma	Nome da área	Responsável pela área	
010.030	Área 2	Responsável	Escolher área

☐ Solicitado pela Comissão de Riscos Operacionais

**Características**

Tipo de ação  
Tecnologia ▼

Descrição da ação  
Implementação do sistema de pagamentos

Benefícios da implantação  
Maior rastreabilidade dos lançamentos e maior segurança sistêmica

**Acompanhamento**

O plano de ação não foi iniciado e está atrasado.

Início planejado	Conclusão planejada
01/01/2010	31/12/2011
Início real	Conclusão real
% Conclusão	% Conclusão esperada

**Lista de alterações - Cronograma e Andamento**

Data	Usuário	Campo alterado	Comentário
6/5/2011	Mariana	% Conclusão	A porcentagem de
6/5/2011	Mariana	Início real	A data se apresen

Imprimir lista de alterações

**A implantação deste plano de ação criará os seguintes controles**

Categoria	Tipo	
▼	▼	Adicionar controle

Controles mapeados

Categoria	Tipo
Atividade de controle	Conciliação
Atividade de controle	Monitoramento

Apagar controle

Salvar
Sair

Figura 41 - Cadastro de plano de ação

- Alterações em Acompanhamento

Caso o analista altere algum campo de Acompanhamento, o formulário “Planos de ação: Alterações” será aberto, e a justificativa d alteração deve ser preenchida.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Figura 42 - Alteração no plano de ação**

- Lista de alterações – Cronograma e Andamento

A lista exibe todas as alterações realizadas para esse plano de ação nos campos de Acompanhamento. O usuário tem a possibilidade de visualizar e imprimir o histórico de todas as alterações do plano em questão, clicando em “Imprimir lista de alterações”.

Alterações nos planos de ação			
<b>Nome:</b>	Sistema de pagamentos		
<b>Tipo de ação:</b>	Tecnologia		
<b>Descrição:</b>	Implementação do Sistema de Pagamentos que efetuará integração com todos os outros sistemas		
<b>Status:</b>	Ativo		
<b>Conclusão planejada:</b>	21/12/2011		
1) 06/02/2011	Mariana	Início real	A data se apresentava errada
2) 18/05/2011	Mariana	% Conclusão	A porcentagem de conclusão foi atualizada

**Figura 43 - Imprimir alterações do plano de ação**

### VI.4.3 Vínculo com causas

A vinculação de planos de ação a um risco funciona de forma semelhante ao para Ambiente de Controle.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Vínculos entre planos de ação e causas**

**Filtros**  
 Área  Macroprocesso  Processo

**Riscos**  

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Riscos	Status
Macroprocesso 1	Área 1	Processo 1.1	1.1 Atividade não au	Desvio no p	Ativo <input type="button" value="↑"/>
Macroprocesso 1	Área 2	Processo 1.2	5.1 Desastres e even	Falhas na d	Ativo <input type="button" value="↑"/>
Macroprocesso 2	Área 3	Processo 2.1	3.1 Relações trabalh	Falha na bo	Ativo <input type="button" value="↓"/>

**Subprocessos e Causas detalhadas**  

SB 1.1.1	SB 1.1.2
Causa detalhada 1	Causa detalhada 2

**Planos de ação**  

Plano de ação 1	100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
-----------------	-----	-------------------------------------	-------------------------------------

Figura 44 - Vínculos entre planos de ação e causas

Para vincular um plano, deve-se clicar em ‘Adicionar Plano de ação’. Caso o analista deseje adicionar um plano que não se encontra na lista, ele pode criar um novo ou editar um existente, através dos botões ‘Cadastrar novo plano de ação’ e ‘Editar plano de ação’, respectivamente.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**Seleção do plano de ação**

Filtro por

Tipo de ação

Área

Palavra-chave

Tipo de ação	Nome	Status	Descrição
Processos	Abertura das inform	Ativo	Abertura das inform
Processos	Aditivo contratual	Ativo	Autorizada, realizad
Processos	Aquisição de uma fe	Cancelado	Conciliação, realizad
Recursos Humanos	Reestruturação da ár	Ativo	Reestruturação da ár
Recursos Humanos	Contratação de colab	Ativo	Contratação de um c
Tecnologia	Arquivos de Carga	Em edição	Os arquivos de carga
Infraestrutura e Ativos	Atividades	Ativo	Atividades realizada
Tecnologia	Aquisição de softwa	Ativo	Aquisição de softwa

Número de causas mitigadas pelo controle

Controle vinculado aos seguintes mapeamentos

Macroprocesso	Nome da Área	Processo	Categoria Nível 2	Risco
Macroprocesso 1	Área 5	Processo 1.3	1.1 Atividade não autorizada	Divulgação de informação sem a
Macroprocesso 3	Área 2	Processo 3.2	1.3 Apropriação indébita, roub	Pagamento fraudulento

**Figura 45 - Vincular plano de ação**

Após encontrar o plano desejado e clicar em “Vincular plano de ação”, ele é adicionado no formulário anterior. O relacionamento entre os planos de ação e as causas é realizado através da vinculação entre eles, ao clicar na caixa de seleção localizada entre os mesmos. Além dos vínculos, o analista deve preencher a aplicabilidade dos planos, localizada ao lado da descrição do plano. Caso o analista deseje desvincular um plano de ação, ele deve desmarcar as caixas de seleção do plano que estão marcadas e clica em Salvar. O formulário “Planos de ação desvinculados” é aberto, exigindo a justificativa.

**Planos de ação: Desvinculados**

Risco

Plano

Fraude na efetivação de pagamentos	
Sistema de pagamentos	

Justificativa

**Figura 46 - Desvincular plano de ação**



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### VI.5 MATRIZ DE RISCOS

#### VI.5.1 Vinculação

Primeiramente, antes de se iniciar o preenchimento dos questionários qualitativos e quantitativos, é realizada a vinculação dos riscos a um responsável. Ademais, como exige o Banco Central, a avaliação do nível de exposição ao risco operacional poderá ser feita em duas visões: cenário esperado, onde as questões devem ser respondidas baseando-se no que é mais provável de ocorrer e cenário de stress, onde devem ser levadas em consideração situações não previstas com efeitos em cascata, mesmo que extraordinárias.

#### VI.5.2 Avaliação de Riscos

Neste formulário, são escolhidos os riscos que se deseja fazer as avaliações, com a limitação de no máximo 12 riscos para responder os questionários.

#### VI.5.3 Questionário Qualitativo de Probabilidade

Para cada risco, o gestor do processo deve classificar a probabilidade qualitativa, que se baseia em três drivers:

1. Nota para Mitigação das causas de um risco – calculada no item VI.3.3.
2. Existência de perdas operacionais para o risco e o processo nos últimos 12 meses em relação à data de avaliação do risco, conforme valores registrados na Base de Dados de Perdas Operacionais reportados à Área de Modelagem de Risco Operacional. A atualização desses dados na ferramenta é de responsabilidade da célula de “Metodologia e Projetos”.
3. Existência de pontos de auditoria para o risco e o processo – A atualização desses dados na ferramenta é de responsabilidade da célula de “Metodologia e Projetos”, trabalhando em conjunto com a área de Auditoria.

De acordo com os três valores acima, o gestor pode escolher a faixa de probabilidade qualitativa. Com base em seu conhecimento do processo, pode escolher uma faixa mais conservadora.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### **VI.5.4 Questionário Qualitativo de Severidade**

O formulário é dividido em quatro blocos ou perguntas. A cada resposta de um bloco é atribuído um valor (peso), cujo somatório determina a faixa mínima de severidade que poderá ser escolhida pelo gestor.

Os campos Perda bruta e Quase Perdas correspondem à média mensal dos últimos 12 meses (em relação à data de avaliação do risco), dos valores registrados na Base de Dados de Perdas Operacionais reportados à Área de Modelagem de Risco Operacional.

Esses valores serão comparados com a faixa de severidade determinada de acordo com as respostas do gestor, e o valor máximo entre eles irá definir a faixa mínima da classificação: baixa, média, alta ou extrema.

### **VI.5.5 Questionários Quantitativos**

Neste formulário, apenas os riscos cujas Avaliações Qualitativas foram realizadas podem ser visualizados. O gestor deve estimar a probabilidade e a severidade quantitativas do risco para os efeitos/campos preenchidos no questionário de severidade qualitativa.

A probabilidade quantitativa de cada campo depende dos valores dos campos tamanho da amostra e número de defeitos e a severidade quantitativa de cada efeito é um campo livre que deve ser estimada pelo gestor.

Com os valores preenchidos, chega-se na probabilidade quantitativa do risco, que é a ponderação das probabilidades quantitativas pelas severidades quantitativas de cada efeito e na severidade quantitativa do risco, que é a soma das severidades de cada efeito.

O resultado da probabilidade é comparado com os valores de cada faixa de probabilidade para classificação em: rara, improvável, moderada ou provável e o resultado da severidade é comparado com os valores de cada faixa de severidade para classificação em: baixa, média, alta ou extrema.

### **VI.5.6 Resultados: Avaliação de Risco Operacional**

O objetivo desse questionário é calcular o nível de exposição ao risco operacional e identificar o melhor tratamento a ser dado, com a implementação ou não de planos de ação.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A partir dos valores obtidos para a probabilidade e a severidade qualitativos e quantitativos, são definidas a Exposição Qualitativa e a Exposição Quantitativa do risco operacional, respectivamente.

A **Exposição Final** do risco operacional é então definida a partir do valor mais conservador entre a Exposição Qualitativa e Exposição Quantitativa.

Depois de realizada a análise da exposição do risco, deve ser definido o tratamento a ser dado ao risco. Caso o risco tenha um nível de exposição baixo, muitas vezes é mais vantajoso para a empresa aceitá-lo, ao invés de implantar um plano de ação para mitigá-lo, pois esta alternativa pode ser muito custosa. Se o nível de exposição for alto, um plano de ação deve ser vinculado. Para realizar a vinculação, o formulário “Planos de Ação: Causas Mitigadas” é aberto, com funcionamento já explicado no item VI.4.3.

## VI.6 RELATÓRIOS

### VI.6.1 Riscos e Causas por Processo

O relatório exhibe os riscos, suas causas e avaliações, de acordo com os filtros preenchidos (Área, Macroprocesso e/ou Processo).

Relatórios de Riscos e Causas										
<b>Critérios de filtro:</b>	Nome da Área: (Em branco) Macroprocesso: Economia Processo: Projeções Econômicas									
	Nome da Área	Macroprocesso	Processo	Cat N2	Risco	Subprocesso	Causa Detalhada	Exp	Trat.	Cenário Status Aval.
<b>Risco 1 Ativo</b>	Ger. Economia	Economia	Projeções Econômicas	7.1	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Análise equivocada das projeções e indicadores econômicos	A	Não aval.	Esperado Concluído
	Ger. Economia	Economia	Projeções Econômicas	7.1	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Erro de digitação, fórmulas e macros na consolidação das informações em planilha Excel	A	Não aval.	Esperado Concluído
	Ger. Economia	Economia	Projeções Econômicas	7.1	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Utilização de dados incorretos / provenientes de fontes não confiáveis	A	Não aval.	Esperado Concluído
	Ger. Economia	Economia	Projeções Econômicas	7.1	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Utilização de modelos inadequados (cálculos incorretos de projeções / correlações)	A	Não aval.	Esperado Concluído
<b>Risco 2 Ativo</b>	Ger. Economia	Economia	Projeções Econômicas	7.2	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Não enviar, enviar em atraso ou enviar errado o boletim econômico aos clientes elegíveis	A	Não aval.	Esperado Concluído
	Ger. Economia	Economia	Projeções Econômicas	7.2	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas	Divulgação de relatórios	Não observância as normas externas, padrões ou erro na publicação de informações	A	Não aval.	Esperado Concluído

Figura 47 - Relatório de Riscos e Causas

No cabeçalho, estão presentes os filtros que foram preenchidos no formulário. Nesse exemplo, Macroprocesso e Processo foram os filtros escolhidos. O Status do risco se encontra

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

na esquerda do relatório, logo após o número do risco e o cenário é exibido juntamente com outras informações sobre a avaliação do risco.

### VI.6.2 Apresentação

O relatório exibe os riscos de acordo com os filtros preenchidos (Área, Macroprocesso e/ou Processo).

Relatório Apresentação

Macroprocesso:	Economia				
Processo:	Projeções econômicas				
Área:	Ger. Economia				
Categoria Nível 2	7.1. Captura, execução e manutenção de transações	Data cadastro	01/05/2011		
01) Risco (Ativo)	Falhas na elaboração de relatórios, emissão de pareceres e projeções econômicas, devido a erros no(s) seguinte(s) subprocesso(s):				
01.01) Subprocesso	Divulgação de relatórios, causados por:				
01.01.01)	Análise equivocada das projeções e indicadores econômicos (imparcialidade na interpretação dos dados e tendências econômicas)				
01.01.02)	Erro de digitação, fórmulas e macros na consolidação das informações em planilha Excel				
01.01.03)	Utilização de dados incorretos / provenientes de fontes não confiáveis				
01.01.04)	Utilização de modelos inadequados (cálculos incorretos de projeções / correlações)				
Ambiente de Controle e Seguros					
Descrição	Avaliação	Atuação	% Mitigação	Causas mitigadas	
1) Reuniões de alinhamento das tendências e cenários econômicos, com o objetivo de discutir, com um nível de detalhamento maior, as projeções realizadas pela área de Economia: - participação das reuniões de alinhamento da área Comercial - reunião de caixa diária das mesas de posição proprietária - reunião de caixa semanal das mesas de Banking	8,5	Simultânea	100	01.01.01) 01.01.03) 01.01.04)	
2) Feito-conferido do relatório diário, divulgado para reunião de caixa e clientes, por colaboradores distintos da área, antes da publicação do mesmo, analisando as informações prestadas, dados econômicos, justificativas de recomendações, etc.	8,5	Simultânea	100	01.01.01) 01.01.03) 01.01.04)	
3) Padronização das fontes de informações que dão base para as análises econômicas realizadas, de forma que os dados são consultados somente em fontes oficiais	8,5	Simultânea	100	01.01.01) 01.01.03) 01.01.04)	
4) Participação em fóruns, palestras e seminários nacionais e internacionais para discussão das tendências e perspectivas econômicas nacionais e internacionais (Bacen, Anbima, Febraban, FMI, Banco Mundial, etc)	8,5	Simultânea	100	01.01.01) 01.01.03) 01.01.04)	
1 Causa(s) não mitigada(s): 01.01.02)					
Avaliação de Risco					
Cenário	Probabilidade	Severidade	Nível de Risco Final	Tratamento	Status Avaliação
1) Esperado	Não avaliado	Não avaliado	Alto	Não avaliado	Concluído
Planos de ação					
Descrição	Tipo de ação	Conclusão planejada		Causas mitigadas	
1) Revisão dos relatórios econômicos (diário, semanal e mensal) pelas áreas de Marketing e Compliance - Controles Internos, com o intuito de formatar os relatórios de acordo com as normas internas e externas	Processos	30/03/2010		01.01.01) 01.01.02) 01.01.03) 01.01.04)	

Figura 48 - Relatório Apresentação

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Para cada Risco, classificado de acordo com seu Macroprocesso, Processo, Área e Categoria Nível 2, são exibidos:

- **Causas mapeadas:** para cada subprocesso
- **Ambientes de controle:** são exibidos todos os ambientes de controle vinculados, com suas respectivas características: Avaliação, Atuação, Porcentual de Mitigação e Causas mitigadas.
- **Causas não mitigadas:** são exibidas as causas que não são mitigadas por nenhum dos controles vinculados;
- **Avaliação de risco:** para cada Cenário cadastrado, são exibidos os campos Exposição Qualitativa e Quantitativa, Avaliação Nível de Risco, Tratamento e Status da Avaliação.
- **Planos de ação vinculados,** com suas respectivas características: Tipo de ação, data de Conclusão planejada, Vínculo e Causas mitigadas. O parâmetro 'Vínculos' apresenta a informação se, na data de geração do relatório, o plano de ação permanece vinculado ou não

### VI.6.3 Tabelas Resumo

O objetivo das Tabelas Resumo é de facilitar para os analistas a visualização de dados quantitativos dos mapeamentos de risco, ambientes de controle, planos de ação e níveis de risco, através de tabelas dinâmicas. Apenas alguns exemplos são mostrados, para evitar excesso de detalhamento.

#### VI.6.3.1 Status do ambiente de controle e seguros

Status ▼		
Cancelado	Novo	Revisado
+ -	+ -	+ -
Quantidade	Quantidade	Quantidade
1	11	4

Figura 49 - Tabelas Resumo: Status dos ambientes de controle

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

De acordo com o preenchimento das datas inicial e final do mapeamento, realizado pelo usuário, cada ambiente de controle é classificado como:

A) Novo: se o vínculo do ambiente de controle ao risco foi cadastrado entre as datas de início e fim do filtro.

B) Revisado: se o vínculo do ambiente de controle ao risco foi cadastrado anteriormente à data de início do filtro.

C) Cancelado: se o vínculo do ambiente de controle ao risco foi cancelado entre as datas de início e fim do filtro e não foi revinculado, ou seu revínculo ocorreu após a data de fim do filtro.

### VI.6.3.2 Características dos controles e instrumentos mitigadores

Desenho ▾	Automatização ▾			
<input type="checkbox"/> Detectivo	<input type="checkbox"/> Preventivo			
Manual	Automatizado	Manual	Parcialmente automatizado	
+ -	+ -	+ -	+ -	
Quantidade	Quantidade	Quantidade	Quantidade	
2	3	7	2	

**Figura 50 - Tabelas Resumo: Características dos ambientes de controle**

Exibe a quantidade de ambientes de controle, classificados de acordo com sua Atuação (Desenho) e Automatização.

### VI.6.3.3 Tipos de planos de ação

Tipo de Ação ▾							
Infraestrutura e Ativos		Processos		Recursos Humanos		Tecnologia	
+ -		+ -		+ -		+ -	
Quantidade		Quantidade		Quantidade		Quantidade	
1		3		2		1	

**Figura 51 - Tabelas Resumo: Tipos de planos de ação**

Exibe a quantidade de planos de ação, classificados de acordo com seu Tipo de ação.

### VI.6.3.4 Nível do Risco

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

		Cenário ▾	
		Esperado	Stress
		+ -	+ -
ExposiçãoFinal ▾		Contagem de Cenário	Contagem de Cenário
Baixo	+ -	4	1
Médio	+ -	2	4
Alto	+ -	2	5
Extremo	+ -	6	2
Não avaliado	+ -	43	39

Figura 52 - Tabelas Resumo: Nível do Risco por Cenário

Exibe a quantidade de avaliações de risco, classificadas de acordo com seu Nível de Exposição e Cenário, para os filtros selecionados (Macroprocesso, Processo e Área) pelo usuário.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### VI.7 ALTERAÇÕES NA FERRAMENTA

Para que a Ferramenta de Mapeamento sempre possua o desempenho necessário para realizar suas funções, ela passa por manutenções preventivas e corretivas. Durante esses períodos fica indisponível para os usuários. A programação das manutenções segue abaixo:

**Manutenções Preventivas:** São realizadas quinzenalmente às segundas-feiras, entre às 09 e 10 horas da manhã.

Para assegurar um desempenho adequado da ferramenta e garantir a integridade do banco de dados, é necessário compactar e reparar seus arquivos regularmente. Nesse processo, o Access cria um novo arquivo igual ao original (que é deletado) e o renomeia, substituindo o original. Porém, algumas vezes, pode ocorrer uma falha no processo, onde o arquivo original e a cópia são deletados. Para evitar a perda dos arquivos, recomenda-se sempre criar um backup da ferramenta antes que seja realizada a compactação.

**Manutenções Corretivas (pontuais):** São realizadas quando forem identificados erros na ferramenta, que necessitem de correções emergenciais. As datas são acordadas com os usuários.

**Manutenções Corretivas (melhorias):** São realizadas mensalmente, durante todo o dia, no último dia útil de cada mês. Cabe ressaltar que durante essas manutenções, são adicionadas na ferramenta as sugestões feitas pelos usuários, que forem consideradas válidas, assim como possíveis alterações dos critérios e requisitos de utilização.

Toda manutenção realizada é precedida de aviso aos usuários e descrição dos pontos alterados. Um dia antes da realização das manutenções, o arquivo que contém a Ferramenta de Mapeamento deve ser devidamente fechado, para que a programação possa se iniciar às 9h da manhã da data prevista.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### VII TREINAMENTO

Para tornar os analistas de Gestão de Risco Operacional aptos a utilizar a nova ferramenta de mapeamento, foram realizadas reuniões, divididas em três etapas:

- I. Uso da ferramenta para Mapeamento de Riscos, Causas, Ambiente de Controle e Planos de Ação;
- II. Conceituação da Matriz de Riscos;
- III. Uso da ferramenta para a Avaliação de Riscos, Terceiros Relevantes e emissão de relatórios.

A conceituação de Matriz de Riscos utilizada pela empresa era demasiadamente desatualizada, pois não considerava diversos pontos importantes. A área de Gestão de Riscos aplicou diversas alterações na metodologia, deixando-a alinhada com as exigências do Banco Central. A mudança foi encaminhada para a Comissão de Riscos Operacionais e, depois de aprovada, foi explicada para os analistas de Gestão de RO, para já ser implantada nos mapeamentos. Por isso foi reservada uma reunião inteira para discutir apenas a metodologia, antes de mostrar o seu funcionamento na ferramenta.

Após as reuniões, foi disponibilizada uma versão da ferramenta, para os usuários se familiarizem com o novo sistema e tirem eventuais dúvidas. Durante uma semana, os analistas tiveram tempo para se dedicar exclusivamente ao aprendizado dos módulos apresentados da ferramenta. Um funcionário de Metodologia e Projetos, responsável pelo desenvolvimento da ferramenta, ainda ficou à disposição dos analistas, para realizar um treinamento *in loco*.

### MANUAL DO USUÁRIO

Este Manual visa demonstrar todas as funcionalidades do sistema, trazendo um passo a passo desde seu acesso até a utilização detalhada dos formulários e relatórios disponíveis, com o objetivo de informar aos usuários os conhecimentos básicos necessários à utilização do sistema.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Esse documento foi elaborado também para que novos funcionários e pessoas externas à área pudessem entender seu funcionamento, mesmo sem terem participado das reuniões de treinamento ou utilizado a ferramenta.

Além de explicitar detalhadamente como o usuário deve trabalhar no sistema, o manual exibe todas as travas criadas para evitar que um registro seja cadastrado erradamente. Possui mais de 80 páginas e, por esse motivo, não faz parte deste trabalho.

Abaixo é mostrado apenas o início do manual, com a explicação de como acessar o programa.

### ACESSO À FERRAMENTA

O acesso à Ferramenta poderá ser realizado através de três formas distintas, conforme descrevemos abaixo.

#### **a) Acesso via rede**

O usuário deve, no seu computador, entrar no diretório específico da rede, onde ela se encontra disponibilizada:

M:\Riscos\RO Gestão\Ferramenta interna de mapeamento\Versão de produção.

#### **b) Acesso remoto**

Os seguintes passos devem ser seguidos, em qualquer máquina da instituição:

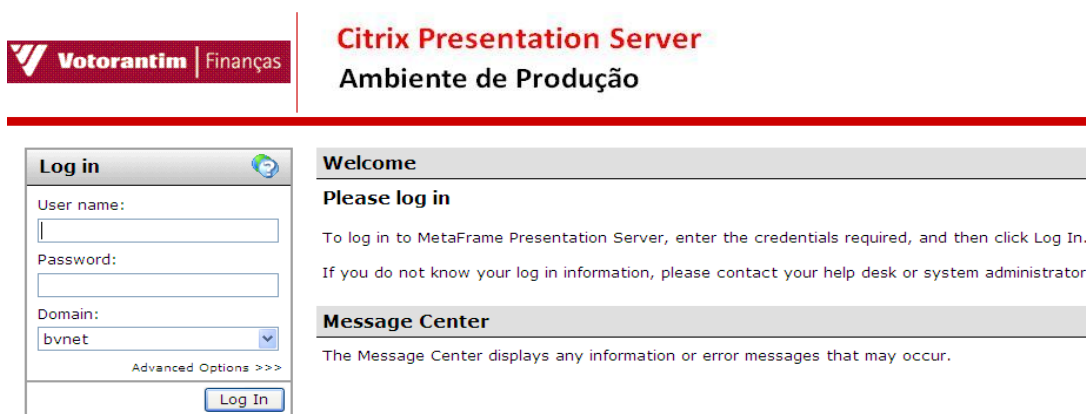
- Manter o computador destino ligado;
- Efetuar login na máquina de origem;
- Acessar o programa de conexão, em Iniciar>Programas>Acessórios>Conexão de Área de Trabalho Remota;
- Digitar o IP da máquina desejada e clicar em Conectar
- Caso a conexão seja realizada com sucesso, será exibida a Área de Trabalho do computador destino;
- Abrir a ferramenta em seu diretório específico, como explicado no item anterior.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

### c) Acesso via Citrix

Também é realizado por qualquer máquina da instituição, com as seguintes etapas:

- A conexão deve ser efetuada numa máquina já logada, através do link <http://citrix;>



**Figura 53 - Login no Acesso via Citrix**

- Uma vez efetuado o login, o usuário deve clicar no botão “Explorer BCO”, como mostrado na Figura 2 e aguardar a conexão;



**Figura 54 - Conexão no Acesso via Citrix**

- No Explorer, basta abrir a ferramenta em seu diretório específico.

Os acessos remoto e via Citrix foram idealizados na fase de implantação do novo programa, para facilitar o trabalho de mapeamento de riscos dos analistas, que agora possuem a opção de se conectar em qualquer máquina disponível na área mapeada e utilizar a

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

ferramenta, disponível em rede. Assim, durante as reuniões com os gestores de cada área, os analistas já podem realizar os cadastros na ferramenta, evitando possíveis retrabalhos e economizando tempo, considerando que anteriormente as informações eram primeiramente escritas à mão pelos analistas nas entrevistas, para só depois serem inseridas no sistema. Além disso, o cadastro imediato realizado juntamente com os gestores evita ainda que informações relevantes sejam esquecidas e que ocorra dissenso com os mesmos.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**VIII PROBLEMAS ENCONTRADOS**

Esse capítulo relata os diversos problemas identificados no processo de implantação da ferramenta desenvolvida, observados sobretudo após a elaboração e/ou disponibilização da mesma para os usuários.

Um dos problemas encontrados ocorreu com o *carregamento de toda a base de dados* existente no antigo programa de mapeamento. Mais de 800 mapeamentos de risco foram adicionados à ferramenta, cada um com diversas causas mapeadas, como também ambientes de controle e planos de ação vinculados. Assim, o programa passou a sofrer de lentidão, que na maioria das vezes não ocorria na versão para testes, que apresentava um número muito menor de cadastros.

A lentidão era previsível pela tecnologia utilizada e não impede o funcionamento do programa: apenas atrasa em alguns segundos o carregamento de uma página, ou o salvamento de um registro, por exemplo. Contudo, é uma dificuldade que deve ser monitorada, considerando que cada vez mais registros serão cadastrados na ferramenta, o que pode acarretar numa piora da lentidão com o passar do tempo.

Para melhorar essa situação foi realizado o estudo por parte dos programadores, buscando encontrar na internet ou literatura especializada, maneiras de deixar o programa menos pesado: seja por utilização de menos objetos nos formulário, ou códigos mais simples no Visual Basic do Access. No caso do formulário “Vínculos entre ambientes de controle e causas”, a situação era a mais crítica: o salvamento do cadastro demorava minutos. O layout do formulário já se apresentava da maneira mais simples, para que não pesasse muito. A solução encontrada foi alterar a programação existente no Visual Basic. A inteligência realizada pelo programa era muito complexa e uma alteração radical não seria viável, pois implicaria em dias de manutenções e testes. O objetivo foi buscar diminuir o tempo de salvamento, sem alterar muito a programação. Para os riscos vinculados a poucas causas e controles o tempo foi reduzido para poucos segundos, e para os riscos com muitos vínculos, foi reduzido para menos de um minuto.

Outra dificuldade encontrada foi a *resistência dos próprios analistas* em utilizar a ferramenta durante as entrevistas com os gestores da área a ser mapeada. Isso se deve ao receio, por parte dos analistas, de que os gestores não teriam tempo e paciência para esperar

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

que os analistas adicionassem todas as informações relevantes (ou não) absorvidas nas entrevistas na ferramenta. O trabalho sempre fora realizado em diversas etapas: as primeiras para o analista entender o funcionamento da área e todos os seus processos, antes de mapear todos os riscos, utilizando apenas cadernos para anotar todas as informações; as últimas para avaliar o nível de exposição de cada risco e o tratamento a ser aplicado em cada caso.

Em reuniões entre as áreas de Gestão de RO, Modelagem e Projetos e Mapeamento de Risco, foi decidido que a ferramenta poderia não ser usada durante as primeiras etapas do mapeamento, sendo ainda utilizados cadernos de anotações. Nas entrevistas posteriores com os gestores, entretanto, depois de conhecida e entendida a área (e seus processos) e seus principais riscos, a ferramenta deve ser sempre utilizada para inserir os relacionamentos dos riscos com os ambientes de controle, assim como para avaliar a exposição do risco e o seu melhor tratamento, através dos planos de ação.

Espera-se mais para frente, depois de intensa utilização do novo sistema, que os analistas se familiarizem e se considerem aptos a usá-lo durante as entrevistas com os gestores.

A vinculação, no antigo programa de mapeamento, dos ambientes de controle e planos de ação a um risco era realizada em campo texto, como explicado na Figura 8 **Erro! Fonte de referência não encontrada.** do Capítulo II. O analista preenchia a descrição dos controles vinculados ao risco, com as causas que cada um deles mitiga. Para carregar essas vinculações, seria demasiadamente trabalhoso para os desenvolvedores do sistema, verificar todos os controles e causas que foram vinculados.

Foi decidido, portanto, que todos os controles vinculados a riscos seriam carregados, considerando que mitigam todas as causas mapeadas para o mesmo risco. Essa solução exige que os analistas revisem os registros, atualizando a vinculação dos ambientes de controle e as causas mapeadas dos riscos. Como são mais de 3000 registros, o trabalho, que deve demorar meses, ainda não foi concluído e atrapalhou a Avaliação de Riscos, que depende do relacionamento entre as causas e ambientes de controle vinculados ao risco.

Outra alteração realizada juntamente com a ferramenta foi a descrição do ambiente de controle, que segue uma definição padronizada de acordo com o normativo da empresa. Os ambientes cadastrados no antigo programa não seguiam nenhuma padronização, pois eram registrados em campos texto, de livre digitação e a classificação de Tipo não era obrigatória.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Os controles foram adicionados na ferramenta com a definição não padronizada e tipo “A definir”.

Assim, os controles também devem ser revisados pelos analistas, encarregados de alterar a antiga definição para o novo formato padronizado, além de definir o Tipo de ambiente de controle a que correspondem. Enquanto essa revisão não é realizada, a vinculação dos ambientes de controles se apresenta comprometida, já que apenas alguns tipos de componentes do ambiente de controle são aplicáveis para mitigação de cada categoria nível 2 de risco.

Outra padronização realizada foi com Processo. Não existe uma listagem de todos os processos existentes nas áreas da empresa, o que possibilita que cada gestor possua diferentes visões e entendimento da definição de processo. Com a necessidade de uma padronização dos processos para fazer o mapeamento, deve haver um alinhamento de definição de processo entre as áreas, para que haja uma lista padronizada universal, que pode ser utilizada por todas as áreas da empresa. Reuniões forem feitas entre as áreas de Gestão de RO e Engenharia de Processos com esse objetivo.

A área de Auditoria Interna deve fornecer à célula de Modelagem os processos da empresa que possuem pontos de auditoria em aberto, para que seja calculada a faixa de classificação da probabilidade qualitativa, no seu respectivo questionário, e assim, chegar ao valor do nível de exposição do risco e o tratamento a ser dado. Com a falta de padronização, a área enviou algumas vezes tabelas com os pontos de auditoria correspondentes a processos não compatíveis com os definidos. Para resolver esse problema, foram realizadas reuniões entre Modelagem e Processos e Auditoria, para que esta última entendesse a nova conceituação, evitando que isso aconteça novamente. Porém, ainda falta o alinhamento com a Engenharia de Processos, para que todas as áreas utilizem a mesma listagem.

Essas padronizações ainda podem impactar no Sistema de Reporte de Eventos de RO. Nele, os responsáveis de cada área devem enviar eventos que ocorreram como Perdas Operacionais, que também influenciam na faixa de classificação da probabilidade qualitativa e nível de exposição ao risco. Ao reportarem os eventos, deve-se definir o processo em que eles estão inseridos e suas respectivas causas, categoria nível 2 de risco, etc. Assim, o entendimento de todos é extremamente importante, para reduzir o trabalho de revisão dos registros por parte da área de Modelagem e Projetos e a realimentação das informações no sistema por parte dos encarregados do reporte, que ocorre mensalmente.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

Além disso, os próprios analistas (e usuários do sistema), responsáveis pelos cadastros na ferramenta, devem compreender as novas conceituações. Qualquer falha no entendimento vai acarretar em cadastros errados e más interpretações, que podem demorar a ser detectados.

Após disponibilização da ferramenta para cadastros dos mapeamentos pelos usuários, foram encontrados alguns problemas operacionais, que impossibilitavam o cadastro adequado dos registros. Assim que encontrados, os usuários alertaram imediatamente os funcionários de Metodologia e Projetos responsáveis pelo sistema. Depois de definida a solução adequada dos problemas, com a realização de diversos testes, o sistema era devidamente alterado. Durante esse período, como relatado na Manutenção Corretiva do item VI.7, os usuários não poderiam acessar a ferramenta, para não haver perda de registros. Esse problema era esperado pelos funcionários, devido à inexperiência dos mesmos em programação e tecnologia de informação. Felizmente, e principalmente por causa dos exaustivos testes realizados no sistema antes de disponibilizá-lo para os usuários, o número de problemas foi pequeno.

Outra limitação é a gestão de informações no sistema, realizada manualmente pela área de Metodologia e Projetos, de maneira a verificar o correto cadastramento dos registros. Enquanto o número de usuários é pequeno, a análise é realizada rapidamente. Mas como a área está em processo de crescimento e aumento de funcionários, a ferramenta será utilizada por um número maior de pessoas, dificultando e inviabilizando o gerenciamento manual da base de dados.



## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**IX CONCLUSÃO**

O presente trabalho aborda o desenvolvimento de um sistema de informação para Gestão de RO. Para isso, foi necessário ambientar o leitor sobre as metodologias atuais que abrangem o risco operacional, mais popularmente conhecidas como acordos de Basileia. O Banco Central é o órgão responsável por fiscalizar o cumprimento dessas metodologias nas instituições financeiras brasileiras, que devem criar métodos próprios para gerenciar os seus riscos.

Quando foi iniciado o estágio na empresa, a autora desconhecia o termo Basileia e os acordos envolvidos. Por isso, foi necessário estudo sobre o assunto, por meio de arquivos e documentos disponibilizados na intranet da empresa, como Normas, Procedimentos e Anexos.

O sistema utilizado anteriormente pela empresa apresentava diversas limitações e foi desenvolvido um novo sistema pela área de Gestão de RO, que se baseou na metodologia usada para o mapeamento de riscos. Ao entrar na área, a elaboração do programa já havia sido iniciada, e a falta de conhecimento com os programas Microsoft Access e Visual Basic dificultaram o início do trabalho da autora. Porém, a ajuda dos colegas de trabalho, as literaturas existentes em livros e artigos na internet e a vontade de aprender propiciaram um rápido crescimento e contribuição da autora para o programa.

A empresa busca constantemente se adequar às exigências do Banco Central e de Basileia. Por isso, a metodologia de mapeamento de risco foi alterada algumas vezes, o que impactou em diversas mudanças no sistema desenvolvido, que contribuiu, juntamente com a inexperiência dos programadores, para que o sistema demorasse meses para ser concluído. Esse tempo abrangeu inclusive todos os testes realizados intensamente, para garantir que o sistema apresentasse o menor número de deficiências.

Além do mais, a metodologia deve ser sempre atualizada, para atender as exigências externas, abrangendo as leis que são criadas. Um exemplo é a Sarbanes Oxley, ou SOX, que estabelece regras obrigatórias para a boa governança corporativa, relativas ao estabelecimento de controles internos e à divulgação e emissão de relatórios financeiros (SANTOS; LEMES, 2007). A lei se aplica a todas as empresas que operam no mercado de capitais norte-americano.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

A SOX foi criada após diversas fraudes e escândalos contábeis recentes que ocorreram em muitas organizações norte-americanas de grande porte, para evitar a perda de confiança de investidores, reduzindo os riscos nos negócios e garantindo a transparência na gestão das empresas. A lei torna executivos “explicitamente responsáveis por estabelecer, avaliar e monitorar a eficácia dos controles internos sobre relatórios financeiros e divulgações” (DELOITTE, 2003, p.3)

Desde 2009, foi estabelecida uma parceria estratégica da empresa com uma das maiores instituições financeira do Brasil que opera no mercado de ações americano. Por isso, a metodologia interna da instituição e o sistema criado deverão ser atualizados para atender à SOX. Essa decisão é recente e deve começar a ser implantada apenas em 2012, e por isso, não está presente neste trabalho.

A ferramenta apresenta diversas vantagens, principalmente quando comparada com o programa utilizado anteriormente. Para relacionar essas vantagens, foram consideradas as opiniões dos usuários, que por terem realizado seus trabalhos de mapeamento nos dois sistemas, são os mais aptos para compará-los.

1. Fácil navegação entre os diversos módulos, possibilitando reaproveitar a descrição de riscos, causas, controles e planos de ação.
2. Diversas checagens são realizadas nos formulários, que impedem que registros sejam salvos incompletos ou sem o preenchimento de dados necessários.
3. Redução dos registros presentes no sistema, através da padronização de diversos cadastros, como riscos, causas, ambientes de controle e planos de ação, facilitando, assim, o gerenciamento da base de dados pela área de Metodologia e Projetos.
4. Desempenho mais rápido que o sistema anterior, reduzindo o tempo de cadastro dos mapeamentos dos analistas.
5. A estrutura hierárquica da empresa, recebida mensalmente da área de Recursos Humanos, é rapidamente importada para a ferramenta, evitando, por exemplo, que cadastros sejam vinculados a uma área ou gestor indevidos, ou que cobranças do acompanhamento de planos de ação sejam feitas para pessoas erradas.
6. Informações importantes para a avaliação de risco, como pontos de auditoria e existência de perdas são agora consideradas no cálculo de exposição ao risco e são visualizadas nos respectivos formulários.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

7. Consultas e relatórios criados especificamente para auxiliar e facilitar o trabalho de mapeamento de risco.

Os relatórios possuem uma aparência amigável e são bem segmentados, possibilitando identificar os riscos, controles e planos de ação. Agora, é possível encaminhá-los diretamente aos gestores, para validação do mapeamento realizado nas áreas. Na antiga ferramenta havia necessidade de elaborar um relatório por meio de planilha. Além do mais, os relatórios contribuem para os diretores e a alta administração da empresa se tornarem cientes dos seus riscos mais relevantes.

As consultas auxiliam a supervisão da base de dados pela área de Metodologia e Projetos, para analisar a inclusão e alteração de informações e são enviadas para a área de Controles Internos, que, como já mencionado, necessita dos dados sobre os controles para verificar sua efetividade.

8. As alterações a serem realizadas no sistema, como mudança na metodologia, ou pedidos dos usuários, são rapidamente realizadas, já que os programadores são da área, e conhecem a metodologia de RO, além das necessidades dos usuários.

Embora tenham sido encontradas algumas falhas, como explicado no capítulo anterior, os usuários elogiaram o sistema, que além de ser mais rápido que o anterior, é personalizado e adequado aos usuários e à metodologia por eles utilizada.

Isso mostrou que apesar de não ter sido criado por especialistas em tecnologia de informação e programação, o programa foi bem avaliado pelos envolvidos.

O planejamento e desenvolvimento do sistema propiciaram para a empresa, de forma conclusiva, maior agilidade no processo de mapeamento de riscos, controles e planos de ação, maior transparência à alta administração quanto aos riscos aos quais a instituição está exposta, através da elaboração de consultas e relatórios, maior integração de informações primárias, como pontos de auditoria e perdas, para as avaliações de riscos e aumento da capacidade no gerenciamento dos riscos, considerando que o número dos registros foi reduzido e que diversos analistas podem acessar a ferramenta simultaneamente, sem perda da eficiência. Além disso, o treinamento realizado promoveu a capacitação dos analistas para a utilização da ferramenta a partir da nova metodologia criada.

Benefícios foram proporcionados não só para a empresa, como também para a autora do trabalho. O tempo permanecido no banco contribuiu para a sua formação acadêmica, possibilitando colocar em prática conceitos novos e aqueles aprendidos no curso de

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

engenharia de produção. Por fim, foi possível ainda aplicar o que foi realizado no estágio no desenvolvimento deste trabalho de formatura, com o acesso às informações necessárias e auxílio dos colegas de trabalho, os quais possibilitaram o crescimento não apenas profissional, como também pessoal da autora, compartilhando suas ideias, conhecimentos e experiências.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

**X REFERÊNCIAS**

BACEN (Banco Central do Brasil). **Resolução nº 2.554**. Brasília, 24 de setembro de 1998. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 12 de julho de 2011.

\_\_\_\_\_. **Resolução CMN nº 3.380**. Brasília, 29 de junho de 2006. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 28 de junho de 2011.

\_\_\_\_\_. **Resolução nº 3.464**. Brasília, 26 de junho de 2007. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 19 de setembro de 2011.

\_\_\_\_\_. **Carta-Circular nº 3.315**. Brasília, 30 de abril de 2008. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 28 de junho de 2011.

\_\_\_\_\_. **Circular nº 3.383**. Brasília, 30 de abril de 2008. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 28 de junho de 2011.

\_\_\_\_\_. **Resolução nº 3.721**. Rio de Janeiro, 30 de abril de 2009. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 19 de setembro de 2011.

\_\_\_\_\_. **Comunicado nº 20.605**. Brasília, 17 de fevereiro de 2011a. Disponível em: <<http://www.bcb.gov.br>>. Acesso em 28 de junho de 2011.

\_\_\_\_\_. **BC divulga orientações preliminares e cronograma de implementação das recomendações de Basiléia III**. Brasília, 17 de fevereiro de 2011b. Disponível em: <<http://www.bcb.gov.br/textonoticia.asp?codigo=2927&idpai=NOTICIAS>>. Acesso em 28 de junho de 2011.

BANCO DO BRASIL (BB). **Relações com Investidores**. Disponível em: <[http://www.bb.com.br/portalbb/page51,136,3696,0,0,1,8.bb?codigoNoticia=7724&codigoMenu=0&codigoRet=5618&bread=9\\_1\\_4](http://www.bb.com.br/portalbb/page51,136,3696,0,0,1,8.bb?codigoNoticia=7724&codigoMenu=0&codigoRet=5618&bread=9_1_4)> Acesso em 25 de março 2011.

BASEL COMMITTEE ON BANKING SUPERVISION. **International Convergence of Capital Measurement and Capital Standards**. Basiléia, Suíça, julho de 1988. Disponível em: <[www.bis.org](http://www.bis.org)>.

\_\_\_\_\_. **Overview of the New Basel Capital Accord**. Basiléia, Suíça, janeiro de 2001. Disponível em: <[www.bis.org](http://www.bis.org)>.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

\_\_\_\_\_. **History of the Basel Committee and its Membership.** Basileia, Suíça, agosto de 2009. Disponível em: < <http://www.bis.org/bcbs/history.pdf> >.

BERNSTEIN, P. L. **Against the Gods: the remarkable story of Risk.** John Wiley & Sons, Inc. New York, 1998.

BIS (Bank for International Settlements). **Core Effective Principles in Banking Supervision.** Basileia, Suíça, setembro de 1997. Disponível em: < <http://www.bis.org> >. Acesso em 11 de julho de 2011.

BIS (Bank for International Settlements). **The New Basel Capital Accord.** Basileia, Suíça, janeiro de 2001, Disponível em: < <http://www.bis.org> >. Acesso em 3 de julho de 2011.

BIS (Bank for International Settlements). **International Convergence of Capital Measurement and Capital Measurement Standards.** Basileia, Suíça, jun. 2004. Disponível em: <<http://www.bis.org>>. Acesso em 12 de julho de 2011.

\_\_\_\_\_. **BIS History - Overview.** Disponível em: <<http://www.bis.org/about/history.htm>>. Acesso em 12 de junho de 2011.

CARVALHO, Dermeval B.; DOS SANTOS, Gustavo M. **Os Acordos de Basileia – Um roteiro para implementação nas instituições financeiras.** Disponível em: [http://www.febraban.org.br/Arquivo/Servicos/Imprensa/Artigo\\_Basileia\\_6.pdf](http://www.febraban.org.br/Arquivo/Servicos/Imprensa/Artigo_Basileia_6.pdf). Acesso em 14 de junho de 2011.

CHAPELLE, Ariane et al. **Basel II and Operational Risk: Implications for risk measurement and management in the financial sector.** 2004. National Bank of Belgium. Disponível em < <http://www.bnb.be/doc/ts/publications/WP/WP51En.pdf> >.

CHERNOBAI, Anna S.; SVETLOZAR, Rachev T.; FABOZZI, Frank J. **Operational Risk. A Guide to Basel II Capital Requirements, Models, and Analysis.** John Wiley & Sons, Inc. New Jersey, 2007.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). **“Gerenciamento de Riscos Corporativos – Estrutura Integrada”.** 2007.

COSTA, Fernando N. da. **Brasil dos Bancos.** Campinas, Livro em processo de produção editorial pela EDUSP, 2008. 336 páginas.

CYRIAC, John. **Operational Risk Management: Considerations for Implementation using Compliance Data.** 2008. Disponível em < <http://johnncyriac.com/blog/wp->

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

content/uploads/2009/02/orm\_using\_compliancedata\_sanitised\_080110.pdf>. Acesso em 13 de outubro de 2011.

DELOITTE. **Lei Sarbanes-Oxley – Guia para melhorar a governança corporativa através de eficazes controles internos.** São Paulo, outubro de 2003. Disponível em:<[http://www.deloitte.com/assets/Dcom-Brazil/Local%20Assets/Documents/guia\\_sarbanes\\_oxley\(1\).pdf](http://www.deloitte.com/assets/Dcom-Brazil/Local%20Assets/Documents/guia_sarbanes_oxley(1).pdf)>. Acesso em 19 de setembro de 2011.

\_\_\_\_\_. **Informativo Tributário - Procedimentos para Instituições Financeiras calcularem o Capital para o risco operacional são divulgados pelo BACEN.** São Paulo, 2008. Disponível em:<<http://www.deloitte.com.br/publicacoes/2008all/042008/Boletim408.pdf>>. Acesso em 01 de junho de 2011.

DEUTSCHE BANK. **Relatório de Gerenciamento de Riscos – Basileia II Pilar 3.** 2010. Disponível em <[http://www.db.com/brazil/pt/docs/relatorio\\_de\\_gerenciamento\\_de\\_riscos\\_basileiaII\\_pilar3.pdf](http://www.db.com/brazil/pt/docs/relatorio_de_gerenciamento_de_riscos_basileiaII_pilar3.pdf)>. Acesso em 15 de setembro de 2011.

DUARTE Jr., Antônio M. **A importância do gerenciamento de riscos corporativos.** Unibanco Global Risk Management, 2000. Disponível em <[www.risktech.com.br/PDFs/RISCORPO.pdf](http://www.risktech.com.br/PDFs/RISCORPO.pdf)>. Acesso em 02 de novembro de 2011.

FEBRABAN. **Os Acordos de Basileia – Um roteiro para implementação nas instituições financeiras.** Disponível em: [http://www.febraban.org.br/Arquivo/Servicos/Imprensa/Artigo\\_Basileia\\_6.pdf](http://www.febraban.org.br/Arquivo/Servicos/Imprensa/Artigo_Basileia_6.pdf). Acesso em 01 de junho de 2011.

JACOBSON, Ivar et al. **Object Oriented Software Engineering: A Use Case Driven Approach.** Addison-Wesley, 1992.

KING, Jack L. **Operational Risk: Measurement and Modelling.** Chichester: John Wiley & Sons, Inc. 2001. 276p.

KOSCIANSKI, André; SOARES, Michel dos S. **Qualidade de Software.** São Paulo: Novatec Editora Ltda, 2006. 2v.

LIBERATO, Denísio. **Esquema Ponzi, pirâmides, bolhas e Madoff.** Instituto Brasileiro de Executivos de Finanças de São Paulo, outubro de 2009. Disponível em <[www.ibef.com.br/ibefnews/pdfs/136/artigo.pdf](http://www.ibef.com.br/ibefnews/pdfs/136/artigo.pdf)>. Acesso em 02 de novembro de 2011.

## SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL

MARSHALL, Christopher. **Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras**. Rio de Janeiro: Qualitymark, 2002. 444p.

NIEMANN, Scott. **Executable Systems Design with UML 2.0**. Disponível em <[http://www.omg.org/news/whitepapers/Executable\\_System\\_Design\\_UML.pdf](http://www.omg.org/news/whitepapers/Executable_System_Design_UML.pdf)>. Acesso em 08 de setembro de 2011. Andover: 2004.

ONO, Fabio H. **O Acordo de Basiléia, a Adequação de Capital e a Implementação no Sistema Bancário Brasileiro**. Campinas: Universidade Estadual de Campinas, 2002.

PAULA FILHO, Wilson de P. **Engenharia de Software: Fundamentos, Métodos e Padrões**. Rio de Janeiro: LTC Editora, 2003. 2v.

ROSENBERG, Doug; SCOTT, Kendall. **Use Case Driven Object Modeling with UML: A Practical Approach**. Massachusetts: Addison-Wesley, 1999. 165p.

SANTOS, Luciana de A. A.; LEMES, Sirlei. **Desafios das Empresas Brasileiras na Implantação da Lei Sarbanes-Oxley**. Base – Revista de Administração e Contabilidade da Unisinos, abril de 2007. Disponível em <[http://www.unisinos.br/publicacoes\\_cientificas/images/stories/pdfs\\_base/v4n1/art03\\_lemes.pdf](http://www.unisinos.br/publicacoes_cientificas/images/stories/pdfs_base/v4n1/art03_lemes.pdf)>. Acesso em 20 de setembro de 2011.

SILVA, Helom O. da. **Os Sistemas Financeiros e a Evolução das regras de supervisão bancária**. Sergipe: Universidade Federal de Sergipe, 2010.

SIVINSK, Camila S. **Evolução do Acordo da Basileia e a Implementação em Instituições Financeiras no Brasil**. Rio Grande do Sul: Universidade Federal do Rio Grande do Sul, 2010.

SOUZA, Ana P.T de. **Modelagem do comportamento do fluxo de desembolso de depósitos com maturidade indefinida**. Brasília: Universidade de Brasília, 2006.

VAUGHAN, Emmett J. **Risk Management**. New Baskerville: John Wiley & Sons, Inc., 1997. 832p.

WTHREEX. **Atividade: Localizar Atores e Casos de Uso**. Disponível em <[http://www.wthreex.com/rup/process/activity/ac\\_facuc.htm](http://www.wthreex.com/rup/process/activity/ac_facuc.htm)>. Acesso em 08 de setembro de 2011.