MEGI

MESTRADO
Estatística e Gestão de Informação

Implementação de um sistema de informação para gestão de Risco Operacional numa instituição bancária portuguesa: Caso de Estudo

Catarina Isabel Frasco Lucas Bento dos Santos

Trabalho de Projeto apresentado como requisito parcial para obtenção do grau de Mestre em Estatística e Gestão de Informação

UNIVERSIDADE NOVA ISEGI

Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

IMPLEMENTAÇÃO DE UM SISTEMA DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL NUMA INSTITUIÇÃO BANCÁRIA PORTUGUESA:CASO DE ESTUDO

por

Catarina Isabel Frasco Lucas Bento dos Santos

Trabalho de Projeto apresentado como requisito parcial para a obtenção do grau de Mestre em Estatística e Gestão de Informação, Especialização em Análise e Gestão de Risco

Orientador/Coorientador: Professor Doutor Rui Gonçalves

Novembro 2012

AGRADECIMENTOS

Dirijo-me às pessoas que contribuíram de forma direta ou indireta para a realização deste projeto agora finalizado, às quais gostaria de expressar o meu agradecimento.

Agradeço, em primeiro lugar, ao meu orientador, Professor Rui Gonçalves por incutir o gosto pela gestão de risco, pela sua disponibilidade e generosidade revelada ao longo da realização deste projeto, assim como pelas críticas, correções e sugestões feitas.

Um agradecimento muito especial à minha mãe pelo incentivo e apoio tão fundamentais para o início e conclusão deste trabalho.

Quero agradecer aos meus colegas de trabalho pela partilha de ideias.

Um agradecimento aos meus amigos pela compreensão pela falta de tempo para estar com eles.

RESUMO

A difícil identificação e medição e a ausência da devida importância do risco operacional por parte do mercado e dos reguladores têm sido as razões para as instituições bancárias centrarem as suas atividades em áreas como o risco de mercado e de crédito. Só recentemente e por imposição da entidade supervisora em Portugal, o Banco de Portugal, as instituições bancárias incluíram o risco operacional na sua política de gestão. Apesar da inclusão do risco operacional na gestão das instituições, estas continuam a ter algumas dificuldades em aceitar este risco, bem como, decidir sobre as ferramentas necessárias para a sua gestão eficaz e eficiente.

Este projeto tem como principal objetivo demonstrar a importância da implementação de um sistema de informação para gestão de risco operacional evidenciando as mais-valias e limitações do sistema na instituição bancária portuguesa. Pretende-se, ainda, analisar a postura e o nível aceitação por parte colaboradores face ao sistema implementado a fim de identificar as oportunidades de negócio criadas pela instituição com o novo sistema, assim como, a utilização do mesmo como suporte à tomada de decisão para a área de risco operacional.

PALAVRAS-CHAVE

Risco Operacional, Sistemas de Informação, Instituição Financeira, Basileia II

JEL Codes: C88, E58, G21, G22, G32.

ABSTRACT

The identification and measurement difficult and the lack of sufficient importance given to operational risk by the market and regulators, have been the reasons for banks to focus their activities in areas such as market risk and credit. Only recently and by the enforcement of the supervisor entity in Portugal, *Banco de Portugal*, other banking institutions included the operational risk in its management policy. Despite the inclusion of operational risk in the institutions management, they still have some difficulties to accept this risk and decide on the necessary tools for their effective and efficient management.

This project's main objective is to demonstrate the importance of implementing an information system for operational risk management highlighting the gains and limitations of the system in a Portuguese bank institution. This study aims also to analyze the the attitude and level acceptance by collaborators over the implemented system, to identify the business opportunities created by the institution with the new system, as well as its use as a support for decision-making in the operational risk area.

KEYWORDS

Operacional Risk, Information System, Financial Institutions, Basel II

JEL Codes: C88, E58, G21, G22, G32.

ÍNDICE

1. Introdução 9
   1.1. Relevância do tema 10
   1.2. Objetivos do projeto 13
2. Risco operacional em instituições financeiras 14
   2.1. Definição e dimensão do risco operacional 15
   2.2. Gestão de risco operacional 18
3. Sistemas de informação para o risco operacional 22
   3.1. Arquitetura de um sistema de informação 22
   3.2. Dados 25
   3.3. Cálculos de quantificação do risco operacional 31
   3.4. Relatórios 34
4. Metodologia 37
   4.1. Processo de investigação 37
5. Resultados e Discussão 40
   5.1. Sistema de informação da instituição bancária 41
      5.1.1. Avaliação do sistema implementado 47
   5.2. Análise swot aplicada ao sistema de informação 48
6. Conclusões 50
7. Limitações e Recomendações para Trabalhos Futuros 53
8. Bibliografia 54

ÍNDICE DE FIGURAS

Figura 1 – Investimentos nas áreas de risco 11
Figura 2 – Importância da gestão de risco operacional 12
Figura 3 – Tipos de riscos nuna instituição 14
Figura 4 –Arquitetura do sistema de informação para a gestão de risco operacional .. 24
Figura 5 –Distribuição de perdas operacionais 34
Figura 6 – Análise *SWOT* 38
Figura 7 – Arquitetura do sistema de informação da instituição estudada 43

ÍNDICE DE TABELAS

Tabela 1 – Eventos mais conhecidos do risco operacional..... 11
Tabela 2 – Categoria de risco operacional..... 16

1. INTRODUÇÃO

Para Buchelt e Unteregger (2004) o risco operacional não é novidade para o sistema financeiro e afirmam que este tipo de risco é mais antigo do que o risco de crédito e de mercado por ter estado presente desde o início do funcionamento do sistema financeiro. Só recentemente as instituições financeiras reconheceram a importância do risco operacional. A dificuldade de identificar e quantificar este tipo de risco e a ausência de relevância dada das instituições, mercado e reguladores são motivos para a negligência da análise e gestão deste tipo de risco (Gonçalves, 2011). No entanto actualmente regista-se um crescimento da importância do risco operacional, para Geiger (2002) as razões que contribuem para este crescimento são: (i) a consciência do crescimento do impacto dos riscos operacionais, (ii) o reconhecimento de que a gestão de risco operacional deve ser uma disciplina por direito, (iii) a inclusão dos riscos operacionais nas metodologias de gestão global de risco e (iv) o interesse crescente das entidades reguladoras pelo risco operacional ao nível dos requisitos de capital e da sua gestão. Na mesma vertente, Moosa (2007) considera que o aumento da dependência da tecnologia e a concorrência mais intensiva, assim como, a globalização tornam as instituições financeiras mais expostas ao risco operacional, realçando a importância da implementação de política para a sua gestão. Na área da banca, Buchelt e Untergger (2004) argumentam que o risco de fraude e os eventos externos estiveram presentes ao longo da história, contudo foi o progresso da tecnologia que elevou o potencial do risco operacional.

O risco operacional é o risco resultante da materialização de vários eventos incluindo fraude, roubo, perda de informação, perda de membro-chave da equipa, processos judiciais, terrorismo, vandalismo e desastres naturais (Moosa, 2007). Brink (2002) alerta para a importância deste tipo de risco através da apresentação dos valores elevados das perdas do risco operacional, aproximadamente 4000-2850 milhões de euros. Ao longo dos anos, o Mercado e as instituições bancárias tiveram conhecimento de eventos de risco operacional que “obrigaram” certas instituições a declarar falência, como foi o caso do Banco Barings, que em 1995 sofreu um colapso financeiro quando um dos seus colaboradores perdeu US$ 1,4 bilhão por especulação em contrato de futuros – operações para as quais não tinha autorização. Exemplos de eventos de risco operacional mais recentes são o da Société Générale e do UBS, ambas vítimas de esquemas de fraude financeira arquitetados por colaboradores.

Em 2007, o risco operacional é incluído no Acordo de Basileia II. Esta inclusão demonstra uma preocupação por parte do regulador com a gestão das instituições e com as perdas que podem advir da incapacidade de sistemas e de processos, suportando a ideia de que as perdas de uma determinada instituição bancária não ocorrem apenas do risco de crédito e de mercado (BCBS, 2004). O tardio reconhecimento do risco operacional contribuiu para o atraso no desenvolvimento de sistemas de informação, tornando a sua implementação uma estratégia mais recente em relação aos sistemas para risco de crédito e de mercado. Para Chorafas (2001) o valor dos sistemas de informação para as instituições e para a gestão de risco operacional é um elo de ligação para o aumento da competitividade, assim como, a melhoria da atividade de marketing no processo de criação de valor nas instituições. Esperando que os sistemas de informação fornecem à instituição o conhecimento que lhe permita tomar as decisões mais adequadas para evitar perdas, enfrentar ameaças e retirar valor de novas oportunidades.

1.1. RELEVÂNCIA DO TEMA

O Acordo de Basileia II foi o maior impulsionador da implementação da gestão de risco operacional nas instituições bancárias. A sua inclusão contribuiu para o crescente investimento nesta área, refletindo o aumento da importância do risco operacional nas instituições (Gonçalves, 2011). Na Figura 1 observa-se que o risco operacional foi uma das principais áreas investimento nas instituições, estes valores sugerem que houve um aumento da importância deste risco para as instituições. A estes resultados pode-se atribuir causas como o tardio desenvolvimento do risco operacional logo as instituições necessitam de maiores investimentos para tomar a gestão mais efetiva. Outra causa é extensão da gestão de risco operacional e dos seus sistemas de informação em áreas como o Compliance ou a Auditoria Interna (Gonçalves, 2011).

Figura 1 – Investimentos nas áreas de risco

Fonte: Enterprise risk management in financial service organizations – Economist Intelligence Unit

Estudos realizados nos Estados Unidos da América, orientados por Cummins, Lewis e Wei (2006), reforçam a necessidade das instituições financeiras em investir na gestão operacional no sentido de alertar para os eventos de risco operacional, os quais têm um elevado impacto nas mesmas. Nestes estudos, defendem que um banco ou qualquer instituição financeira após um anúncio referente a uma perda elevada pode sofrer quebras no seu valor de mercado, quebras estas que podem ser superiores às perdas iniciais. Marshall (2001) opta por citar a pesquisa realizada pela Operational Risk Inc., onde é demonstrado que desde 1980 as instituições financeiras têm perdido mais de US$ 200 bilhões devido a riscos operacionais (Tabela 1). Alertando, assim, para a importância de uma instituição incluir a gestão de risco operacional na sua política de gestão.

Instituição	Atividade	Ano	Perda em US$ milhões
Daiwa Bank, Nova york	Negociação não-autorizada de bônus devido a maus controles gerenciais	1984-95	1,100
Sumitomo Corp., Londres	Negociação não-autorizada de cobre, fraude e falsificação	1986-96	1,700
Crédit Lyonnais	Mau controle de empréstimos	Anos 80 e 90	29,000
Bancos, varejistas e corporações dos EUA	Fraudes de cheques	1993	12,000
Kidder Peabody	Negociação de bônus, falta de controles internos	1994	200
Condado de Orange	Negociação de bônus, falta de supervisão gerencial	1994	1,700

Tabela 1 – Eventos mais conhecidos do risco operacional

Fonte: Marshall (2001)

O requisito das entidades supervisoras continua a ser o principal fator para o desenvolvimento da gestão de risco operacional nas instituições financeiras porém existem outras razões para que a gestão de risco operacional comece a ganhar importância dentro das instituições (Figura 2), das quais salienta-se a redução das perdas operacionais e melhoria da performance. Independentemente dos fundamentos utilizados na gestão do risco operacional, o resultado de diversos estudos sustentam de forma consistente a ideia de que deste tipo de risco representa uma verdadeira ameaça ao valor de mercado dos bancos e de qualquer instituição financeira (Gonçalves, 2011).

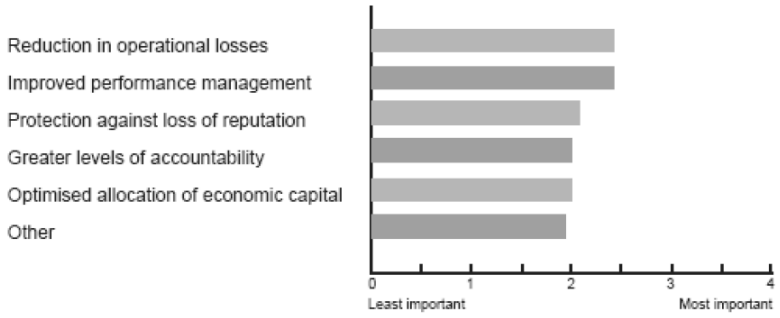

Figura 2 – Importância da gestão de risco operacional
(Fonte: Internal Bencharmark Survey Conducted by SAS and Risk Magazine, Agosto de 2003)

A competência face a gestão do risco operacional depende da existência de um sistema de informação que possibilitar à instituição configurar os seus procedimentos e operações (Gonçalves, 2011). A informação sendo a componente fundamental para o funcionamento dos sistemas de informação neste tipo de risco representa um dos principais problemas a que a implementação destes sistemas enfrenta. Contudo é importante salientar que os sistemas de informação podem evoluir rapidamente e permitem a sua utilização de forma eficiente ou com incorreções (Gonçalves, 2011).

Na área de risco operacional os sistemas de informação encontram-se pouco desenvolvidos comparativamente aos riscos de mercados e de crédito. Para Gonçalves (2011) o desenvolvimento de novos sistemas não passa apenas pela melhoria e automatização das tarefas dos atuais sistemas, mas também, pela integração com outras aplicações e a expansão das funcionalidades a novas áreas em que a gestão de risco operacional seja fundamental nos processos de gestão da instituição. Na mesma

vertente Brink (2002) alerta para a necessidade de desenvolver modelos e sistemas de informação capazes de responder ao aumento da dinâmica e complexidade das atividades em que as instituições estão envolvidas.

1.2. OBJETIVOS DO PROJETO

Este projeto tem como principal objetivo comprovar a importância da implementação de um sistema de informação para gestão de risco operacional na instituição bancária portuguesa considerando as razões que originaram a necessidade de utilização destes sistemas.

O segundo objetivo do projeto será dividido em duas vertentes. Na primeira vertente será realizada uma análise *SWOT* com a finalidade de avaliar o sistema de informação, onde procurar-se-á apresentar os pontos fortes e fracos do sistema implementa na instituição alvo de estudo, as oportunidades que a implementação proporcionou a instituição na área de risco operacional, bem como, as limitações e ameaças identificadas na fase de implementação do sistema. A segunda vertente centra-se na análise do comportamento dos colaboradores face ao sistema e em que medida estes criam valor e oportunidades de negócio para a instituição recorrendo ao sistema implementado. E utilizam o mesmo no suporte à tomada de decisão por parte dos gestores da instituição.

2. RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS

A atividade bancária existe porque os bancos têm capacidade de reduzir os custos de transação e de informação, o que não acontecia se os aforradores ou investidores contractassem diretamente com os tomadores de crédito tendo esta atividade uma envolvência com riscos (Ferreira, 2004: 1-13). O risco associada a esta atividade é inerente a qualquer situação que implique a tomada de decisões, cujos resultados tenham lugar no futuro, podendo implicar que estes venham a diferir do esperado. A volatilidade presente nos resultados das atividades das instituições desperta a essência do risco e necessidade de proteção contra o mesmo (Ferreira, 2004: 1-13).

Em geral, as empresas enfrentam uma diversidade de riscos, conforme apresentado na Figura 3, sendo particularmente relevante para a banca o risco financeiro contudo, recentemente o risco operacional tem vindo a ganhar importância dentro das instituições requerendo politicas e medidas para este tipo de risco. Esta expansão do risco operacional criou o interesse para a realização deste estudo.

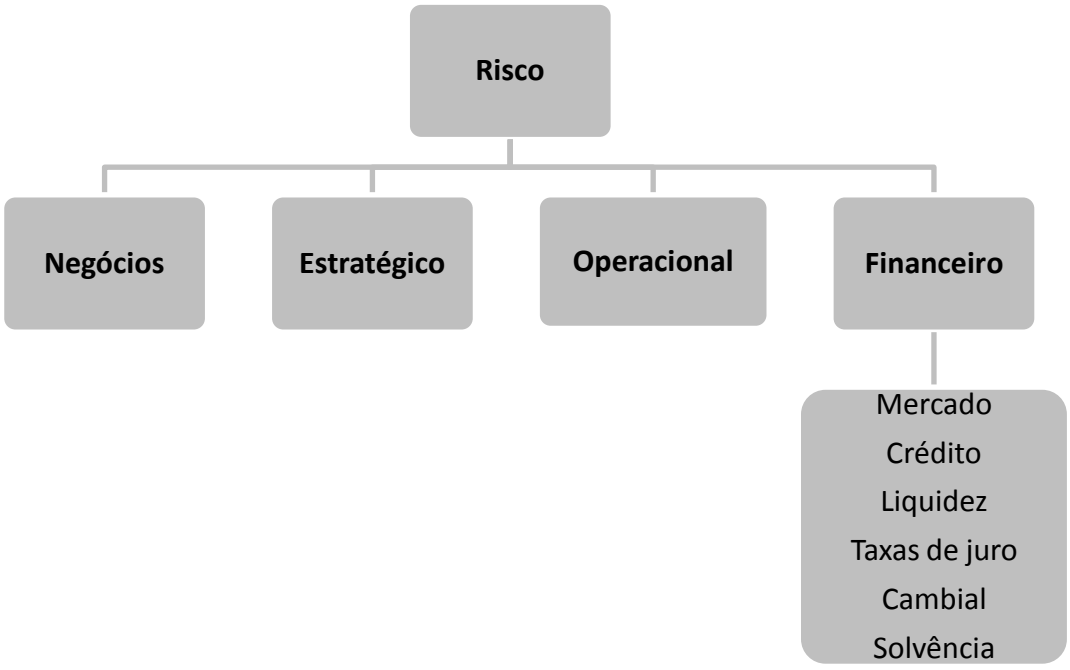

Figura 3 – Tipos de riscos nuna instituição

Fonte: Elaboração própria

A diversidade de risco a que a instituição está exposta implica alterações no papel da gestão de risco. Esta deixa de ser apenas uma política de mitigação dos riscos, passando a comtemplar modelos financeiros e econométricos complexos. Neste sentido, o Acordo de Basileia II e as entidades supervisoras consideram o risco operacional, um risco a incluir na gestão das instituições financeiras.

2.1. DEFINIÇÃO E DIMENSÃO DO RISCO OPERACIONAL

A tendência para uma maior dependência das novas tecnologias, o aumento da concorrência e da globalização deixaram o sistema financeiro exposto ao risco operacional mais do que nunca (Moosa, 2007). No entanto, apesar de Buchelt e Unteregger (2004) também defenderem que foi o progresso tecnológico que aumentou potencialmente o risco operacional, em relação à área da banca defendem que o risco de fraudes e eventos externos são os maiores impulsionadores do risco operacional. Da mesma forma, Halperin (2001) argumenta que "tradicionalmente o rico operacional está abaixo dos riscos de crédito e de mercado", mas progressos como e-commerce, o surgimentos de novos produtos e linhas de negócio têm colaborado para o aumento da exposição ao risco operacional.

O risco de mercado continua a ser o grande foco das instituições financeiras, contudo o risco operacional tem ganho relevância para instituições por ser mais prejudicial do que o risco de mercado ou de crédito (Moosa, 2007). Como tal, as consequências da exposição ao risco operacional não podem ser ignoradas e neste sentido Blunden (2003) argumenta que a ocorrência de um evento de risco operacional pode levar uma instituição à falência e provocar um colapso de Mercado. Contrariamente, Rao e Dev (2006) defendem que o risco operacional é uma categoria que engloba tudo o que não for passível de se considerar como risco de crédito ou de mercado. Na mesma vertente, Modeva e Kyriacou (2001) consideram que o risco operacional "engloba tudo o que não é considerado na exposição ao risco de crédito e de mercado". Noutra óptica, o Banco da Austrália (1998) considerou que o risco operacional é "todos os riscos que não sejam riscos de crédito ou de mercado, que possam causar volatilidades nos proveitos, despesas e no valor de negócio dos bancos". Para Crouchy, Galai e Mark (1998) a definição de risco operacional é "o risco de eventos externos, ou deficiências em controlos internos ou sistemas de informação resultando numa perda, quer seja antecipada ou completamente inesperada". Já Lopez (2002) considera que o risco operacional é o risco não quantificável a que a instituição financeira está exposta. Esta dificuldade em definir o que é o risco

operacional surge, porque este risco é um conceito distorcido dado que "é difícil fazer uma distinção clara entre o risco operacional e as incertezas normais que as operações diárias de uma organização enfrentam" (Crouchy, 2001).

A existência de diversas definições para o risco operacional contribuiu para o Comité de Basileia atribuir a este tipo de risco uma definição global. Considero como risco operacional o "risco resultante de processos internos inadequados, falhas de pessoas ou de sistemas e eventos externos" (BCBS, 2004). Este projeto tem como base a definição de risco operacional dada pelo Acordo de Basileia II por ser a utilizada pelo Banco de Portugal e pelas instituições bancárias portuguesas. Definido o conceito de risco operacional, Bielski (2003) e BCBS (2004) caracterizam este risco segundo o seu tipo e a categoria (Tabela 2).

Tipo	**Categoria**
Fraude Interna	Atividade não Autorizada Roubo e fraude – interna
Fraude Externa	Roubo e fraude – externa Segurança de sistemas
Relações Trabalhistas	Relações com empregado Segurança ambiental Diversidade e discriminação
Relações Comerciais	Adequação, confiabilidade e divulgação de informações Práticas de negócio ou comerciais impróprias Falhas de produtos Seleção de clientes Aconselhamento
Danos ativos	Desastres e outros eventos
Interrupção de negócio e falhas de Sistemas	Sistemas
Execução e gestão de Processos	Captura, execução e manutenção de transações Monitoramento e reporte Aceitação de clientes e documentação Gerenciamento de contas e clientes Correspondentes Fornecedores e terceiros

Tabela 2 – Categoria de risco operacional

Fonte: Elaboração própria com consulta Bielski, 2003 e BCBS, 2004

Como origem dos eventos de risco operacional, Brink (2002) aponta quatro fatores: (i) pessoas: decorrente de equívoco, omissão, distração ou negligência de funcionários ou terceiros contratados e de comportamentos fraudulentos (adulterações de controles, descumprimento intencional das normas, vazamento de informações privilegiadas, desvio de valores, divulgação de informações erradas); (ii) processos: ocorrem da não observância de normas operacionais e de limites, resultando em falta de funcionamento de comités, não cumprimento de alçadas de crédito, guarda indevida de documentos confidenciais, não implantação de controlos, falta de cumprimento de normas, falta de monitoração/conciliação e outros; (iii) sistemas: decorre da descontinuidade das atividades apoiadas por serviços tecnológicos, salientando a sobrecarga de sistemas de processamento de dados (risco de overloads), incapacidade dos sistemas de prover informações confiáveis e suficientes, incompatibilidade e/ou indisponibilidade de informações, falta de meios seguros de acesso aos sistemas, obsolescência dos sistemas e equipamentos, falhas de hardware, faltas de backup e de legalização do software, inadequação de sistemas operacionais/aplicativos e outros; e (iv) fatores externos: originados por terremotos, catástrofes e a outros desastres naturais. Já Wahler (2002) defende que o risco operacional é originado por fontes internas e externas: (i) mudança: causas externas e internas; (ii) complexidade: em produtos, processos e tecnologia; (iii) complacência: gestão ineficiente do negócio e do seu risco, contrariamente aos eventos do risco de crédito e de mercado que são influenciados pelas transações e parceiros de negócio da instituição.

Assim um dos desafios do risco operacional reside numa abordagem de gestão que auxilia a direção de topo a definir as diferentes categorias de risco operacional a considerar em cada uma das linhas de negócio. Complementarmente, deverá ser criada uma estrutura interna de supervisão e de organização deste tipo de risco, que conjuntamente definirão a função de gestão do risco operacional onde se inclui o papel de cada parte envolvida e de como cada função interage dentro do banco, tais como, a auditoria interna e outras funções de suporte (Gonçalves, 2011).

De acordo com os princípios instituídos pelo Comité de Supervisão de Basileia as instituições financeiras devem (BCBS, 2001):

- Possuir um ambiente adequado de gestão de risco que contemple a identificação, avaliação, monitorização, controlo e mitigação;
- Estabelecer planos de contingência;

- Estabelecer políticas de gestão de risco operacional e efetuar a sua avaliação regular, competindo ao supervisor a realização de ações de inspeção periódicas que abranjam este risco, assegurando que os bancos estabelecem e avaliam essas políticas;
- Documentar e divulgar internamente os processos e controlos de gestão do risco operacional;
- Aprovar e realizar uma revisão periódica pelo órgão da administração, da estratégia de gestão deste risco, que inclua uma definição institucional de risco operacional;
- Submeter a estratégia de gestão de risco operacional, desenvolvida no banco, a uma auditoria interna conduzida por pessoal habilitado e independente;
- Executar a nível dos órgãos operacionais responsáveis, uma estratégia de gestão de risco operacional, acompanhada de uma auditoria interna conduzida por pessoal habilitado e independente;
- Empreender a nível dos órgãos operacionais responsáveis, uma estratégia de gestão de risco aprovada pela administração que contemple o desenvolvimento de políticas e procedimentos específicos de gestão de risco operacional;
- Identificar e avaliar o risco operacional inerente a todos os produtos, atividades, processos e sistemas, definindo um mínimo de perda;
- Desenvolver processos de acompanhamento periódico do perfil de risco e exposição a perdas significativas, passando pelo reporte ao órgão de gestão de topo e ao regulador;
- Estabelecer práticas de controlo e de mitigação de risco operacional.

2.2. GESTÃO DE RISCO OPERACIONAL

A introdução da gestão de risco operacional nas instituições resulta do aumento da sensibilidade face ao risco, da tomada de consciência de outros tipos de risco e não só dos de crédito e de mercado, do desenvolvimento de novas práticas bancárias como o aumento da sofisticação dos produtos financeiros e a globalização dos produtos financeiros e o acesso à banca electrónica (BCBS, 2004).

O Comité de Basileia (BCBS, 2001) define a gestão de risco operacional com base em quatro processos: (i) classificação dos eventos, (ii) compreensão dos riscos, (iii) apresentação regular de relatórios e (iv) controlo dos riscos, de modo, a orientar os

objetivos da gestão de risco operacional para que seja possível identificar e medir os riscos operacionais que põem em causa a sobrevivência das instituições tendo como base as três principais dimensões: fonte, risco e consequência. Na mesma vertente, Kingsley, Rolland e Holmes (1998) identificam que objetivos mais abrangentes para a gestão de rico operacional nas instituições devem ser: (i) evitar perdas catastróficas, (ii) definir bem as questões do risco operacional, (iii) permite às instituições antecipar a ocorrência do risco de forma mais eficaz, (iv) medir objetivamente o desempenho, (v) mudanças de comportamento para reduzir o risco operacional, (vi) fornecer informação objetiva e (vii) garantir que não haverá diligências quando são realizadas fusões e aquisições. Em 2001, Marshall afirma que a gestão de risco operacional deve ser sistemática na análise das causas subjacente às perdas esperadas e não esperadas, assim como, na avaliação do racional para a prevenção de risco, mitigação, transferência e financiamento. Define, ainda, que este processo é composto por seis etapas: (i) definição de âmbito e objetivos, (ii) identificação dos riscos críticos, (iii) estimação de riscos, (iv) análise de riscos, (v) implementação de ações de gestão e (vi) controlo e reporte.

Em 2005, Bolton e Berkey voltam a realçar os objetivos da gestão de risco operacional definidos pelo Comité de Basileia, argumentam que o documento *"Sound Practices for the Management and Supervision of Operational Risk*" é um bom orientador para a conceção de um quadro de gestão de risco operacional, podendo fornecer benefícios, tendo em conta os desafios do risco operacional. De acordo com este documento, as instituições financeiras devem criar um conjunto de medidas para que possam acompanhar e controlar o risco operacional. Das medidas apresentadas pelo Comité de Basileia destacam-se (BCBS, 2003):

1. A instituição deve estar ciente dos principais aspetos de riscos operacionais, bem como, a categoria distinta de risco que devem ser englobados e, ainda, deve aprovar e rever, periodicamente, a estrutura de gestão de risco operacional da instituição. A estrutura deve fornecer uma definição ampla e segura de risco operacional e ditar os princípios de como o risco operacional é para ser identificado, avaliado e controlado/mitigado.
2. A instituição deve garantir que a estrutura de gestão de risco operacional está sujeita a auditoria interna efetiva que engloba uma equipa operacionalmente independente, apropriadamente treinada e competente.

3. Os gestores de risco devem ter a responsabilidade de implementar a estrutura de gestão de risco operacional aprovada pelo grupo de diretores. Esta estrutura deve ser consistentemente implementada através de toda organização e todos os níveis da equipa devem entender as suas responsabilidades em relação à gestão do risco operacional. Os gestores devem também ter responsabilidade por desenvolver políticas, processos e procedimentos para gestão do risco operacional em todos os produtos, atividades, processos e sistemas da instituição.
4. A instituição deve identificar e avaliar o risco operacional inerente em todos os produtos, atividades, processos e sistemas. Devem, também, garantir que antes de novos produtos, atividades, processos e sistemas serem introduzidos ou empreendidos, o risco operacional inerente a eles esteja sujeito a adequados procedimentos de avaliação.
5. A instituição deve implementar um processo para monitorizar regularmente perfis de risco operacional e exposições materiais a perdas. Deve haver um relatório regular de informações pertinentes ao gestor sênior e ao grupo de diretores que dá apoio à gestão proativa do risco operacional.
6. A instituição deve ter políticas, processos e procedimentos para controlar e/ou mitigar riscos operacionais materiais. Esta deve periodicamente rever as suas limitações de riscos e estratégias de controlo e devem ajustar adequadamente o seu perfil de risco operacional recorrendo a estratégias apropriadas.
7. A instituição deve implementar planos de contingência e de continuidade dos negócios, de forma, a garantir competências para operar numa base progressiva e limitar perdas no evento de interrupção severa de negócios.
8. Os supervisores devem requerer que todas as instituições, independentemente de tamanho, tenham uma estrutura adequada para identificar, avaliar e controlar/mitigar riscos operacionais como parte de uma abordagem geral de gestão de risco.
9. Os supervisores devem conduzir, diretamente ou indiretamente, avaliações regulares independentes de políticas, procedimentos e práticas de um banco relacionadas ao risco operacional. Os supervisores devem garantir que existam mecanismos apropriados/adequados que permitam estes estarem informados dos desenvolvimentos nos bancos.

10. A instituição deve fornecer informação suficiente para que permita aos participantes do mercado avaliar as abordagens para a gestão do risco operacional.

Foram apresentadas diversas abordagens de autores e investigadores para gestão de risco operacional em que algumas destas vão de encontro às do Comité de Basileia e outras não. Por exemplo, Rebonato (2007) critica o desenho de gestão de risco operacional do Comité de Basileia apresentando as diferenças existentes entre os reguladores e os gestores de risco. Refere que os reguladores focam-se nos eventos catastróficos e que os gestores de riscos estão interessados no retorno diário das suas operações. Pezier (2003), também, critica o Acordo de Basileia II por não reconhecer os riscos de negócio e de reputação, porque defende que estes podem ser mais significativos do que perdas operacionais.

Qualquer que seja a metodologia adotada pelas instituições financeiras, esta deve ser objetiva na concretização dos objetivos atribuídos pelos gestores de riscos, e ainda deve responder aos requisitos definidos por cada um dos supervisores para a gestão de risco operacional. Em todo o caso, os objetivos não devem inserir-se apenas na prevenção/redução do risco operacional, mas também, deve englobar a transferência e o financiamento do risco (Moosa, 2007).

Após a definição da metodologia da gestão de risco operacional, a instituição deve adquirir uma ferramenta que lhe permita efetuar a gestão deste tipo de risco. Segundo Gibson (1997), as principais razões que levam as instituições financeiras a implementar sistemas de informação na gestão de risco operacional são as necessidades: (i) de medir os riscos a que estão expostas e (ii) de procurar a melhor forma de poder recompensar as unidades de negócio ou os seus colaboradores e permitir aos acionistas um trade-off ótimo entre o risco e retorno.

3. SISTEMAS DE INFORMAÇÃO PARA O RISCO OPERACIONAL

Um sistema de informação deve conter informação de qualidade, atualizada e coerente, de forma, a ser possível identificar os indicadores de exposição aos riscos da instituição e registar os eventos e impacto financeiros do risco operacional reunindo, assim, toda a informação necessária à gestão de risco operacional (Mestchain, 2003). Os sistemas de informação devem ser configurados para responder às necessidades das instituições financeiras, tendo como base as seguintes funções: ter a capacidade de avaliar a perda potencial para as atividades da instituição, bem como, prever novas oportunidades de negócio, conseguir identificar as causas ou fontes de riscos que podem originar perdas, apontar fatores que determinam a falha nos controlos que conduzem a perdas e conter informação histórica relativa às perdas e aos tipos de perdas de modo a produzir cenários e relatórios (Kingsley et all, 1998). Para Peccia (2003) o sistema deve ser uma ferramenta de apoio à tomada de decisões. Para tal, uma das funções a destacar do sistema é a identificação dos indicadores de ocorrência de risco operacional e, consequentemente, fornecer um aviso prévio do aumento do risco de perdas futuras (BCBS, 2003). Além disso, o sistema deve avaliar a vulnerabilidade dos riscos permitindo à instituição compreender melhor o seu perfil de risco, e conseguir orientar eficazmente os recursos de gestão de risco.

3.1. ARQUITETURA DE UM SISTEMA DE INFORMAÇÃO

Para a gestão de risco operacional, Kross (2009) afirma que o sistema de informação deve conter estrutura de risco operacional da instituição incluído as políticas internas e externas, garantir a captura dos fatores de risco operacional, através de questionários e/ou análises, deve ser capaz de integrar dados de perdas internos e externos, ser orientado para o cálculo de requisitos de capital, conciliar os dados com os sistemas internos e externos de reporte e ter uma arquitetura para a recolha sistemática de dados e o desenvolvimento de iniciativas e análises da gestão de risco operacional na instituição, com o objetivo de avaliar a sua efetividade e custos associados. Mestchain (2003) sugere cincos passos essenciais para a implantação de um sistema eficaz de gestão de risco operacional:

1. Definição de políticas de gestão: políticas eficazes de gestão do risco operacional com uma definição clara do objetivo da instituição, incluindo todos os aspetos do desempenho do negócio;

2. Determinação de planos: a política implementada deve ter uma estrutura eficaz de gestão assim como os seus planos;
3. Implementação: o sistema de gestão de risco operacional deve ser sistemático, eficaz e ter como objetivo mitigar a ocorrência dos riscos da instituição. Os métodos de avaliação dos riscos são utilizados para decidir e estabelecer prioridades. Na implementação do sistema é necessário determinar os seguintes processos: definir/rever os riscos e as suas categorias, avaliá-los e definir a melhor estratégia, determinar os principais indicadores de riscos, definir as ações estratégicas de mitigação e criar progressos;
4. Medição do desempenho do sistema: a performance do sistema é medida consoante as melhorias que possibilita. O bom desempenho do sistema passa por automatizar todos os processos de funcionamento, relevando assim, uma eficácia de gestão;
5. Auditoria e Revisão: analisar sistematicamente o desempenho das bases de dados em atividades de controlo. A análise do desempenho do sistema demonstra um forte compromisso em melhorar qualquer deficiência/anomalia detetada no decorrer dos processos. As melhorias podem consistir em alterações de políticas, técnicas de medição e controlo do risco. Como tal, os resultados das atividades devem ser incluídos num relatório de revisão onde são explicados todos os processos implementados para a gestão, bem como, as origens dos resultados. Estes relatórios são disponibilizados para auditorias internas/externas (BCBS, 2003).

Com as afirmações de Mestchain (2003) e de Kross (2009) considera-se que, para além dos aspetos regulamentares, um sistema de informação de gestão permite à instituição financeira conhecer os riscos, definir os índices dos riscos chaves e agir para diminuir os fatores de riscos e reduzir as perdas. O sistema deve ainda proporcionar a criação de políticas de controlo, a análise da performance, a rentabilidade e risco das atividades e a proteção do património líquido, através de uma análise quantitativa e qualitativa dos riscos. Desta forma, considera-se que os objetivos da gestão de risco operacional são fundamentais para a decisão de funcionalidades específicas do sistema a implementar na instituição (Mestchian, 2003).

Tal como foi referido anteriormente, o desenvolvimento de sistemas de informação para área de risco operacional ainda é recente. Inicialmente os sistemas existente foram desenvolvidos com objetivo de cumprir os requisitos impostos pelos reguladores. Com a sua evolução pretende-se sistemas de informação com arquiteturas (Figura 4) que servirão para direcionar os colaboradores face aos objetivos da gestão de risco operacional, sem desconsiderar a estratégia global da instituição (Gonçalves, 2011).

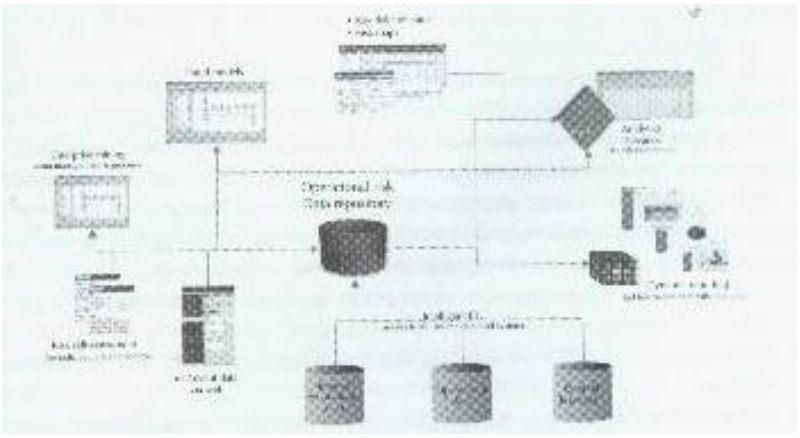

Figura 4 –Arquitetura do sistema de informação para a gestão de risco operacional
Fonte: Marshall (2001)

Face à abordagem da gestão de risco operacional, qualquer sistema de informação implementado deve ser capaz de recolher informação, medir e controlar os riscos que as instituições enfrentam diariamente (Mestchian, 2003). Como tal, estes sistemas são constituídos por dados internos (eventos, impactos financeiros e não financeiros, avaliações de riscos e de controlos e indicadores de riscos) e por dados externos. E com a exploração dos dados, o sistema permite a criação de diversos indicadores, estatísticas e metodologias de análise de cenários a fim de consciencializar para a instituição para os riscos a que está exposta e definir as estratégias a mitigar. Por fim de criar relatórios para a instituição divulgar aos supervisores os resultados das suas políticas de gestão.

3.2. DADOS

Os dados de risco operacional são, sem dúvidas, o maior obstáculo para uma gestão eficaz deste tipo de risco. Esta realidade surge da falta de políticas de recolha de dados e da diversidade de tipos de risco que produzem eventos com informação muito distinta (Haas e Kaiser, 2004). O mesmo não acontece com as perdas dos riscos de crédito e de mercado onde existe uma cultura de registo e enraizada, estando todas perdas bem documentadas (Gonçalves, 2011). Para destacar a dificuldade de recolha dos dados, Muzzy (2003) argumenta que "qualquer pessoa que se aventure na gestão de risco operacional aprende depressa que o processo está condenado ao fracasso se não se tiver dados robustos".

Esta falta de dados deriva do fraco número de eventos de risco operacional, sendo esta falta originada por dois tipos de causa: a primeira centra-se na falta, ou desconhecimento, do conceito de risco operacional nas instituições financeiras, o que implicara que eventos deste risco não tenham sido considerado como tal, acabando por serem registados em outros sistemas (Gonçalves, 2011). A segunda foca-se na falta de uma política de gestão do risco operacional sendo esta uma consequência do desconhecimento do conceito e da essência do risco operacional (Gonçalves, 2011). Sobre esta mesma problemática, Haas e Kaiser (2004) consideram que os problemas do processo de recolha de dados são resultantes da necessidade de uma cultura de risco, das dificuldades em classificar/separar os eventos de risco operacional dos de mercado e de crédito, do registo tardio dos eventos e da existência de eventos que não podem ser diretamente ligados a perdas financeiras.

Para minimizar a falta de dados de risco operacional, os supervisores recomendam a junção dos dados internos com dados externos. No entanto Rao e Dev (2006) alertam para dois processos resultantes do envolvimento este tipo de dados: adequação às realidades dos negócios das instituições e a escala. Já Wei (2007) defende que os dados externos são muito uteis para eventos raros. Segundo Gonçalves (2011) a instituição poderá minimizar esta problemática através de planos de formação aos colaboradores. A formação deve consistir na definição do conceito do risco operacional fornecendo aos colaboradores conhecimento que lhes permita identificar e reportar, de forma clara, os eventos.

Dados internos

Os dados internos de perdas são cruciais para as estimativas de risco, porque são a experiência real das perdas, e são um elemento fundamental para o cálculo de capital para as metodologias avançadas (Gonçalves, 2011). Além de serem um requisito dos supervisores, os dados internos são essenciais sempre que encontram ligados a dimensões, aos processos tecnológicos e aos procedimentos de gestão de risco de forma a melhorar os processos de controlos internos que existem para minimizar o impacto de eventuais perdas (Gonçalves, 2011). Depende da instituição garantir que dados internos sejam compreensíveis e tenham informação sobre os montantes de perdas totais e as perdas de risco operacional relacionadas com outros tipos de riscos (Gonçalves, 2011).

Para obter dados internos Mestchian (2003) considera que os processos de recolha devem cumprir os seguintes aspetos: ser capaz de mapear os seus dados históricos de perdas internas de acordo com as categorias de risco do Acordo de Basileia II e fornecer informação às entidades supervisores. Com o intuito de garantir e criar um processo de recolha de dados a instituição financeira deve criar incentivos dado que estes são recolhidos manualmente e, ainda, criar controlos para assegurar a qualidade e cobertura de dados (Gonçalves, 2011).

Dados externos

Além dos dados de perdas internas, a instituição deve utilizar dados externos relevantes (dados públicos e oriundos de consórcios) principalmente quando existirem razões para acreditar que a instituição está exposta a perdas pouco frequentes mas potencialmente elevadas ou quando existe a possibilidade de a instituição não ser capaz de identificar determinados tipos de risco (Gonçalves, 2011). Este tipo de dados deve conter informação sobre montantes de perda pouco frequentes, a escala de negócio onde ocorre os eventos, as causas dos eventos e os fatores que contribuíram para avaliar a relevância dos eventos para as instituições (Gonçalves, 2011). Para Cagan (2005) e Gonçalves (2011), os gestores utilizaram os dados externos para obter conhecimentos sobre a realidade que as outras instituições enfrentam e ainda são utilizados para casos de estudos no âmbito das análises de cenários.

Apesar, de ser requisito do Acordo de Basileia II, é notória a utilidade dos dados externos para a instituição. No entanto Haas e Kaiser (2004) alertam para alguns problemas da utilização destes tipos de dados: é necessário criar uma ligação entre os eventos da base de dados externos e as categorias de risco e as linhas de negócio da

instituição; o outro problema das bases de dados externas centra-se de estas serem constituídas por perda que foram publicadas compulsivamente nos meios de comunicação. A entidade que recolhe este tipo de dados deve garantir que a informação disponibilizada apresenta um elevado nível de fiabilidade e representatividade. Por último, é precisar saber qual a classificação e escala utilizada. Com o objetivo de minimizar os problemas apresentados por Haas e Kaiser (2004), Gonçalves (2011) sugere que a instituição deve desenvolver metodologias para integrar os dados, e que estas práticas devem ser revistadas, documentadas e sujeitas a revisões periódicas. Na mesma vertente, Samad-Khan, Moncelet e Pinch (2006) apresentam algumas sugestões para a integração dos dados externos: (i) a escolha não subjetiva mas empírica do fator de escala; (ii) a escolha, ou não, de perdas externas com grande possibilidade de ocorrer dentro da instituição – as instituições que operam nas mesmas áreas de negócio estão expostas aos mesmos riscos, quer as perdas desses riscos tenham ocorridos ou não no passado; (iii) não escolher apenas os dados externos com base na semelhança das linhas de negócio ou outro tipo de fatores; e (iv) considerar a falta de estudos uteis para mapear a qualidade e os efeitos do ambiente de controlo interno de cada instituição na frequência ou severidade das suas perdas.

Self-assessments

Os *self-assessments* (auto-avaliação) são utilizados como metodologia para identificar falhas em controlos e riscos que impeçam a concretização dos objetivos da instituição financeira, permitindo relacionar os processos de identificação de riscos e o programa de gestão de risco com o intuito de melhorar a compreensão e o controlo dos seus riscos operacionais (Gonçalves, 2011). Desta forma, os *self-assessments* são elemento fundamental para o objetivo do risco operacional que pretende identificar, avaliar, controlar e mitigar este risco.

Para o Institute of Operational Risk (2010) um programa interno de *self-assessments* consiste nos seguintes componentes: (i) a identificação de objetivos de negócio; (ii) o reconhecimento de risco que põe em causa os objetivos definidos, e as atividades e os processos da instituição; (iii) a identificação e avaliação dos controlos implementados para a redução de risco operacional; (iv) a definição de responsabilidade para a realização dos controlos; e (v) a avaliação da efetividade dos controlos ativos e do nível de risco residual. Os resultados dos *self-assessments* permitem criar planos de ação para mitigar os riscos e melhorar os controlos. Como tal, os seus dados potenciam a importância do processo de gestão de risco

operacional, assim como, a combinação destes com outros dados, uma vez que, permite gerar indicadores valiosos - indicação de áreas susceptíveis à ocorrência de eventos de risco operacionais - e comparar os resultados da frequência e severidade registada através da matriz de risco (Gonçalves, 2011).

Os *self-assessments* como metodologia de recolha de informação proporcionam, ainda, às instituições financeiras uma arquitetura mais coerente e integrada no seu programa de gestão de risco operacional sendo uma das mais apresentadas por superiores porque é a componente que recolhe mais informação no processo de gestão de risco operacional por avaliar todos os seus procedimentos (Gonçalves, 2011).

Análise de cenários

O Acordo de Basileia II sugere às instituições financeiras a utilização de análises de cenários, juntamente com dados externos, para avaliar a sua exposição a eventos de baixa frequência e alta severidade e para identificar potenciais riscos cuja ocorrência ainda não foi detetada pelos sistemas ou que ainda não ocorreram. As instituições financeiras também utilizam as análises de cenários para avaliar o impacto de perdas potenciais que surgiram de múltiplos eventos em simultâneo, e assim possibilita avaliar a correlação entre eventos (Gonçalves, 2011). Segundo Bilby (2008) as análises de cenários são um processo orientado para recolha de opiniões de gestores de negócio e de riscos para constituir uma avaliação da frequência.

A análise de cenários é o resultado da utilização da abordagem de cálculo avançada (AMA) para modelação e quantificação de risco operacional. Este tipo de análises pode ser confundido com os testes de *stress* por os seus elementos serem orientados para o futuro no entanto a análise de cenários é apenas um dos pré-requisitos para a realização os testes de *stress* Gonçalves (2011). Na área de risco operacional, a análise de cenários pode ter objetivos quantitativos e qualitativos. Os objetivos quantitativos consistem na capacidade de complementar os dados usados para o cálculo de risco enquanto os qualitativos centram-se na avaliação de riscos que podem ser transversais em diferentes processos e ter impacto em várias unidades de negócio (Gonçalves, 2011).

O recurso à criação de cenários proporcional à instituição: (i) análises de riscos que ocorrem ou têm impacto em várias áreas da instituição; (ii) antecipar a ocorrência dos riscos – ao utilizar a análise de cenários, a instituição consegue identificar os riscos

potenciais antes que estes ocorrem sem recorrer ao processo tradicional de recolha de dados; e (iii) identificar as fragilidades – a instituição tem a capacidade de identificar as falhas nos processos de controlo (Gonçalves, 2011). A análise de cenários fornece muita informação que pode ser utilizada para melhorar os processos da instituição evitando os eventos potenciais de risco ou a elaboração de medidas que permitam reduzir perdas financeiras (Gonçalves, 2011).

Indicadores de riscos (KRI)

O modelo de avaliação de risco da instituição deve ser capaz de identificar indicadores e fatores de controlo interno que alterem o seu perfil de risco operacional (Gonçalves, 2011). Os *KRI's (key Risk Indicators)* é uma área de menor desenvolvimento nas instituição financeiras apesar de fornecer evidencia acerca a habilidade da instituição para gerir e mitigar o risco ou qual a evolução do risco ao longo do tempo (Gonçalves, 2011).

Os indicadores de risco de uma instituição fornece informação de perdas reais e potenciais possibilitando identificar antecipadamente as áreas de maior risco, assim como, indicar as tendências proporciona aos indicadores de riscos alertam para as situações de perigos são prejudiciais aos objetivos da instituição. Desta forma, a instituição pretende prevenir perdas, potenciando a tomada de decisões a tomada de decisões de mitigação pró-ativa (Gonçalves, 2011). Os indicadores de controlo (KCI) avaliam a eficácia e eficiência dos mecanismos de controlos e a capacidade da instituição de mitigar o risco operacional através dos controlos internos (Gonçalves, 2011). Para Davies, Finlay, McLenaghen, Wilson (2006) os *KRI's* produzem benefícios nas áreas de estabelecimento de limites de exposição ao risco, na otimização de estratégias de risco e na melhoria da probabilidade da instituição concretizar os objetivos com uma gestão de risco operacional mais eficaz. Da mesma forma, Gonçalves (2011) considera que a implementação de um programa de *KRI's* numa instituição financeira previne potenciais perdas e criar mecanismos de controlo que evidenciam a eficácia e eficiência dos mesmos (Gonçalves, 2011).

Apesar dos indicadores de riscos serem bastantes úteis para a instituição, estes enfrentam alguns desafios na face de aplicação: (i) conseguir demonstrar que os indicadores são capazes de identificar potenciais perdas; (ii) definição e especificação dos indicadores; e (iii) capacidade de integrar e agregar os indicadores na estrutura da instituição (Gonçalves, 2011). Para garantir o uso efetivo dos indicadores, a instituição deve documentá-los devidamente de forma a assegurar a transparência e clareza na

interpretação e implementação dos seus indicadores e deve aplicá-los numa estrutura de limites com a finalidade de controlar e acompanhar (Gonçalves, 2011).

Bases de Dados

Segundo Moosa (2008) a construção de base de dados para risco operacional iniciou-se por dois motivos: requisitos da supervisão e gestão de risco operacional. As base de dados são utilizadas para registar e classificar eventos de perdas, assim como, os resultados dos processo de auto-avaliação, os valores dos indicadores de risco e as análises de cenários (Gonçalves, 2011). Na mesma vertente, Mestchian (2003) afirma que para a construção da base dados de risco operacional, as instituições financeiras podem recorrer a seis fontes de informação: (i) dados dos sistemas operacionais da instituição – estes dados já estão disponíveis em outros sistemas da instituição e devem servir como fonte de informação para o risco operacional; (ii) dados de eventos internos – dados recolhidos através de aplicações desenvolvidas para esse fim; (iii) *self-assessments* – permitem saber qual a frequência e a severidade de determinados eventos, para os quais não há dados suficientes para análise; (iv) dados externos – atualmente existe um conjunto de consórcios (até ao momento os mais conhecidos são Global Operacional Loss Data Base – GOLDB – e o Operacional RiskData eXchange association - ORX) que desenvolvem bases de dados de eventos de risco operacional passíveis de utilizar como uma fonte de informação para o sistema; (v) análise de cenários – eventos de baixa frequência requerem um período longo de observações para realizar qualquer tipo de análise estatística; e (v) KRI – fonte relacionada com a qualidade dos ambientes operativos e de controlo da instituição.

Considerando que a base de dados de risco operacional poderá ter várias fontes de informação e os dados são fundamentais para os sistemas de informação, Marshall (2001) alerta para questões inerentes a este tipo de risco que afetam a construção da base de dados: (i) as perdas podem ser politicamente sensíveis – é necessário recolher o máximo de informação possível sobre as perdas incluindo a informação sobre clientes e colaboradores; (ii) a falta de dados para eventos pouco frequentes – neste aspeto cria-se a necessidade de integração de dados externos ou análises de cenários; (iii) utilização de dados externos; (iv) integração de dados externos com dados internos – é um processo que enfrenta desafios complexos como foi referido anteriormente; (v) integração de diferentes abordagens de modelação requerendo diferentes tipos de dados e diversos níveis de desagregação; (vi) dificuldade em modelar o comportamento humano, no sentido, em que o risco operacional é fortemente

relacionado com a componente humana; e (vii) dinâmica do risco operacional – a constantes mudanças internas e externas carecem de acompanhamento por ter consequências na realidade dos tipos de riscos e na frequência e impacto dos eventos do risco operacional.

Para Moosa (2008) existem três pontos essenciais na construção de uma base de dados para a área de risco operacional: (i) a infra-estrutura deve capturar eventos em todos os níveis da instituição; (ii) registar todas as perdas acima do nível definido e com toda a informação necessária; e (iii) existência de processo de qualidade de dados para garantir que os dados registados representam fielmente os eventos. De acordo com Gonçalves (2011), durante o processo de implementação da base de dados surgem outras questões ao nível organizacional: (i) definição de quem deverá ser responsável pelo registo da informação; (ii) quem é que deve deter a base de dados – esta questão tem sido colocada em muitas instituições e está fortemente ligada a razões históricas, a questões de reporte ou às direções responsáveis pelas atividades de controlo interno dentro da instituição; (iii) a capacidade de classificar corretamente um evento de risco operacional – ausência de formação ou esclarecimento interno sobre a forma como deverão ser classificados os eventos deste tipo de risco; e (iv) a data em que os eventos são registados – os eventos devem ser registados assim que sejam descobertos, porém normalmente o seu registo acontece ao fim de um determinado período.

A construção de uma base de dados com informação relevante e de qualidade é fundamental para calcular os indicadores da exposição da instituição aos riscos, identificar tendências e/ou encontrar as causas para determinados eventos (Mestchian, 2003). Para o sucesso da gestão de risco operacional é importante atualização frequente e utilização eficiente das bases de dados. Assim, e de acordo com as novas exigências das entidades supervisoras, todos os processos de criação e manutenção destas bases de dados devem estar devidamente documentadas.

Power (2005) refere que todos estes aspetos, bem como o processo de recolha de dados e as questões comportamentais devem estar registados na base de dados.

3.3. CÁLCULOS DE QUANTIFICAÇÃO DO RISCO OPERACIONAL

A melhor forma para gerir o risco operacional consiste na identificação e minimização deste, recorrendo a técnicas de quantificação adequadas à realidade da instituição (Bocker e Klupplber, 2005). Estas técnicas de risco operacional constituem

um conjunto de modelos estatísticos e econométricos capazes de calcular o capital económico a alocar para o risco operacional (Gonçalves, 2011).

Considerando a afirmação Mestchian (2003) sobre a utilidade da construção de base de dados para a realização de cálculos, os resultados destas análises é fornecer um conjunto de métricas possibilitando saber qual é o nível de risco a que a instituição está exposta para implementar os processos corretivos ou medidas de mitigação mais adequadas à instituição.

Uma das abordagens possível dos modelos de risco operacional divide-se em modelos *top-down* e *bottom-up*. Os modelos *bottom-up* consistem na análise de eventos de perdas em processos individuais utilizando objetivos agregados para analisar os fatores de risco operacional e eventos que causam flutuações neste objetivos (Gonçalves, 2011; Netter e Poulsen, 2003). Nos modelos *top-down* a análise é iniciada no topo da instituição seguindo para as linhas de negócio desagregando os objetivos em sub-objetivos mais detalhados e analisa que fatores e eventos têm nestes (Gonçalves, 2011; Netter e Poulsen, 2003). Para Gelderman, Klaassen e Lelyveld (2006) os modelos *top-down* apresentam limitações, porque não definem claramente a forma de gerir e controlar os resultados do modelo e que neste aspeto a abordagem *bottom-up* é mais prática neste conceito. Netter e Poulsen (2003) argumentam ainda que a abordagem *top-down* é financeiramente menos dispendiosa e mais fácil de implementar, enquanto os modelos *bottom-up* podem ser mais eficazes e relevantes para as necessidades das instituições financeiras. Currie (2004) defende o uso em simultâneo dos dois tipos de modelos para o cálculo de requisitos de capital para o risco operacional.

De acordo com Smithson e Song (2004) os modelos de risco operacional devem ser classificados em três abordagens: (i) abordagem de processos, (ii) abordagem de fatores e (iii) abordagem atuarial. A abordagem de processos incide sobre os processos individuais que compõe as atividades operacionais como tal os modelos que se focam nesta abordagem são os modelos *bottom-up*. A abordagem referida é composta por modelos causais, análises estatísticas de controlo de qualidade, análise de conectividade e dinâmica de sistemas. A abordagem de fatores centra-se na identificação dos determinantes significativos de risco operacional, quer seja ao nível de topo da organização ou quer aos níveis mais baixos engloba indicadores de riscos, modelos CAPM ou modelos preditivos. Nesta abordagem os indicadores de risco permitem identificar fatores de risco enquanto os modelos CAPM são uteis para relacionar a volatilidade dos resultados com os fatores de risco operacional. A última

abordagem, a atuarial, consiste na distribuição de perdas associadas ao risco operacional. Nesta abordagem são utilizadas as seguintes técnicas:

- Distribuições empíricas de perdas – levantamento de dados internos e externos de perdas representadas em histogramas de frequência e de severidade;
- Distribuição de parametrização explícita – estima a frequência de severidade da técnica anteriormente apresentada. A junção das duas técnicas permite obter a distribuição de perdas efetivas;
- Teoria do valor extremo (EVT) – área da estatística para aplicação a comportamento de dados externos. A teoria EVT é aplicada à modelação dos eventos externos da distribuição de perdas.

O Comité de Basileia (BCBS, 2004) propõe o cálculo de capital para risco operacional, baseando em três abordagens: (i) Indicador Básico, (ii) *Standard* e (iii) Avançada (AMA). Na abordagem do indicador básico foca-se na aplicação de uma percentagem sobre o indicador de exposição. Na abordagem S*tandard*, as atividades são divididas por linhas de negócio, correspondendo a cada uma um indicador de exposição, o qual será multiplicado por um fator de risco que reflete as perdas operacionais. A abordagem *advanced*, é reconhecida aos bancos como a capacidade para o uso de medidas internas de gestão de risco operacional, permitindo o cálculo das necessidades de capital mediante aceitação casuística pelo supervisor (BCBS, 2004). O Acordo de Basileia II determina ainda que as instituições devem demonstrar que os métodos utilizados captam eventos de perda potencialmente gravosos, de reduzida probabilidade de ocorrência, mas cujas perdas, caso ocorram, são elevadas e geradoras de medidas de risco operacional com um nível de relevância significativo similar à do método IRB (BCBS, 2004). De acordo com Pritchard (2004: 242-243), o desenvolvimento dos modelos para este tipo de risco permite produzir estimativas de perdas e informação suplementar sobre eventuais ajustamentos de capital exigidos pelo supervisor.

Na ótica das modelos avançados, a abordagem mais utilizada é a distribuição das perdas potenciais do risco operacional para um período de tempo (Figura 5). Esta abordagem foca-se na combinação das distribuições da frequência e severidade das perdas permitindo obter o *Value at Risk* (VAR) que representa o valor que a instituição estima perder a um determinado nível de confiança (Gonçalves, 2011).

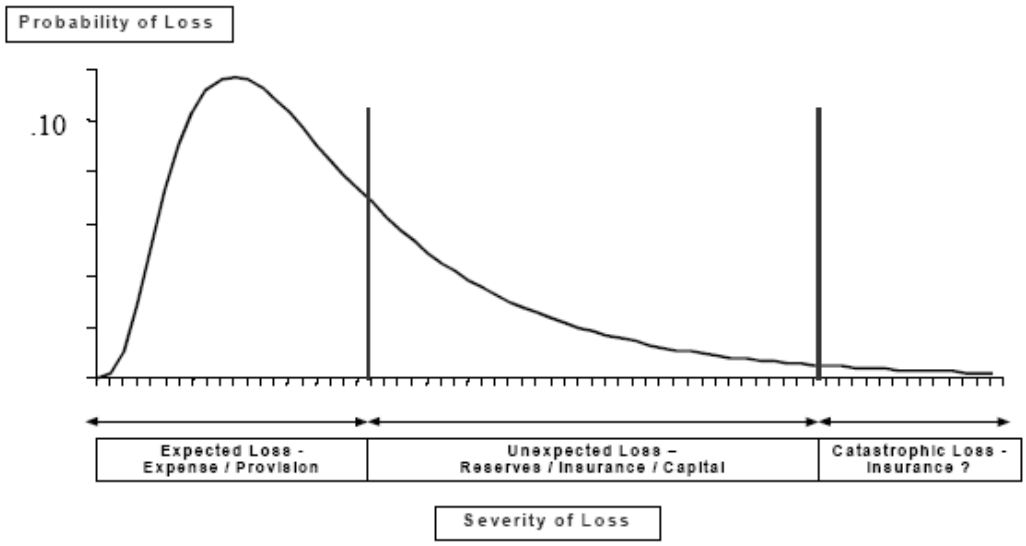

Figura 5 –Distribuição de perdas operacionais

Fonte: Rosengren 2001

Independentemente da abordagem implementada na instituição, esta deve ser transparente, capaz de captar o perfil de risco e ser aceite por toda a instituição. Esta deve documentar a estratégia adotada, referindo-se ao peso de cada abordagem para o cálculo de capital, bem como as fontes em que se baseiam os modelos (Gonçalves, 2011).

Apesar da importância da modelação do risco operacional, a sua utilização requer custos elevados e a alocação de recursos, assim como a sua utilização deve ser alargada além dos requisitos do supervisor. A utilização de modelos possibilita à instituição produzir informação útil para os processos de tomada de decisão por indicar o quanto a instituição está exposta a risco operacional e diminuir as quantidades de capital necessitário reservar para eventuais ocorrências de risco operacional (Gonçalves, 2011).

3.4. RELATÓRIOS

Sendo a apresentação da informação um requisito do Comité da Basileia, as instituições recorrem as análises para produzir relatórios que permitem uma melhor gestão de risco operacional. Helbok e Wagner (2006) afirmam que a existência de relatórios de risco operacional pode ter impactos nos custos devido às ações regulamentares e na redução do custo de capital, uma vez que o risco operacional é

um elemento fundamental na atribuição de *ratings* por parte das agências de *ratings* que disponibilizam informação o que, diretamente ou indiretamente, tem impacto no custo de capital das instituições. A dependência do risco operacional da qualidade da gestão e dos recursos das instituições torna natural o desenvolvimento de interesse dos intervenientes dos mercados financeiros na informação disponibilizada pela instituição. De acordo com esta realidade espera-se que as instituições com melhor performance são as primeiras apresentar os resultados de gestão de risco operacional o que lhes permite garantir melhores oportunidades de negócio e captar mais investimentos (Gonçalves, 2011).

Contudo, as entidades supervisoras são a maior influência para a apresentação da informação e para Watts e Zimmerman (1986) a divulgação da informação das instituições bancárias evita atenções indesejadas por parte das entidades supervisoras. Sendo o papel dos supervisores garantir a estabilidade financeira do sistema bancário, estes concentram as suas atenções nas instituições bancárias com estruturas mais fracas de capital por estas terem mais dificuldades em superar uma elevada perda operacional (Gonçalves, 2011). Além de evitar a atenção dos supervisores, a existência de relatórios de risco operacional é fundamental no processo de comunicação dentro da instituição. Estes permitem aperfeiçoar os processos de análise de riscos e de deteção de eventos de perdas e acompanhar todas as medidas de mitigação de risco.

Na área do risco operacional, assim como em outras áreas de riscos, existem um conjunto de princípios básicos para a criação de relatórios de risco operacional de forma a promover a sua gestão. Por isso, os relatórios devem apresentar de forma clara as causas dos riscos, assim como, os seus efeitos (Gonçalves, 2011). Marshall (2001) partilha a mesma opinião, afirmando que os relatórios necessitam de ser claros, completos, consistentes e com o mínimo de redundância. Considera, ainda, que devem ser normalizados para que se possa efetuar comparações com outros valores da instituição. Os relatórios devem ser disponibilizados aos gestores para que possam:

1. Avaliar o nível e a tendência dos riscos materiais e o seu efeito no capital;
2. Estimular a sensibilidade e a racionalidade de suposições usadas no sistema de cálculo de capital;
3. Determinar que as instituições asseguram o capital suficiente para os diferentes riscos e que se encontra em conformidade com os objetivos de adequabilidade de capital;
4. Avaliar os seus requisitos de capital futuro, baseados nos relatórios de perfil de risco da instituição e realizar os ajustamentos necessários.

De forma acompanhar todas as vertentes do risco operacional, os relatórios tem tido com base os *scorecards,* porque estes permitem relacionar as causas às ações e também às pessoas que são afetadas ou responsáveis por eles, tornando possível a integração de toda a organização (Mestchian, 2003). Contudo, esta área ainda é recente e não existem normas que defina um exemplo de tipo de relatórios ou os tipos de relatórios fundamentais para a gestão de risco operacional. São os gestores de riscos que definem o desenho dos relatórios para cada unidade da instituição, disponibilizando a estes um resumo de todas as atividades e áreas da gestão de risco operacional (Gonçalves, 2011). No entanto, existe um conjunto de relatórios que estão presentes na maioria dos sistemas de informação, dos quais destacam-se: o top 10 de eventos, o cálculo das perdas esperadas e não esperadas, o impacto e a frequência dos eventos em cada unidade da instituição, linhas de negócio, região, processos, entre outras dimensões, os mapas de riscos e custos e benefícios de medidas de mitigação.

Atualmente, as instituições estão a desenvolver a necessidade de agregar informação de diferentes áreas da instituição nos relatórios e análises. A razão do aparecimento desta necessidade consiste na partilha de informação entre várias áreas da instituição que contribuírem com dados para relatórios internos e para os supervisores. Como tal, são implementados sistemas de informação cuja estrutura de dados possibilita a inter-relação com dados e análises de cada área. A existência ou não de sistemas de informação sofisticados numa instituição, pretende-se que estas desenvolvam e facultem informação de risco operacional aos gestores (Gonçalves, 2011). Existem procedimentos que as instituições podem utilizar para minimizar esta questão, como por exemplo, a gestão ao nível das linhas de negócio recorre aos sistemas para visualizar questionários, identificar os indicadores de riscos, concentração de categorias de riscos e analise. Desta forma, os gestores controlam eficazmente as suas atividades, reduzem as perdas e melhoram o seu negócio.

4. METODOLOGIA

4.1. PROCESSO DE INVESTIGAÇÃO

O método científico salienta para a escolha de procedimentos sistemáticos, de modo a que seja descrita e explicada uma determinada situação sob estudo. A sua escolha deve ser baseada em dois critérios básicos: a natureza do objetivo no qual é aplicado e se o objetivo tem em vista o estudo (Fachin, 2001).

O método mais apropriado para esta investigação é um caso de estudo, porque esta investigação consiste na observação de um fenómeno no seu ambiente natural e os dados são obtidos a partir da observação. Para Yin (1994) o método do caso de estudo é aplicável quando o investigador tem dificuldades em identificar as variáveis consideradas importantes e quando o objetivo do investigador é descrever ou analisar o fenómeno de uma forma profunda e global.

Assim, Yin (1994) considera que "caso de estudo" é definido através das características do objeto de estudo e, também, as características associadas ao processo de recolha de dados e às estratégias de análise dos mesmos. Por outro lado Fidel (1992) refere que o "caso de estudo" é um método específico de pesquisa de campo. Este tipo de pesquisa são investigações de fenómenos à medida que ocorrem sem qualquer interferência significativa do investigador. Fidel refere ainda que o objetivo do caso de estudo consiste na compreensão do objeto em análise e ao mesmo tempo desenvolver teorias mais genéricas a respeito do fenómeno estudado. Para o Yin (1994) o objetivo do caso de estudo é explorar e descrever ou explicar. Refere que o caso de estudo como plano de investigação são muito extensos e demoram muito tempo para serem concluídos no entanto nem sempre é necessário recorrer a técnicas de recolha de dados que mais demoradas. Considera, ainda, que o caso de estudo apresenta alguma falta de rigor apesar de existem formas de evidenciar a validade e confiabilidade do estudo que dependem da experiência do investigador.

O objeto de estudo deste projeto é uma instituição financeira portuguesa do setor bancário. Esta está entre os líderes no plano nacional e tem um conjunto de empresas especializadas na gestão de fundos de pensões, investimento, planos de proteção, seguros, residências assistidas. Por motivos de confidencialidade não foi referido o nome da instituição alvo de estudo.

A realização deste estudo será feita com base na observação de todos os procedimentos efetuados na implementação do sistema de informação desde o

levantamento de requisitos até à fase de testes da implementação. Este acompanhamento terá sempre em atenção o papel desempenhado pela tecnologia, bem como o comportamento da instituição bancária e a sua gestão. Serão, ainda, observados os intervenientes para compreender o seu comportamento perante a implementação do sistema de informação com a finalidade de identificar as vantagens e desvantagens de utilização deste sistema no seu dia-a-dia. De forma a simplificar as mais-valias do sistema, bem como, os pontos a melhorar será efectuada uma análise de *SWOT* ao sistema implementado na instituição.

A análise *SWOT* é um sistema simples utilizada para posicionar ou verificar a posição estratégica da empresa (Dyson, 2002). É a sigla originada (Figura 6) do inglês Forças (*Strengths*), Fraquezas (*Wakness*), Oportunidades (*Opportunies*) e Ameaças (*Threats*) (Dyson, 2002).

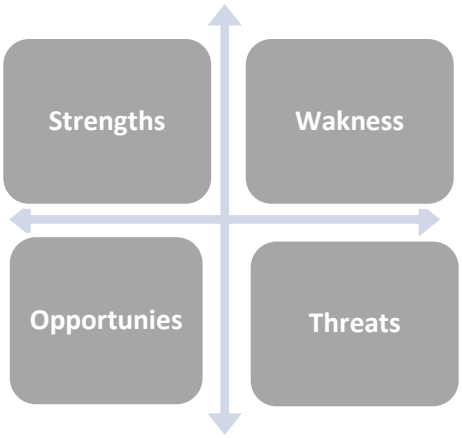

Figura 6 – Análise *SWOT*
Fonte: Elaboração própria

Esta ferramenta é composta pelo confronto entre ambientes externos e as capacidades internas do objeto em estudo. Considera-se ambientes externas as oportunidades criadas e as ameaças e as capacidades os pontos fontes e fracos do objeto em estudo (Wijngaarden, Scholten and Wijk, 2010). Com base no confronto entre estes dois pontos, a instituição pode identificar as opções estratégicas ou até mesmo um novo rumo estratégico (Johnson e Scholes, 1999). Na mesma vertente Mandour , Bekkers and Waalewijn (2005) consideram que na formulação da análise *SWOT* é fundamental a realização dos seguintes pontos:

1. Analisar como ambiente externo as oportunidades e as ameaças;
2. Analisar como ambiente interno os pontos fortes e fracos;
3. Confrontar os pontos fortes e fracos com as oportunidades e ameaças;

4. Use os resultados para formular opções estratégicas.

Por conseguinte, a análise *SWOT* consiste na descrição da relação entre eos ambientes internos e externos da instituição utilizando um conjunto de regras (Wijngaarden et al, 2010). Deste modo, esta metodologia torna-se uma ferramenta ideal no processo de gestão da implementação do sistema de informação, porque permite de uma forma muito interessante de analisar eficientemente todo o processo de desenvolvimento e, consequentemente, identificar as contrapartidas da utilização do sistema de informação no apoio à gestão de risco operacional (Dyson, 2002). Esta metodologia, ainda, é utilizada para promover a análise de cenários, uma vez que possibilita analisar o ambiente interno e externo da instituição face ao sistema implementado e permite maximizações dos processos organizacionais (Dyson, 2002). Como tal, a análise *SWOT* torna-se uma boa ferramenta de análise para atingir os objetivos deste projeto.

5. RESULTADOS E DISCUSSÃO

Como foi referido no capítulo anterior, esta investigação teve como base a observação de todas as funcionalidades do sistema de informação para a gestão de risco operacional, sua implementação numa instituição bancária e, consequentemente, avaliar esta tecnologia.

O sistema foi avaliado de acordo com os objetivos da sua implementação, incluído as mais-valias e custos face à estratégia adotada. Gonçalves (2011) apresenta

1. Capacidade de responder aos requisitos do supervisor – este critério baseia-se no funcionamento do sistema de informação: existência de *workflows* de aprovação de dados e o nível de segregação;
2. Redução de perdas e custos operacionais – este critério consiste na capacidade do sistema de informação criar conhecimento para a instituição e, assim, serem desenvolvidos planos de mitigação ou processos de negócio. Neste aspeto a avaliação foca-se na análise direta da frequência e severidade das perdas recorrendo a consultas das contas de custos operacionais ou pelo número de vezes que certas medidas de mitigação são acionadas;
3. Eficácia dos controlos internos e das medidas de mitigação – um critério referente à capacidade da instituição adotar mecanismos de controlos internos com objetivos de detetar e evitar potenciais perdas, bem como, o desenvolvimento de medidas de mitigação que melhorem os processos ou reduzam a severidade dos eventos. Para tal, o sistema deve recolher informação associada aos seus controlos e proporcionar a implementação de medidas que aumentem as capacidades dos mecanismos reduzirem a exposição da instituição ao risco operacional;
4. Melhoria na qualidade de produtos e serviços – este critério consiste na análise do impacto da gestão de risco operacional na melhoria da qualidade dos produtos e serviços. A grande questão deste critério está na correlação entre a gestão de risco operacional e as melhorias, que ainda podem ser ligadas a outros fatores. Os indicadores de riscos auxiliam a instituição a compreender a evolução da potencial melhoria, como por exemplo, o número de reclamações feitas por clientes, a diminuição dos custos de manutenção e a redução de número de falhas no processamento de operações;

5. Melhoria da cultura de risco – é um critério baseado na aceitação de risco operacional por todos os colaboradores e níveis da instituição. Esta adesão terá influência nos processos de gestão de risco operacional no sentido de aumentar o registo dos dados deste risco: recolha de eventos e responder aos questionários de avaliação de riscos e de controlos;
6. Melhoria de imagem para o mercado e para os investidores – este critério não é fácil de quantificação, contudo é um aspeto de extrema importância para a instituição, porque demonstra a qualidade e o valor da sua imagem para o mercado e para os investidores. Permitindo, assim, garantir a estabilidade e segurança da instituição e, consequentemente, aumentar o nível de confiança dos seus clientes.

Como a entrega deste projeto coincide com a conclusão da implementação do sistema na instituição, o seu processo de avaliação centra-se no desempenho do sistema até à fase de teses. Assim considerando apenas os seguintes critérios de avaliação do sistema apresentados por Gonçalves (2011): capacidade de responder aos requisitos dos supervisores, melhoria da cultura de risco e melhoria de imagem para o mercado e para os investidores. No processo de avaliação deste sistema, também, foi comtemplado a existência de uma política de risco operacional na instituição financeira e, por conseguinte, a presença de um sistema de informação para a sua gestão. Desta forma, foi inevitável realizar algumas comparações entre os sistemas.

No próximo capítulo serão apresentados os processos e funcionalidades do sistema de informação na instituição bancária, assim como, a análise SWOT.

5.1. SISTEMA DE INFORMAÇÃO DA INSTITUIÇÃO BANCÁRIA

A instituição bancária portuguesa necessitava de um sistema de informação capaz de realizar todo o processo de gestão de risco operacional de forma eficaz e eficiente a fim de produzir relatórios para disponibilizar à entidade supervisora, o Banco de Portugal, cumprindo os requisitos do segundo e terceiro pilar do Acordo de Basileia II face ao anterior sistema. Estes objetivos da instituição bancária coincidem com os requisitos definidos Mestchain (2003) afirmando que um sistema deve ser capaz de recolher a informação, medir e controlar os riscos que a instituição está exposta.

A abordagem do sistema de informação é uma decisão importante na face de implementação. Como objetivo da instituição centra-se na análise de eventos com perdas potenciais, abordagem que mais assemelhar a este objetivo é a *bottom-up.* Considera-se que a instituição adotou pela melhor abordagem de risco operacional no sentido em que esta irá ser mais eficaz e relevante para as necessidades dos gestores. O processo de implementação do modelo é bastante semelhante ao sugerido por Marshal (2001) dividindo-se em quatro etapas de forma a responder às alterações nas exposições operacionais das diferentes linhas de negócio da instituição:

1. Identificação de riscos – consiste na identificação dos riscos, processos, áreas as quais irão ser alvo de análise na gestão, são considerados apenas os que tenham um impacto significativo para as atividades e objetivos da instituição;
2. Recolha da informação – nesta etapa serão recolhidos os indicadores de análise que serão a base da apresentação de resultados;
3. Análise – permite aos gestores da instituição compreender melhor o comportamento de vários fatores de risco dentro da sua empresa bem como o seu comportamento no futuro e o impacto desses riscos na evolução do negócio da instituição;
4. Desenvolvimento de planos de resposta – a última etapa foca-se na implementação de melhores processos de controlo para que sejam antecipadas situação graves para a instituição e consequentemente melhorar os planos de ação, de modo, a responder efetivamente às situações que afetam os objetivos da instituição.

Para Gonçalves (2011), outro fator importante no sistema de informação é a arquitetura do mesmo. Refere que a arquitetura do sistema deve servir para orientar os colaboradores em direção aos objetivos essenciais da gestão de risco operacional, tendo em conta, a estratégia global da instituição. A base de dados de risco operacional da instituição bancária é composta por algumas das fontes de informação consideradas por Mestchian (2003) como fundamentais para a construção das bases de dados deste risco. As fontes de informação deste sistema são: dados dos sistemas operacionais da instituição, dados de eventos internos, *self-assessments* e *KRI's*. Os dados externos são uma fonte sugerida por Mestchian (2003) e Acordo de Basileia II no entanto a instituição não recorre a este tipo de fonte apesar da arquitetura (Figura 7) do sistema os comtemplar.

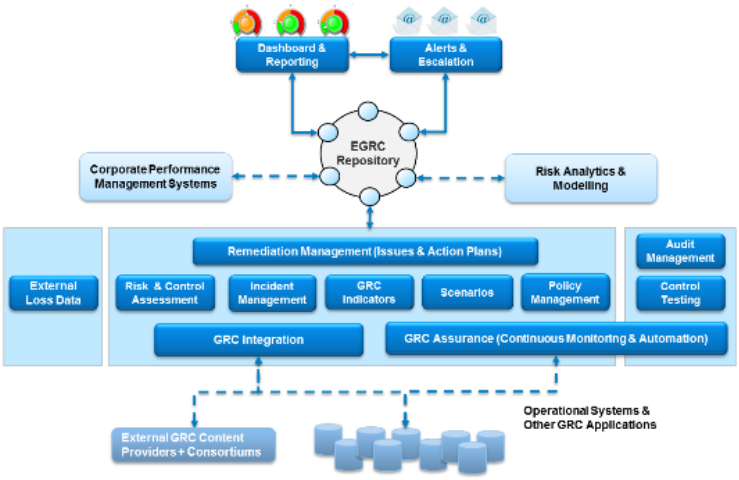

Figura 7 – Arquitetura do sistema de informação da instituição estudada
(Fonte: Documentação da instituição em estudo)

A componente dos utilizadores do sistema, também, é uma questão relevante nesta face de implementação. A instituição decidiu quais os colaboradores que teriam acesso ao sistema, quais as suas responsabilidades, o nível de autorização dentro do sistema, qual a área operacional de intervenção e, ainda, qual o âmbito e responsabilidades dos colaboradores que recebem a informação por relatórios. Foi considerado um colaborador por nível da instituição para as competências de registo, investigação, validação e aprovação; dado que ao risco operacional está associado informação sensível cada colaborador com acesso ao sistema apenas consegue observar os dados referentes à sua área operacional e competências no sistema. No final da implementação do sistema, os colaboradores terão uma formação sobre o funcionamento do sistema e, também, uma revisão do conceito de risco operacional.

Como foi referido anteriormente, este projeto consiste na gestão e criação das seguintes componentes:

1. Criação e gestão de eventos;
2. Criação e gestão de questionários;
3. Criação e gestão de KRI's;
4. Criação e Gestão de ocorrências e planos de acção;
5. Exploração de relatórios.

Criação e gestão de eventos

Na política de registo dos eventos operacionais é importante definir o *workflow* deste processo - assim como nos restantes. Este é constituído pela atribuição de capacidades/responsabilidades aos colaboradores de acordo com a hierarquia da instituição neste ponto são definidos os intervenientes nos processos de registos, investigação e validação aos quais o sistema tem a capacidade de enviar uma notificação do estado evento. Com este *workflow*, a instituição encorajem os seus colaboradores a registar todos os eventos de risco operacional sem haver algum receio de o fazer incorretamente.

Para registar um evento deve-se preencher todos os campos obrigatórios e necessários para caracterizar o evento dos quais destacam-se: o ponto operacional referente ao colaborador e o ponto operacional de deteção onde é detalhado o evento deste o nome do mesmo, às data de início, fim e deteção, a unidade orgânica onde ocorre o ventos, as linhas de negócio entre outros. Ao detalhar o evento, a instituição consegue obter maior conhecimento dos eventos a que está exposta e relacional com outros objetos. Como a um evento está quase sempre associado a um impacto financeiro, o sistema possibilita fazer este tipo de associação considerando se o evento operacional teve um impacto financeiro para instituição com natureza de perda ou ganho. No entanto o evento poderá ter um impacto ao qual a instituição não é capaz de estimar ou não é possível atribuir qualquer valor, como o caso do risco de reputação, a este cenário dá-se o nome de impactos não financeiros. Da mesma forma que o evento pode ser relacionado a impacto também pode ser considerado uma recuperação cuja origem é direta ou via segura. Como tal, um evento pode ter diversos impactos financeiros, não financeiros e recuperações.

Em suma, esta correlação entre os objetos dos eventos proporciona a instituição melhorar os relatórios a apresentar à entidade supervisora e ao mercado.

Criação e gestão de questionários

É sem dúvida a componente mais complexa e consequentemente que enfrentam mais questão na fase de implementação. Esta componente na avaliação de riscos e controlos aplicados a unidade orgânica da instituição ao qual são designadas instâncias de risco e controlo. A instituição realiza a avaliação em duas abordagens: questionário de instância de risco e controlos internos e questionários de instâncias de controlos externos – uma unidade orgânica pode estar associado a um controlo de outra unidade orgânica. Cada tipo de questionário tem um *template* no qual é definido as

questões específicas de cada objeto de avaliação. Para a avaliação dos riscos é considerado o impacto máximo e médio, a frequência máxima e média, o risco residual e inerente, o nível de risco e a mitigação do mesmo no caso da avaliação de controlos são classificadas a eficácia e eficiência do controlo na mitigação dos riscos associados.

Por norma os questionários eram enviados anualmente para avaliação contudo ao implementar este sistema os responsáveis do departamento de risco operacional consideram que outras periodicidades para avaliações. Assim, os questionários fornecem a esta instituição o conhecimento que lhe permite identificar as falhas nos controlos e, consequentemente melhorar a compreensão dos seus riscos operacionais.

Criação e gestão de KRI's

Os indicadores de risco criados através deste sistema irão ajudar a instituição avaliar o seu sucesso no que refere a níveis de risco e eficácia de controlos, possibilitando fornecer aos gestores uma visão estratégica para os desenvolvimentos de controlos e processos para mitigar riscos e ameaças. Os indicadores de riscos são quantitativos e podem ser moedas, percentagens ou outros valores. A instituição bancária alvo de estudo tem como exemplo de KRI's: o número de controlos e negócios falhados, falhas nos sistemas, falhas no reporte obrigatório, crescimento do número de colaboradores, entre outros. Os KRI's apresentam um valor máximo e mínimo bem como limites intermédios - é a instituição que define as métricas para atribuir a prioridade aos KRI's.

No processo de criação de *KRI's* o sistema da instituição permite carregá-los automaticamente via sistemas operacional e de forma manual. Este último procedimento inicia-se pela definição de um *template* para cada área em específico - recursos humanos, reclamações, entre outras. Estes *templates* deverão ser o mais detalhado possível, devem ser associados ao nível de topo da unidade orgânica e são a base de criação de *KRI's*. No momento da sua criação são definidos os proprietários do indicador, que no caso de um carregamento manual é quem introduz o valor do indicador.

Criação e Gestão de ocorrências e planos de ação

Uma ocorrência é definida como um evento que ocorreu e que exige uma resposta para a remoção desse mesmo problema, para a sua mitigação ou ambos. Já um plano de ação é tipicamente desenvolvido para a mitigar ou responder às ocorrências, muito embora possam ser criados para dar resposta a outro tipo de

eventos. Muitos dos planos de ação são criados em resposta a uma ocorrência. No entanto, um plano de ação pode ser independente da ocorrência.

Este sistema permite realizar o processo de criação de ocorrências e o desenvolvimento de planos de ação. A gestão do ciclo de vida das ocorrências e planos de ação é alcançado através da conclusão do *workflow* destas componentes. As ocorrências e planos de ação tem *workflow* separados no entanto a integração de ambos permite à instituição criar informação útil para a auditoria e relatórios. A gestão das Ocorrências inicia-se com a criação de uma ocorrência que consiste O criador da ocorrência pode notificar num conjunto de utilizadores existência da criação da ocorrência no momento da sua publicação. Na fase de de aceitação da ocorrência é possível criar um plano de ação associada à ocorrência criada. É neste momento que se inicia o processo de gestão de planos de ação, o procedimento desta componente é semelhante com o das ocorrências. Em todos os processos de gestão é enviado aos intervenientes um e-mail com o estado do objeto.

Exploração de relatórios

Os relatórios perfazem um elemento fundamental no processo de gestão de risco operacional permitindo à instituição financeira, bem como, a entidade supervisora, avaliar a sensibilidade desta ao risco operacional. Desta forma, é garantida a transparência e da efetiva disciplina de mercado.

Com base este princípio, a instituição bancária juntamente com o sistema de informação desenvolveu relatórios para cada componente de gestão: (i) eventos – top 10 de eventos, eventos com impactos financeiros e não financeiros e eventos por linhas de negócio e tipo de evento; (ii) ocorrências e planos de ação – são produzidos relatórios com um determinado período e com a prioridade e estado do objeto; (iii) *KRI's* – o utilizador define o período de reporte (mensal, trimestral e anual) e o nível de risco num determinado período; e (iv) *selft-assessments*: matriz de tolerância ao risco.

Em cada relatório o gestor pode considerar apenas os pontos operacionais mais cruciais para as suas análises e ainda tem a possibilidade de obter o detalhe nos objetos analisados com navegação pela aplicação através dos relatórios. Os exemplos de relatórios produzidos pelo sistema implementado são exemplos que Gonçalves (2011) sugere que os sistemas sejam capazes de gerar.

5.1.1. Avaliação do sistema implementado

Como foi referido anteriormente a avaliação do sistema de informação teve como base três critérios apresentados por Gonçalves (2011): capacidade de responder aos requisitos dos supervisores, melhoria da cultura de risco e melhoria de imagem para o mercado e para os investidores.

O sistema implementado na instituição bancária portuguesa tem a capacidade de responder aos requisitos do supervisor: permite a parametrização de alerta na gestão das componentes apresentadas anteriormente, no processo e estrutura da política da gestão de risco operacional da instituição estão incluídos os processos de recolha de eventos operacionais, a auditabilidade, a existência de *workflows* e a segregação de funções dos colaboradores onde são definidas responsabilidades de cada um no sistema e apenas visualizam a informação respetiva às suas responsabilidades. Estas funcionalidades existentes no sistema de informação são fatores avaliados pelo supervisor. A arquitetura do sistema possibilita a instituição melhorar a sua gestão qualitativa e quantitativa através do aumento do conhecimento dos processos, a redução das perdas e da exposição ao risco e a eventos internos e externos. De forma a garantir que a instituição cumpre os requisitos do Banco de Portugal, a instituição teve de melhorar o conceito de risco operacional perante aos colaboradores através de formações com a finalidade de garantir a recolha de dados de risco operacional contudo os colaboradores colocaram alguns entraves na implementação do sistema quando havia divergências entre o novo e o antigo sistema. A apresentação dos resultados da gestão de risco operacional torna-se fundamental no processo de comunicação dentro da instituição para demonstrar aos colaboradores mais desconfiados a importância do risco operacional e sensibilizá-los para os impactos da ocorrência de eventos deste tipo de risco. Ao divulgar os resultados a instituição garante mais oportunidades de negócio e capta mais investimento devido transmite uma estabilidade para os agentes económicos.

Com esta implementação deste sistema foi melhorada a visão dos investidores em relação à instituição que investem é alterada, este sabe qual a capacidade da instituição face à ocorrência de eventos operacionais, bem como, a melhor forma de os prevenir e mitigar. A imagem da instituição para o mercado também é melhorada como a implementação de política de gestão de risco operacional e sistemas de informação por garantir e transparecer uma segurança no funcionamento da instituição, bem como o seu desempenho. Esta realidade defende a solidez do sistema

financeira garantido que os intervenientes no mercado tenham acessos às atividades da instituição bancária.

5.2. ANÁLISE SWOT APLICADA AO SISTEMA DE INFORMAÇÃO

Este capítulo centra-se na avaliação do sistema de informação implementado na instituição bancária. Como foi referido em outros capítulos, esta avaliação será feita através da análise de *SWOT* tendo em conta os critérios no capítulo anterior, as funcionalidades pretendidas pela instituição e as do próprio sistema.

De seguida, são apresentadas as componentes da análise de *SWOT* para o sistema de informação:

- Pontos fontes: (i) a base de dados é composta por dados internos (eventos operacionais), *self-assessments* e *KRI's*, sendo capaz de efetuar a sua recolha, assim como, a sua gestão. Desta forma, são cumpridos os requisitos de Mestchain (2003) para um sistema de informação; (ii) o sistema implementado sustenta a teoria apresentada por Kingsley et al. (1998) face à configuração do sistema para responder à especialidade de cada tipo de risco e em todos eles incluí as funções base: capacidade de avaliar a perda potencial das atividades da instituição, identifica as causas ou as fontes de risco que pode originar uma perda, indicar os fatores que determinam a falha nos controlos que contribuírem para perda e apresentar informação histórica face ao tipo de perda; (iii) também, pode-se comprovar este sistema a presença de algumas considerações de Kross (2009) das quais destacam-se: uma arquitetura permita a recolha sistemática de dados, a base de dados contém as perdas internas passível de integração com dados externos e possibilita apontar os fatores de riscos através dos questionários; (iv) nos processos de recolha de dados de perdas internas da instituição o sistema respeita as linhas consideradas pelo Comité de Basileia (BCBS, 2003) e Mestchian (2003): a instituição mapeia os seus dados históricos de perdas internas – linha orientada, também, por Kingsley et al. (1998) – perdas de risco operacionais relacionada com o risco de crédito, o sistema faculta a instituição na recolha de informação sobre a data de evento, quaisquer recuperações e descrição das causas de evento de perdas; (v) a

interligação entre as dimensões da instituição: linha de negócio, unidade orgânica, processos, riscos e controlos, permite melhorar a qualidade dos relatórios e das análises (Gonçalves, 2011); (vii) foram dadas aos colaboradores que irão utilizar o sistema formações sobre o conceito de risco operacional e o comportamento do sistema na política de registo de dados de risco operacional. Assim são minimizados os problemas da falta de dados deste tipo de risco apresentado por Muzzy (2003).

- Pontos Fracos: (i) elevados custos e manutenção: dado o nível de complexidade do sistema implementado, a instituição necessita de recursos qualificados tanto ao nível técnico como ao funcional.
- Oportunidades: (i) cálculo de quantificação de risco operacional, embora a instituição não tenha requerido esta funcionalidade, o sistema permite a realização de cálculos para quantificar este risco possibilitando, futuramente, a utilização da mesma. Um dos exemplos é o cálculo do Value-at-Risk (VAR) possibilita à instituição calcular a estimação de perdas recorrendo aos dados de risco operacional; (ii) dados externos: embora a instituição bancária não esteja a utilizados este tipo de dados a arquitetura do sistema implementado está preparada para ter fontes de dados externos; (iii) análise de cenários; (iv) utilização de abordagens mais avançadas tornando a instituição mais sensível às questões do risco operacional e mais autonomia por parte da instituição em relação aos requisitos dos supervisores;
- Ameaças: (i) dificuldades culturais inerente à gestão de risco operacional: a maioria dos colaboradores da instituição desconhece o conceito e importância do risco operacional vertente salientada por Gonçalves (2011); (ii) assimilação das ferramentas: a presença de outro sistema de gestão de risco operacional na instituição financeira tornou-se um entrave à implementação de um novo por limitar as suas funcionalidades uma vez que os colaboradores estavam bastante dependentes do antigo sistemas querendo que a disposição da informação fosse semelhante quando os sistemas abordam as competências de diferentes perspetivas. De certa forma foram minimizadas algumas das potencialidades deste sistema portal dependência.

6. CONCLUSÕES

Há muita discordância entre os investigadores e profissionais de risco operacional em relação ao conceito deste tipo de risco, bem como, as suas causas, consequências, características e gestão. Esta falta de consenso aumenta as questões sobre o que é o risco operacional, o que é considerado como risco operacional e, ainda, como medir e classificar o mesmo. No entanto, nos últimos anos o risco operacional tem vindo a ser alvo de programas de gestão nas instituições, de regulamentação e de estudos académicos, representando assim o início da consciencialização para o risco operacional e o seu impacto nas instituições. Com o objetivo de incentivar as instituições a criar processos de gestão de risco operacional, o Acordo de Basileia II exerce pressões para que estas incluem o risco operacional na sua política de gestão de risco.

Apesar das críticas feitas ao Acordo de Basileia II, as instituições financeiras seguem as suas orientações tirando partido da gestão de risco operacional para diminuir as perdas e melhorar produtos e serviços. Não há dúvidas da importância da implementação de uma política de gestão de risco operacional e, a parte das pressões regulamentares, a maioria das instituições financeiras estão a desenvolver os seus próprios procedimentos na criação de políticas e processos de gestão de risco operacional. Considerando este objetivo, as instituições bancárias estão a optar por implementação ou desenvolvimento de um sistema de informação para gestão de risco operacional. Gonçalves (2011) considera que os sistemas de informação para as instituições têm como objetivo primário apenas a captura de informação necessária para responder aos requisitos da entidade supervisora. A maioria das instituições pretende funcionalidades que lhe forneçam informação e, consequentemente, a construção de uma base de dados de risco operacional. O sistema encara fortes desafios na área de integração de dados com outras aplicações, assim como, na aderência dos colaboradores face à sua utilização.

Apesar das dificuldades indicadas, as instituições deverão continuar a desenvolver/melhorar os seus sistemas de informação criando novas funcionalidades para recolher e criar informação que lhes permita reduzir as perdas e os custos operacionais, melhorar os processos, serviços e produtos tendo como principal objetivo o aumento do nível de satisfação dos clientes e dos colaboradores.

No estudo apresentado, observou-se a existência da necessidade de um sistema de informação para a área de risco operacional que cumprisse os objetivos da gestão

deste tipo de risco da instituição, e que respondesse aos requisitos do Banco de Portugal. É de salientar que a instituição analisada já possuía um sistema de informação para gestão de risco operacional que considerava a gestão de eventos e de questionários de controlos e riscos - desta forma, era apenas cumprindo o básico dos requisitos do Acordo de Basileia II. Com as novas exigências da entidade supervisora para a instituição bancária, destacando as áreas de reporte, segregação de funções e auditabilidade, formou-se a necessidade de desenvolver um sistema que obedecesse às imposições e fosse mais completo.

Embora a principal razão para instituição bancária implementar este sistema fosse responder as novas exigências da entidade supervisora, o sistema não contêm apenas os aspetos regulamentares, permitindo à instituição conhecer os riscos, definir os índices dos riscos chaves e agir para diminuir os fatores de riscos, desta forma, são sustentadas as afirmações de Mestchain (2003) e de Kross (2009). No processo de implementação do sistema também foi comprovada outra afirmação de Mestchian (2003): os objetivos da gestão de risco operacional foram a chave para decidir as funcionalidades específicas do sistema implementado. Neste sentido, a instituição apenas considerou as funcionalidades que cumprissem os seus objectivos iniciais apesar do sistema possuir funções que iriam enriquecer o conhecimento dos gestores e os objetivos da política de gestão. Destas funcionalidades do sistema destacam-se: utilização de métodos avançados, controlo interno e auditoria.

Durante a implementação do sistema de informação na instituição bancária foram identificados algumas dificuldades dos quais se destacam:

- Integração dos dados – dado que a instituição estudada é um grupo económico foi necessário agrupar os dados provenientes das várias entidades da instituição. Para isso, foi essencial saber a exposição global da instituição em relação ao risco operacional, bem como, analisar o perfil de risco e as medidas de mitigação;
- Recolha de dados – continua a ser a problemática da prática da gestão de risco operacional. O desconhecimento do conceito de risco operacional por parte dos responsáveis pelo registado dos eventos deste risco origina a má classificação dos eventos sendo estes registados em outros sistemas ou então não são considerados eventos de risco operacional. Como tal, foi sugerida a formação aos utilizadores do sistema implementado;

- Colaboradores – por parte dos colaboradores da instituição houve algumas imposições face ao novo sistema fazendo comparações entre os dois sistemas.

Em Portugal, esta estratégia é bastante comum devido à pouca experiência de implementação de sistemas de informação para a gestão de risco operacional e o desconhecimento das vantagens de utilização de sistemas complexos e mais desenvolvidos (Gonçalves, 2011). Por isso, prevê-se que os futuros sistemas de informação deixem de ser apenas um instrumento de resposta aos requisitos da entidade supervisora passando a possuir ferramentas de processamento de dados, de descoberta de comportamentos e padrões, assim como, produzir informação que proporciona à instituição melhorar os seus processos internos e de incutir uma cultura de risco na instituição (Gonçalves, 2011). Para o sistema de informação implementado na instituição bancárias surge-se que os próximos desenvolvimentos sejam focados na integração do sistema de riscos operacional com outros sistemas da instituição: uma das fontes de informação de risco operacional são os sistemas de outras áreas da instituição. Por isso, é importante que esta integração seja feita, porque possibilita melhorias quantitativas e qualitativas na forma como os processos serão implementados; e modelação de dados: é evidente a falta de técnicas e metodologias para a modelação de risco operacional. As técnicas de *data mining* são uma boa ferramenta para a criação de modelos e comportamentos que permite às instituições identificar os fatores de risco mais significativos.

7. LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Atualmente as instituições financeiras estão apostar fortemente em ferramentas de gestão de risco operacional, mais concretamente na implementação de sistemas de informação. Esta aposta surge por pressões regulamentares, em que a maioria das instituições pretende responder aos requisitos das entidades supervisores.

Assim, esta investigação centra-se na importância de um sistema de informação para a gestão de risco operacional apresentando as dificuldades/desafios decorrentes da implementação do sistema, identificar os pontos fortes e fracos, bem como, as oportunidades. Ou seja, esta investigação pretende evidenciar as mais-valias da implementação do sistema e alertar para os problemas que podem advir desta implementação, permitindo à instituição tomar medidas para minimizá-los. Contudo, não foi possível concluir todos os objetivos aos quais foram propostos realizar por o final da implementação do sistema na instituição alvo de estudo coincidir com a entrega deste projeto. Dos objetivos não concluídos destacam-se: as oportunidades de negócio que a instituição poderá criar com a implementação do sistema e a criação de valor proporcionada pela implementação do sistema. Estes objetivos terão resposta ao fim de algum período de utilização do sistema como tal a falta de resposta para estes objetivos vai de encontro como uma das limitações deste projeto, a data de entregue do mesmo coincidir com a conclusão da implementação do sistema de informação.

Com a evolução da gestão de risco operacional nas instituições incentiva a novos desenvolvimentos e exigências nos sistemas de informação. As alterações nas atividades da instituição requerem sejam redefinidas novas estratégias salientando, também, a necessidade de efetuar novos desenvolvimentos aos sistemas. Na instituição bancária alvo de estudo recomenda-se os seguintes estudos:

- Avaliar os restantes critérios de avaliação dos sistemas de informação sugeridos por Gonçalves (2011) com a finalidade a fazer uma avaliação detalhada das funcionalidades e utilidade do sistema para a instituição;
- Analisar os resultados dos processos de auditoria efectuados pelo Banco de Portugal e pelas auditoras externas ao desempenho do sistema de informação implementada na instituição bancária.

8. BIBLIOGRAFIA

Allen, L., & Bali, T. G. (2004). Cyclicality in Catastrophic and Operational Risk Measurements. *Unpublished paper, City University of New York.*

BCBS. (2001). Basel II: The New Basel Capital Accord-Second Consultative Paper. *Basel: Bank for International Settlement.* www.bis.org [Consultado em janeiro].

BCBS. (2001). Operational Risk – Supporting. *Document to the New Basel Capital Accord, (January),* pp. 1-17. www.bis.org [Consultado em janeiro].

BCBS. (2003). Basel II Acord, *BIS: Bank for International Settlements.* www.bis.org [Consultado em novembro].

BCBS. (2003). Sound Practices for the Management and Supervision of Operational Risk. *BIS: Bank for International Settlements, (February)*. www.bis.org [Consultado em abril].

BCBS. (2004). International Convergence of Capital Measurement and Capital Standards – A Revised Framework. *BIS - Bank for International Settlements (June)*, pp. 1-239. www.bis.org [Consultado em maio].

Bielski, Lauren (2003). On the eve of Basel II, banks get a move on ops risk. *American Bankers Association. ABA Banking Journal, vol. 95, n.º 10, (Outubro),* pp. 59-62.

Bielski, L. (2003). On the eve of Basel II, banks get a move on ops risk. *American Bankers Association (ABA) Banking Journal, vol. 95, n.º 10*, (Outubro), pp. 59-62.

Bilby, R. (2008). Using Scenario Analysis to Achieve Sound Operational Risk Management. *Paper Presented at the OpRisk Asia Conference*, Singapore 2–4.

Blunden, T. (2003). Operational Risk: Regulation, Analysis and Management, ed. C. Alexander. London: Prentice Hall- Financial Times. Scoreboard Approaches. Pp. 229–240

Bocker, K., & Kluppelberg, C. (2005).Operational VAR: A Closed-Form Approximation. *Risk December*, pp 90–93.

Bolton, N. & Berkey, J. (2005). Aligning Basel II Operational Risk and Sarbanes- Oxley 404 Projects. *Operational Risk: Practical Approaches to Implementation, ed. E. Davis.* London: Risk Books. Pp. 237–246

Brink, G. J. (2002). Operational risk: the new challenge for bank (1ªedição). Palgrave, New York.

Buchelt, R., & Unteregger, S. (2004). Cultural Risk and Risk Culture: Operational Risk after Basel II. *Financial Stability Report 6.* http://www.oenb.at/en/img/fsr 06 cultural risk tcm16–9495.pdf.

Cagan, P. (2005). External Data: Reaching for the Truth. www.operationalriskonline.com.

Chorafas, D. N. (2001). Managing Operational Risk: Risk reduction strategies for investment and commercial banks. *Euromoney Books*.

Comissão de Coordenação da Segurança. (2010). Riscos de Corrupção e Infracções Conexas. *Banco de Portugal Maio*. pp. 22-28.

Crouchy, M., Galai, D. & Mark, R. (1998). Key Steps in Building Consistent Operational Risk Management and Measurement. *Operational Risk and Financial Institutions*. London: Risk Books. Pp. 45–62.

Crouchy, M. (2001). Risk Management. *New York: McGraw Hill*.

Cummins, J. D., Lewis, C. M., & R. Wei. (2006). The Market Value Impact of Operational Loss Events for US Banks and Insurers. *Journal of Banking and Finance*. Pp 2605–2634.

Currie, C. V. (2004). Basel II and Operational Risk: An Overview. *Operational Risk Modelling and Analysis. London: Risk Books*. Pp. 271–286

Currie, C. V. (2006). A Test of the Strategic Effect of Basel II Operational Risk Requirements on Banks. *ICFAI Journal of Monetary Economic*. Pp 6-28.

Daníelsson, J., Embrechts, P., Goodhart, C., Keating, C., Muennich, F., Reneault, O., & Shin, Hyun Song. (2001). Academic Response to Basel II. LSE Financial Markets Group. Maio. pp13-14.

Davies, J. F., M. McLenaghen, T., & Wilson, D. (2006). Key Risk Indicators – Their Role in Operational Risk Management and Measurement. *The Advanced Measurement Approach to Operational Risk*. *London: Risk Books*. Pp. 215–245

Dayson, G. D. (2002). Strategic development and SWOT analysis at the University of Warwick. *European Journal of Operational Research 152.* pages 631–640

Deparmento de Supervisão Bancário. (2007). MAR - Modelo de Avaliação de Riscos, *Banco de Portugal*. pp 97-114.

Derrien, Yann & Goldenberg, Joël (2003). Risque Prudentiel – Risque opérationnel – Bâle 2 : premier bilan de la mise en place des bases incidents à la Caisse des d´pôts. *BANQUEmagazine, n.º 647 (Maio).* pp. 58-61.

Documentação da Instituição Bancária utilizada como objeto de estudo.

Fachin, Odília (2001). Fundamentos de metodologia. São Paulo: saraiva.

Ferreira, Luís. (2004). O risco na indústria financeira. Disponível em: http://www.ifb.pt/publicacoes/info_61/artigo02_61.htm. [Consultado em maio]

FIDEL, Raya (1992). The case study method: a case study. *GLAZIER, Jack D. & POWELL, Ronald R. Qualitative research in information management. Englewood, CO: Libraries Unlimited*. Pp.37-50.

Geiger, Hans. (2002). Regulation and Supervising Operational Risks for Banks. *Future of Financial Regulation: Global Regulatory Reform and Implications for Japan.*

Gelderman, M., P. Klaassen, & Lelyveld , I. van. (2006). Economic Capital: An Overview. *Economic Capital Modelling: Concepts, Measurement and Implementation, London: Risk Books*. Pp. 1–12

Gibson, Michael S. (1997). Information Systems for Risk Management,. www.bog.frb.fed.us.

Gonçalves, R. (2001). Sistema de informação para gestão de Risco Operacional em instituições financeiras.

Haas, M., & Kaiser, T. (2004). Tackling the Inefficiency of Loss Data for the Quantification of Operational Loss. *Operational Risk Modelling and Analysis: Theory and Practice, London: Risk Books*. Pp. 13–24

Halperin, K. (2001). Balancing Act. *Bank Systems and Technology pp22–25*.

Helbok, Gunther., & Wagner, Christian. (2006). Determinants of Operational Risk Reporting in the Banking Industry. *Journal of Risk*.

Institute of Operational Risk. (2010). Risk Control Self-Assessment.

Johnson G., & Scholes K. (1999). Exploring Corporate Strategy. *Prentice Hall: London.*

Kaiser, T., & Kohne, M. (2006). An Introduction to Operational Risk. *London: Risk Books*.

Kingsley, S., Rolland, A., Tinney, A., & Holmes, P. (1998). Operational Risk and Financial Institutions: Getting Started. *Operational Risk and Financial Institutions. London: Risk Books*. Pp. 3–28

Kross, W. K. (2009). Integrating Management into Oprisk Management. *Operation Risk Toward Basel III, ed. Greg N. Gregoriou. New Jersey: John Wiley & Sons*. Pp. 249-288

Lopez, J. A. (2002). What is Operational Risk?. *Federal Reserve Bank of San Francisco Economic Letter January.*

Mandour Y., Bekkers M., & Waalewijn P. (2005). Praktische kijk op marketing- en strategiemodellen (Dutch). *Academic Services: Schoonhoven*.

Marshall, C. (2001). Measuring and Managing Operational Risks in financial institutions – Tools. *Techniques and Other Resources, John Wiley & Sons*.

Medova, E. A., & Kyriacou, M. N. (2001). Extremes in Operational Risk Management. *Unpublished paper, University of Cambridge*.

Mestchian, Peyman. (2003). Operational Risk Management: The Solution is in the Problem. *Advances in Operational Risk – Firm-wide Issues for Financial Institutions (2 Ed.), Risk Books*.

Mintzberg H., & Quinn JB. (1992). The Strategy Process: Concepts and Context. *Prentice Hall international: London*.

Moosa, I. A. (2007). Misconceptions about Operational Risk. *Journal of Operational Risk Winter, pp* 97–104.

Moosa, I. A. (2007). Operational Risk Management. *London: Palgrave*.

Moosa, I. A. (2007). Operational Risk: A Survey. *New York University Salomnn Center, Financial Markets, Institutions & Instruments, V. 16. No.4.*

Moosa, I. A. (2008). Quantification of Operational Risk Under Basel II. *The Good, Bad and Ugly. Financial and Capital Market Series, University of Reading.*

Morris, Robert Associates., & British Bankers. (1999). Association and International Swaps and Derivatives Association. *Operational Risk: The Next Frontier. Philadelphia: RMA.*

Muzzy, L. (2003). The Pitfalls of Gathering Operational Risk Data. *RMA Journal 85*: pages 58–62.

Netter, J. M., & Poulsen A. B. (2003). Operational Risk in Finance Service Providers and the Proposed Basel Capital Accord: An Overview. *Advances in Financial Economics, 8*, pages 147-172.

Peccia, A. (2003). Using Operational Risk Models to Manage Operational Risk. *Operational Risk: Regulation, Analysis and Management. London: Prentice Hall-Financial Times.*

Pezier, J. (2003). A Constructive Review of the Basel Proposals on Operational Risk. *Operational Risk: Regulation, Analysis and Management London: Prentice Hall-Financial Times*, pages 49–73

Ponte, J. P. (2006). (1994). Estudos de caso em educação matemática. *Bolema, 25,* page 105-132.

Power, M. (2005). The Invention of Operational Risk. *Review of International Political Economy 12*, pages 557-599.

Pritchard, J. (2004). Implementing Basel II in the Norwich and Peterborough Building Society. *Journal of Financial Regulation and Compliance, vol. 12, n.º 3 (Agosto)*, pages 240-243.

Rao, V., & Dev, A. (2006). Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institutions. *The Advanced Measurement Approach to Operational Risk, London: Risk Books*, pages 273–294

Rebonato, R. (2007). The Plight of the Fortune-Tellers: Thoughts on the Quantitative Measurement of Financial Risk. *Unpublished manuscript.*

Ripault, M., & Look, I. (2003). Risque & Prudentiel, Bâle II – Les enjeux du risqué opérationnel pour les brokers. *BANQUEmagazine, n.º 646 (Abril)*, pages 62-64.

Rodríguez, L. J. (2003). Banking Stability and the Basel Capital Standards. *Cato Journal, vol. 23, n.º 1 (Spring/Summer)*, pages 115-126.

Rosengren, E. (2001). Capital Allocation for Operational Risk – Implementation Challenges for Bank Supervisors*. Joint Operational Risk Conference*.

Samad-Khan, A., Moncelet, B. & Pinch, T. (2006). Uses and Misuses of Loss Data. www.opriskadvisory.com.

Smithson, C., & P. Song. (2004). Quantifying Operational Risk. *Risk July*, pages 50–52.

Wahler, B. (2002). Process-Managing Operational Risk – Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II-Framework. http://papers.ssrn.com/sol3/papers.cfm?abstract id=674221.

Watts, R., & Zimmerman, J. (1986). Positive Accounting Theory. *London: Prentice Hall International.*

Wei, R. (2003). Operational Risk in the Insurance Industry. *Unpublished paper, University of Pennsylvania.*

Wei, R. (2006). An Empirical Investigation of Operational Risk in the United States Financial Sectors. *University of Pennsylvania.*

Wei, R. (2007). Quantification of Operational Losses Using Firm-Specific Information and External Databases. *Journal of Operational Risk 1 Winter,* pages 3–34.

Wijngaarden, J. D. H., Scholten, G., Wijk, R. M. & Kees P. van. (2010). Strategic analysis for health care organizations: the suitability of the SWOT-analysis. *International Journal of Health Planning and Management Int J Health Plann Mgmt 2012, Published online 5 July 2010 in Wiley Online Library.* 27, pages 34–49

Yin, R. (1994). Case Study Research: Design and Methods. *Thousand Oaks, CA: SAGE Publications*

Yin, R. (2001). Case study research: Design and methods. *Newbury Park, CA: Sage*.