DEPARTAMENTO DE
Engenharia Mecânica e Industrial

NOVA SCHOOL OF
SCIENCE & TECHNOLOGY

Gonçalo Maria Steglich Canas Lopes Ribeiro
Licenciado em Ciências da Engenharia e Gestão Industrial

Estudo e Avaliação de um Sistema de Gestão de Risco Operacional: O Caso de uma Empresa Seguradora em Portugal

Dissertação para obtenção do Grau de Mestre em Engenharia e Gestão Industrial

Mestrado Integrado em Engenharia e Gestão Industrial
Universidade NOVA de Lisboa
Setembro, 2023

Departamento de Engenharia Mecânica e Industrial

Estudo e Avaliação de um Sistema de Gestão de Risco Operacional: O Caso de uma Empresa Seguradora em Portugal

Dissertação para obtenção do Grau Mestre em Engenharia e Gestão Industrial

Gonçalo Maria Steglich Canas Lopes Ribeiro

Licenciado em Ciências de Engenharia e Gestão Industrial

Orientadora: Doutora Maria do Rosário de Meireles Ferreira Cabrita,
Professora Associada com Agregação da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Júri:

Presidente: Doutora Maria Celeste Rodrigues Jacinto,
Professora Associada com Agregação da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Arguente: Doutor Joaquim Amaro Graça Pires Faia e Pina Catalão Lopes,
Professor Associado da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Orientador: Doutora Maria do Rosário de Meireles Ferreira Cabrita,
Professora Associada com Agregação da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Membros: Dr. António Vieira,
Manager - Departamento de Gestão de Risco Operacional da Fidelidade - Companhia de Seguros SA

Mestrado Integrado em Engenharia e Gestão Industrial

Universidade NOVA de Lisboa
Setembro, 2023

Estudo e Avaliação de um Sistema de Gestão de Risco Operacional: o Caso de uma Empresa Seguradora em Portugal

Copyright © Gonçalo Maria Steglich Canas Lopes Ribeiro, Faculdade de Ciências e Tecnologia, Universidade NOVA de Lisboa.

A Faculdade de Ciências e Tecnologia e a Universidade NOVA de Lisboa têm o direito, perpétuo e sem limites geográficos, de arquivar e publicar esta dissertação através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, e de a divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

À minha família

AGRADECIMENTOS

Começo por agradecer à Professora Maria do Rosário Cabrita pela orientação, disponibilidade e dedicação neste projeto. Por me ter acompanhado nesta etapa da minha vida académica.

Gostaria de agradecer a toda a equipa do Departamento de Gestão de Risco Operacional da Fidelidade pela oportunidade de desenvolver a minha dissertação e pelo apoio e dedicação durante o estágio. Quero demonstrar o meu agradecimento, em especial, ao António Vieira, Manager do Departamento de Gestão de Risco e Operacional, por todo o apoio e orientação no desenvolvimento desta dissertação.

À minha família, Mãe, Ruben, Pai, Susana, irmãos, avós e primos pelo apoio incondicional, pela ajuda nas várias etapas da minha vida e a quem devo um enorme obrigado.

À Rita, que esteve lá sempre a acompanhar nos melhores e nos piores momentos, sempre pronta a motivar-me para ultrapassar esta etapa tão importante.

Aos meus amigos, por me acompanharem neste percurso, por toda a ajuda, motivação e compreensão e por tornarem o meu percurso melhor.

"To succeed in an environment of growth and change,
we must accept risk as a part of the process." (Phil Knight).

RESUMO

Face ao aumento da importância do risco operacional e das suas consequências, nas últimas décadas, as instituições financeiras e os reguladores têm-se focado cada vez mais na criação de sistemas de gestão de risco operacional robustos. Por conseguinte, a regulamentação tem evoluído para que se reduza a exposição ao risco operacional.

Desta forma, a União Europeia introduziu o regime de Solvência II para diminuir os problemas de solvência do mercado segurador e ressegurador europeu. O Pilar I compreende os requisitos quantitativos de Capital, em que se calcula o Requisito de Capital de Solvência (SCR), através da aplicação da fórmula-padrão. O Pilar II compreende os requisitos qualitativos, que abrange os sistemas de governação. O Pilar III compreende a transparência e a disciplina de mercado, através da divulgação pública de informação e de reporte. O Pilar II é uma novidade do regime de maneira a colmatar algumas das limitações do Pilar I e da aplicabilidade da fórmula-padrão para determinar o requisito de capital do Risco Operacional.

A presente dissertação destaca a importância de implementar sistemas de gestão de risco e controlo interno robustos e eficazes, bem como implementar estratégias e medidas para mitigar e reduzir a exposição do risco operacional.

Para tal, recorreu-se ao método aplicado e desenvolvido pela Fidelidade, o Ciclo ROCI (Risco Operacional e Controlo Interno) composto por cinco etapas, que permite identificar e avaliar os riscos e os controlos associados às atividades das áreas de negócio, bem como reportar a sua exposição e propor oportunidades de melhoria.

Analisaram-se os processos de 17 áreas e identificaram-se 414 riscos, 204 controlos e 67 oportunidades de melhoria. Apenas 20% dos riscos possuíam avaliação quantitativa, aproximadamente, com um VaR acumulado de 3,5M€. Comparou-se a avaliação do risco com o registo de 10 eventos de risco operacional. Constatou-se que 24% dos controlos têm deficiências a nível da eficácia e execução.

Por fim, o Ciclo ROCI fornece informação mais detalhada e realista sobre a exposição do risco operacional, algo que a fórmula-padrão não é capaz, evidenciando a utilidade e eficácia do método.

Palavras chave: Risco Operacional, Sistemas de Gestão de Risco, Solvência, Pilar I, Pilar II, Ciclo ROCI, Exposição, VaR, Controlo Interno, SCR, Fórmula-Padrão, Eventos de risco operacional

ABSTRACT

Given the growing importance of operational risk and its consequences, financial institutions and regulators have increasingly focused on creating robust operational risk management systems in recent decades. As a result, regulations have evolved to reduce exposure to operational risk.

The European Union introduced the Solvency II regime to reduce solvency problems in the European insurance and reinsurance markets. Pillar I comprises the quantitative capital requirements, in which the Solvency Capital Requirement (SCR) is calculated by applying the standard formula. Pillar II comprises qualitative requirements, covering governance systems. Pillar III comprises transparency and market discipline, through public disclosure of information and reporting. Pillar II is new to the regime to address some of the limitations of Pillar I and the applicability of the standard formula for determining the Operational Solvency capital requirement.

This dissertation highlights the importance of implementing robust and effective risk management and internal control systems, as well as implementing strategies and measures to mitigate and reduce operational risk exposure.

To do so, the method applied and developed by Fidelidade was used, the five-step ORIC Cycle (Operational Risk and Internal Control), which makes it possible to identify and assess the risks and controls associated with the activities of the business areas, as well as to report on their exposure and propose opportunities for improvement.

The processes of 17 areas were analysed and 414 risks, 204 controls and 67 opportunities for improvement were identified. Only approximately 20 per cent of the risks had a quantitative assessment, with an accumulated VaR of €3.5 million. The risk assessment was compared with the recording of 10 operational risk events. It was found that 24 per cent of controls were deficient in terms of effectiveness and execution.

Finally, the ORIC Cycle provides more detailed and realistic information on operational risk exposure, something that the standard formula is not capable of, demonstrating the usefulness and effectiveness of the method.

Keywords: Operational Risk, Risk Management Systems, Solvency, Pillar I, Pillar II, ORIC Cycle, Exposure, VaR, Internal Control, SCR, Standard Formula

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

SIGLAS

Adj	Ajustamento das Provisões Técnicas e dos Impostos Diferidos em função da capacidade de absorção das respetivas perdas.
ASF	Autoridade de Supervisão de Seguros e Fundos de Pensões.
BSCR	Requisito de Capital de Solvência Básico
BCP	*Business Continuity Planning*
BES	Banco Espírito Santo
BN	*Bayesian Networks*
CBSB	Comité de Supervisão Bancária de Basileia
CEIOPS	*Committee of European Insurance and Occupational Pensions Supervisors*
CGD	Caixa Geral de Depósitos
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CRO	Chief Risk Officer
DGRO	Direção Geral de Risco Operacional
EFQA	*European Foundation for Quality Management*
EIOPA	*European Insurance and Occupational Pension Authority*
ERM	*Enterprise Risk Management*
Expul	Despesas anuais (bruto de resseguro)
GRC	*Governance, Risk and Compliance*

IA	Inteligência Artificial
IAA	*International Actuarial Association*
IAIS	*International Association of Insurance Supervisors*
IASB	*International Accounting Standards*
ISO	*International Organization for Standardization*
KRI	Indicadores Chave de Risco
LDA	Modelo de distribuição de perdas
MCR	Requisito de Capital Mínimo
Oplnul	Coeficiente básico de risco operacional
ORSA	Autoavaliação do risco e da solvência
QIS	*Quantitative Impact Study*
RJASR	Regime Jurídico de Acesso e Exercício da Atividade Seguradora
ROCI	Risco Operacional e Controlo Interno
SCR	Requisito de Capital de Solvência
SCRop	Requisito de Capital de Solvência para o risco operacional
SGQ	Sistemas de Gestão de Qualidade
SOX	Sarbanes-Oxley
TI	Tecnologias de Informação
UE	União Europeia
Ulf	Coeficiente a aplicar ao montante das despesas anuais
VaR	Valor em Risco

1

INTRODUÇÃO

A presente dissertação foi baseada no estágio curricular realizado na Fidelidade, a maior companhia de seguros de Portugal, com presença em 4 continentes. O estágio teve uma duração de 5 meses, que permitiu adquirir conhecimentos sobre a importância do risco operacional e a forma como as empresas estão a direcionar-se para gerir e reduzir a sua exposição ao mesmo.

Este capítulo apresenta o tema da presente dissertação, abordando, em primeiro lugar, o enquadramento da temática em estudo, de seguida os objetivos, a metodologia aplicada e a estrutura do documento.

1.1 Enquadramento

Temos vindo a assistir, nas últimas décadas, a incontáveis falhas operacionais, desde fraudes, falhas de sistemas, erros nos procedimentos, que colocam em risco a sobrevivência de várias empresas e, em casos extremos, conduzem à falência de inúmeras organizações, provocando um colapso de mercado com consequências muito graves na estabilidade dos sistemas financeiros mundiais. Assim, regista-se de capital importância, tentar evitar estes eventos e os seus possíveis danos.

Para além disso, o crescimento do mercado, a tendência para uma maior dependência de novas tecnologias, o aumento da concorrência, o desenvolvimento de novos serviços de negócios para atrair clientes e a globalização têm contribuído para um aumento significativo da exposição dos sistemas financeiros internacionais ao risco operacional (Moosa, 2007). Portanto, o risco operacional tem-se tornado cada vez mais complexo, potencialmente mais devastador e cada vez mais complicado de prever e antecipar (van Grinsven & Bloemkolk, 2009).

O risco operacional é um risco que ultimamente tem vindo a ganhar cada vez mais importância nas instituições financeiras e seguradoras. É considerado como uma categoria que engloba tudo o que não for passível de se considerar como risco de crédito ou de mercado. No entanto, é possivelmente, o risco de avaliação mais difícil e subjetiva que enfrentam (Franzetti, 2016; Samad-Khan, 2008). O risco operacional costuma refletir-se em perdas, das quais umas sem valor para a empresa, outras mais significativas. É, pois, vital encontrar mecanismos capazes de controlar, mitigar ou alertar as consequências provenientes deste risco (Cruz *et al*., 2015).

O crescimento e desenvolvimento da gestão de risco potenciou a criação de regulação mais complexa para acompanhar as novas ferramentas e técnicas de gestão. No passado, cada país tinha a sua legislação nesta matéria e, por isso, os seus efeitos eram muito desiguais. Atualmente, a legislação é abrangente com impacto nos sistemas internacionais. À medida que a globalização aumentava, a necessidade de supervisão e regulação mais simétrica também se foi consolidando (Cruz *et al*., 2015).

Face a esta preocupação, a supervisão da União Europeia (UE) veio reestruturar e introduzir novos parâmetros, tais como focar-se mais na parte legislativa, para avaliar e resolver os problemas de solvência dos mercados europeus das seguradoras, representando um passo em frente neste setor e, por sua vez, estabelecer um regime estável, harmonioso e consistente com as novas realidades sociais e económicas (Bauer, 2012; Clipici, 2012; Istrate & Badea, 2017). Sendo assim, é possível proteger os *Stakeholders*, providenciando garantias de capital face aos riscos mais significativos e contribuir para um desenvolvimento sustentável nos mercados.

Solvência II é um regime com um conjunto atualizado de requisitos regulamentares para as seguradoras, pertencentes à União Europeia. O presente regime foi adaptado das regulações do Basileia II e a sua *framework* foi construída sob 3 pilares (EIOPA, 2020). No caso da banca e seguros, os respetivos regimes de solvência atribuem a gestão dos riscos, nomeadamente do risco operacional, ao critério de cada entidade. Com a atualização dos requisitos de Solvência, o risco operacional foi uma das principais novidades e passou a ser considerado nos processos de uma empresa e a ter peso na estrutura de uma empresa (Vukovic, 2015).

O perfil de risco, a introdução de práticas de gestão de risco operacional, sistemas de controlo interno eficazes e a sua inclusão na estrutura e com todos os colaboradores são parâmetros muito importantes a ter em consideração no sistema de governação, objetivos e estratégias estabelecidos por uma seguradora (Lavelle *et al*., 2010).

Em relação à *framework* implementada, é preciso fazer uma avaliação interna ou externa dos processos utilizados na gestão de risco, tais como a cultura de risco, responsabilidades, plano de negócio, potenciais novas atividades, questionários de avaliação de riscos e controlos, testes de stress, utilização de sistemas certificados e, por fim, documentar os processos.

É essencial reconhecer e definir as funções envolvidas na gestão de risco. Esta ação não é algo simples, porque a gestão envolve todos os níveis da companhia. Para isso, todos os níveis devem estar interligados e a cada nível o sistema deve integrar diferentes elementos: risco operacional, coordenação da tomada de riscos e supervisão da tomada de riscos (Dupont *et al*., 2012).

A gestão do risco operacional não é uma atividade fácil de desenvolver. A sua subjetividade, extensão, imprevisibilidade reflete-se em várias dificuldades e desafios com os quais os colaboradores e gestores têm de lidar diariamente. Por isso, é necessário apresentar respostas capazes de identificar, avaliar, monitorizar e melhorar continuamente os riscos operacionais que as várias unidades de negócio enfrentam. Só assim é que uma instituição financeira possui os meios para se fortalecer e desenvolver o seu valor.

1.2 Objetivos

Face ao crescimento dos mercados, as organizações financeiras estão a expor-se cada vez mais a possíveis perdas operacionais. Para garantir um desenvolvimento sustentável, as instituições financeiras, em especial as seguradoras, têm aumentado a sua preocupação em relação ao risco operacional e às suas possíveis consequências. Para tal, as empresas têm procurado desenvolver estratégias e práticas que implementem sistemas de governação adequados e, por sua vez, sistemas de gestão risco operacional eficazes, que estejam de acordo com a legislação em vigor.

O trabalho desenvolvido ao longo da dissertação tem os seguintes objetivos:

- Identificar o grau de cumprimento dos requisitos impostos pelo regime de Solvência II, na instituição sob análise;
- Sinalizar as dificuldades e desafios que uma seguradora enfrenta ao gerir risco operacional;
- Estabelecer as boas práticas de um sistema de gestão de risco operacional;
- Avaliar se a estratégia utilizada reduz a exposição ao risco da instituição.

1.3 Estrutura do documento

A presente dissertação está dividida em 6 etapas, esquematizadas na Figura 1.1.

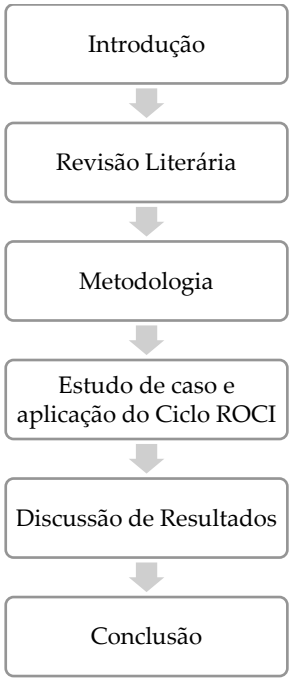


Figura 1.1 - Estrutura da dissertação

O capítulo 1 apresenta uma breve introdução ao problema em estudo e contextualização do tema, destacando a sua importância para as organizações financeiras. Inclui os objetivos do estudo, a descrição da metodologia adotada e a estrutura do documento.

No capítulo 2 realiza-se um estado de arte baseado na literatura existente sobre o risco operacional e a preocupação na implementação de sistemas de gestão adequados, de forma a não depender somente dos requisitos quantitativos estabelecidos pelo regime prudencial do setor segurador e da importância de apresentar um modelo de governação robusto capaz de suportar a gestão qualitativa do risco operacional.

O capítulo 3 consiste na fundamentação da aplicação da metodologia de estudo e apresentação das etapas do Ciclo ROCI, que ajudam a reduzir a exposição a risco.

No capítulo 4 descreve-se o estudo de caso da dissertação. Inicialmente, foi realizado um enquadramento da empresa Fidelidade, Companhia de Seguros Lda., que foi o ponto de partida para a realização deste documento. De seguida, explicou-se o problema que uma companhia de seguros enfrenta quando gere o risco operacional. Assim, segue-se para a análise dos dados recolhidos para efetuar uma gestão eficaz do risco, desde o sistema de governação, através da política de gestão e do modelo de governação até ao sistema de gestão

de risco operacional adotado pela empresa, que se desenvolve sob as atividades realizadas no Ciclo ROCI (Risco Operacional e Controlo Interno).

No capítulo 5, procede-se à análise dos resultados obtidos, onde se compara os dados recolhidos nos eventos perda com a avaliação prospetiva do risco.

No capítulo 6, são sintetizadas as principais conclusões do estudo, contribuições da investigação, limitações e trabalhos futuros.

2

REVISÃO DE LITERATURA

Neste capítulo é realizada uma revisão de literatura, onde é feito um enquadramento teórico sobre os conceitos abordados ao longo da dissertação.

2.1 Gestão de Risco

O risco é uma área relativamente recente que começou a ser estudada só depois da Segunda Guerra Mundial (Cruz *et al*., 2015). As definições de risco variam consoante aplicações específicas e determinados contextos. Tradicionalmente, o risco é considerado uma perda real ou potencial falha (Islam & Tedford, 2012).

O risco é a probabilidade/possibilidade de ocorrer algo adverso, ou seja, um acontecimento incerto, fortuito ou danoso. Atualmente, o seu conceito inclui uma quantificação e qualificação de incerteza, tanto no que diz respeito às "perdas" como aos "ganhos" em relação ao rumo dos acontecimentos esperados, por outras palavras, quanto maior a possibilidade de ganho ou perda, maior o risco envolvido (Assi, 2021; Islam & Tedford, 2012).

De acordo com o *Blackwell Encyclopedic Dictionary of Finance*, o risco é definido como exposição à mudança, sendo a probabilidade de algum evento futuro ou um conjunto de eventos ocorra. Portanto, a análise do risco envolve a identificação de mudanças potenciais adversas e do impacto esperado como resultado na organização (Assi, 2021).

O risco está presente nas atividades pessoais e profissionais, refletindo-se em perdas, bem como em oportunidades. No sentido de o evitar, são desenvolvidos e implementados mecanismos que evitam ou reduzem a sua ocorrência e/ou seu impacto.

O risco operacional é um risco, que ultimamente tem vindo a ganhar cada vez mais importância nas instituições financeiras e seguradoras. No entanto, é, possivelmente, o risco de avaliação mais difícil e subjetivo que as empresas enfrentam. A história demonstra que

inúmeras perdas significativas, que levam muitas vezes à insolvência de certas empresas, são reflexo de falhas operacionais (Franzetti, 2016; Samad-Khan, 2008).

Existe uma grande variedade de riscos com diversas características. Dessa forma, é necessário criar ferramentas capazes de responder aos diversos riscos. Na seleção das ferramentas, deve-se ter em consideração o custo, a eficiência e a eficácia. Exemplos de ferramentas:

- Prevenir perdas: Envolve a redução das responsabilidades de um evento, enquanto se reduz a magnitude da ocorrência de um evento indesejado.
- Tratamento do risco: envolve todas as atividades para controlar e reduzir o risco até a um nível aceitável.
- Tolerância ao risco: A exposição pode ser tolerável, não sendo necessário tomar mais ações, uma vez que pode ser opção e/ou a estratégia de negócio da empresa.

A importância deste conceito tem vindo a crescer ao longo das últimas décadas. As instituições financeiras deparam-se com inúmeros riscos ao tentarem atingir os seus objetivos. Por esta razão, começaram a surgir cada vez mais abordagens para fazer uma gestão eficaz dos riscos.

Inicialmente, as organizações procuravam fortalecer-se financeiramente para conseguirem suportar os impactos negativos de eventos incertos. Atualmente, a gestão de risco é aplicada quer para eventos negativos quer para oportunidades positivas. As instituições têm o objetivo de lucrar, mas para atingir tais lucros existem riscos que devem ser controlados (Oluwafemi, 2019).

No mundo empresarial, sempre existiu a necessidade de possuir sistemas de gestão de riscos. Mas só nas últimas décadas é que a definição de gestão de risco teve uma maior evolução e a sua relevância aumentada em diversos setores económicos, sendo uma área corporativa relativamente recente.

Independentemente do setor a ser considerado, existem semelhanças na gestão do risco. Trata-se de um conceito definido ao nível corporativo que se refere às contribuições compartilhadas entre todos os gestores de uma organização; preocupada com fatores de risco e está intimamente relacionada, mas não restrita, aos sistemas de gestão e supervisão. Exige um planeamento adequado, execução adequada e um sistema de monitorização contínuo. Deste modo, a gestão de riscos precisa de respostas proativas, bem como respostas reativas rápidas dos tomadores de decisão para diminuir a exposição ao risco (Islam & Tedford, 2012).

Committee of Sponsoring Organisations of the Treadway Commission considera a gestão de risco como um processo, afetado por um conselho de administração, direção e outros colaboradores das entidades, aplicado na definição de estratégia e por toda a empresa, com o objetivo de identificar potenciais eventos que possam afetar a entidade, e gerir o risco de acordo com o apetite de risco, de modo a fornecer garantias razoáveis sobre a realização dos objetivos da entidade (Williams *et al*., 2006).

A *European Foundation for Quality Management* (EFQA) define a gestão de risco como a utilização sistemática de processos em toda a organização para identificar, avaliar, gerir e monitorizar riscos, de forma que a informação agregada possa ser utilizada para proteger, libertar e criar valor (Williams *et al*., 2006).

O Comité de Basileia define a Gestão de Risco como um processo para Identificar, Avaliar, Monitorizar, e controlar ou mitigar todos os riscos materiais e avaliar a adequação geral do capital das entidades bancárias em relação ao seu perfil de risco (Franzetti, 2016).

2.1.1 Indústria

Primeiramente, é necessário dar relevância à gestão de risco na Manufatura. A produção é a base de qualquer economia nacional e, por conseguinte, deve ser alimentada a um elevado nível de padrão e maturidade, a fim de ser robusto, autossustentável e autossuficiente.

Atualmente, o setor industrial enfrenta muitos desafios devido à concorrência, à legislação, às normas internacionais, à globalização e às mudanças tecnológicas (Oduoza, 2020). Para além disso, é necessário um ambiente dinâmico de produção capaz de responder ao elevado consumismo.

Contudo, no setor industrial, é necessário ter consciência da ampla variedade de riscos inerentes à atividade. Uma gestão de risco proativa, especialmente no setor da engenharia, e um controlo das principais variáveis de risco podem evitar baixos desempenhos e, em casos mais extremos, a cessação de atividades (Oduoza, 2020).

A maioria dos riscos associados a fatores internos ou externos focam-se essencialmente em 3 categorias (Islam & Tedford, 2012):

- Risco operacional: risco associado a perdas diretas e/ou indiretas resultantes de falhas de sistemas ou equipamentos, processos de produção ou de pessoas.
- Risco ocupacional: risco associado à saúde e segurança dos empregados. Engloba os riscos que podem causar acidentes de trabalho, doenças profissionais ou danos físicos/psicológicos durante a realização da atividade laboral. A exposição a substâncias químicas perigosas, riscos ergonómicos, riscos de acidentes com máquinas e equipamentos, e exposição a níveis elevados de ruído são possíveis exemplos.

- Risco económico: risco associado com o desempenho de negócio e comercial, nomeadamente a flutuação do preço das matérias-primas, alterações em regulamentações, a existência de novos concorrentes.

O aumento da automação permite diminuir a quantidade de produtos defeituosos, ou seja, aumentar o controlo da qualidade, diminuindo erros operacionais, mas por outro lado, aumentar o risco relacionado com sistemas de informação (Oduoza, 2020).

A Indústria 4.0, também denominada de *Industrial Internet of Things*, tem permitido que haja uma maior incorporação de tecnologia capaz de aumentar a produção, melhorar a comunicação e monitorização, através de diagnósticos feitos a si próprio e aumento da análise entre equipamentos/máquinas e sistemas. No entanto, veio aumentar o risco de ataques de hackers, sendo necessário a implementação de uma *framework* de cibersegurança, capaz de mitigar este risco (Oduoza, 2020).

2.1.2 Serviços

Na década de 1950, surgem as primeiras ferramentas ou novas formas para gerir os riscos, uma vez que se tornava cada vez mais complicado suportar os custos de vários tipos de coberturas de seguros. Muitos riscos de negócios eram complicados ou muito caros para segurar. Entretanto, há o desenvolvimento do BCP (*Business Continuity Planning*), pondo-se em prática várias atividades e instrumentos de prevenção do risco (Cruz *et al*., 2015).

Nos anos 60, começa-se a oferecer os primeiros seguros de acidentes de trabalho (Dionne, 2013). Em 1963, ainda sem haver o conceito de gestão de risco presente, *Mehr e Hedges* afirmam que a gestão desses riscos é útil para a organização, bem como os princípios e técnicas adequados à gestão dos seguros (Cruz *et al*., 2015).

Nos anos 80, há uma espécie de revolução da gestão de risco, que tem o seu maior avanço através do uso de derivativas como instrumentos para gerir riscos financeiros. Até então, eram utilizados para comodidades e produtos agrícolas. Deve-se ao facto de haver um grande número de eventos macroeconómicos, que aconteceram nesta década, tais como o desaparecimento das paridades de moedas fixas, o preço das comodidades torna-se muito volátil, bem como as flutuações do preço de muitos ativos financeiros. Assim, é imprescindível a gestão destes riscos financeiros para a tomada de decisões, tornando-se uma prioridade para a maioria das empresas (Cruz *et al*., 2015; Dionne, 2013).

É importante salientar que a regulamentação internacional do risco surge nesta altura. As instituições financeiras começaram a desenvolver modelos internos de gestão de risco e

aplicar fórmulas para calcular o capital para se protegerem de riscos inesperados ou reduzir o capital regulatório. A governação torna-se essencial para uma organização e integra-se a gestão de risco na sua estrutura e estratégia. Por fim, para colmatar esta "revolução" surge a posição *Chief Risk Manager* (CRO) (Dionne, 2013).

Entretanto, é apresentada uma definição mais próxima da atual, que segundo *Bannister e Bawcutt*, gestão de risco é a identificação, medição e controlo económico dos riscos que ameaçam os ativos e ganhos de um negócio ou empresa. Na mesma altura, *Crockford* sugere que se englobe, principalmente, aquelas atividades desempenhadas para prevenir perdas acidentais (Cruz *et al*., 2015).

Na década de 90, surge a gestão de risco operacional e de liquidez (Dionne, 2013). A missão de gestão de riscos operacionais consiste em identificar, analisar e mitigar as diferentes operações de risco a que estão expostas as inúmeras atividades comerciais, nas quais podemos identificar duas partes principais que podem ser encontradas nas organizações: a existência e integridade da gestão e controlos operacionais da empresa, com cenários culturais adequados para satisfazer a legislação em vigor em matéria de segurança no emprego, dados, ambiente e outros, e para prevenir a fraude; a capacidade de cumprir a promessa feita aos clientes, fazendo as atividades e processos necessários para servir os clientes e reunir-se com outras partes interessadas, incluindo acionistas, colaboradores ou fornecedores (Epetimehin, 2013).

2.1.3 Gestão da Qualidade

A gestão da qualidade é uma filosofia que consiste em princípios, práticas e ferramentas que incluem práticas e valor, tais como serviço ao cliente, melhoria contínua e decisões baseadas em factos (Siva *et al*., 2016). Com ela as organizações pretendem satisfazer as necessidades, expectativas dos seus clientes, por outras palavras, dependem das funções e desempenho dos seus produtos e serviços para reter mercado e clientes e, dessa forma, atingir os seus objetivos (Hoyle, 2007; Wicher *et al*., 2018).

O conceito atual e as práticas de qualidade surgem da contribuição e adaptação das filosofias dos seguintes autores (Wicher *et al*., 2018):

- W. Edwards Deming desenvolveu conjunto de 14 princípios e adotou o ciclo PDCA para melhorar a qualidade e a eficiência dos processos;
- Joseph M. Juran desenvolveu a lei de Pareto, onde menciona que 80% dos problemas são derivados de 20% das causas;
- Armand Feigenbaum usou uma abordagem mais abrangente, o controlo total da qualidade, que defende que a qualidade não é só responsabilidade do departamento de qualidade, é da organização;

- Philip Crosby estabeleceu um sistema para alcançar melhores níveis de qualidade deveria ser principalmente preventivo e, assim, estabeleceu o zero defeito como uma direção a seguir;
- Kaoru Ishikawa desenvolveu o diagrama de *Ishikawa* que permite identificar as possíveis causas de um problema específico. Acreditava que a qualidade é responsabilidade de toda a organização.
- Genichi Taguchi desenvolveu métodos robustos de design para melhorar a qualidade de produtos e processos através da experimentação (Wicher *et al*., 2018).

Qualidade é determinada pela medida em que um produto ou serviço serve com sucesso as finalidades do utilizador durante a utilização (e não apenas no ponto de venda), ou seja, o impacto da qualidade é sustentado muito tempo depois da atração ou das dificuldades impostas pelo preço e entrega terem diminuído (Hoyle, 2007).

Assim, a integração a gestão da qualidade, bem como a gestão de risco, nomeadamente o operacional, torna sustentável o desenvolvimento das organizações, uma vez que atrai negócios, através da criação de valor.

A experiência e a especialização da gestão da qualidade podem refletir-se numa gestão de risco mais eficaz (Williams *et al*., 2006). Há 3 maneiras:

- Distinção entre quais riscos podem ou não ser tratados estatisticamente;
- A partir do conhecimento e experiência em gerir processos fundamentais;
- Implementação de grandes mudanças organizacionais e culturais;

Para mostrarem o valor e garantir qualidade, as empresas podem adquirir certificações de qualidade, que estão de acordo com normas, padrões internacionais. As normas da série ISO *(International Organization for Standardization)* 9000 foram lançadas pela primeira vez em 1987 e, desde então, têm existido atualizações da ISO 9000. Atualmente, as empresas para garantirem a sua qualidade focam-se na última versão denominada de ISO 9001:2015. Esta última versão pretende refletir as práticas empresariais modernas, mudanças do ambiente de negócios e tecnologia; manter abordagem por processos; incorporar mudanças nas práticas de SGQ (sistemas de Gestão da qualidade); proporcionar maior ênfase na obtenção de conformidade do produto; melhorar a compatibilidade com outras normas de sistemas de gestão, nomeadamente gestão de risco (Wicher *et al*., 2018).

2.1.4 Sistemas de Gestão de Risco

Alguns fatores importantes, bem como pressupostos foram identificados na elaboração de diferentes abordagens de gestão de risco, que permitem desenvolver uma *framework* comum de gestão de risco: a participação e contribuição de todos os elementos, pode exigir uma mudança da cultura de risco; a avaliação contínua do desempenho da gestão, dos funcionários e do próprio sistema, que deve ser integrada com estratégias empresariais; ferramentas e técnicas de avaliação de riscos precisam ser propositadas e específicas; mudanças no ambiente de trabalho (interna e externa) que precisam de ser continuamente monitorizadas e ajustadas dentro da estratégia de gestão de riscos; é necessário providenciar formações aos colaboradores (Islam & Tedford, 2012).

Para além do mencionado anteriormente, uma *framework* baseia-se nos seguintes pressupostos:

- Os riscos são parte inerente das operações do negócio e que não é possível eliminá-los completamente;
- Os riscos estão em constante alteração e evolução, por isso, a sua gestão é um processo contínuo que precisa de ser continuamente revisto e atualizado;
- A gestão de risco é uma parte integral da estratégia da empresa e devia estar alinhada com os seus objetivos.
- A gestão do risco deve ser um processo sistemático e estruturado, e não uma abordagem reativa.
- A gestão do risco deve basear-se em dados e provas, em vez de pressupostos ou suposições.
- A gestão de risco é uma responsabilidade partilhada e que todos os trabalhadores têm um papel a desempenhar na identificação, avaliação e mitigação dos riscos.
- O custo da gestão do risco deve ser proporcional ao impacto potencial do risco, e que os recursos devem ser concentrados nos riscos mais críticos.
- A gestão dos riscos deve ser transparente e comunicada eficazmente a todas as partes interessadas.

Uma *framework* é composta, tipicamente, pelos seguintes elementos (KPMG, 2017):

- Identificação: Envolve identificar todas as fontes potenciais de risco. Inclui a identificação de riscos novos e emergentes.
- Avaliação: Análise e avaliação dos riscos identificados, bem como a avaliação da probabilidade e do impacto desses riscos. Priorizar riscos e determinar os que requerem mais atenção.

- Controlo: Implementação de medidas para controlar ou mitigar os riscos identificados. Inclui implementação de novas políticas e procedimentos e de tecnologias ou o reforço dos controlos existentes.
- Monitorização: Monitorização e revisão contínua do processo de gestão dos riscos. Isto inclui a monitorização da eficácia dos controlos postos em prática e a identificação de quaisquer riscos novos ou emergentes.
- Governação: Estabelecimento de uma estrutura de governação que é concebida para identificar, avaliar e gerir riscos operacionais. Inclui estabelecer linhas claras de responsabilidade e responsabilização pela gestão dos riscos e assegurar que o processo de gestão dos riscos esteja alinhado com a estratégia e objetivos globais da organização.
- Reporte: Comunicação regular de riscos operacionais à direção e ao conselho de administração, bem como aos organismos reguladores relevantes, quando necessário. Assim, permite à direção de alto nível tomar decisões informadas sobre a gestão de riscos e tomar as medidas apropriadas quando necessário.

Em suma, estes pilares estão interligados e devem ser integrados e coordenados para formar uma *framework* robusta de gestão do risco.

Atualmente, os sistemas de gestão de risco apresentam as seguintes etapas como se verifica na Figura 2.1 (Oduoza, 2020):

- Estabelecer o contexto do risco e a potencial exposição ao perigo;
- Avaliação do risco, onde envolve a identificação, análise e avaliação. Esta etapa permite estabelecer onde estão as maiores vulnerabilidades e onde está a probabilidade de falha;
- Tratamento do risco: reduzir, evitar, transferir, atenuar, reter o risco ou se for uma oportunidade para explorar, partilhar, realçar ou ignorá-lo;
- Monitorizar e rever:
- Comunicar e consultar;

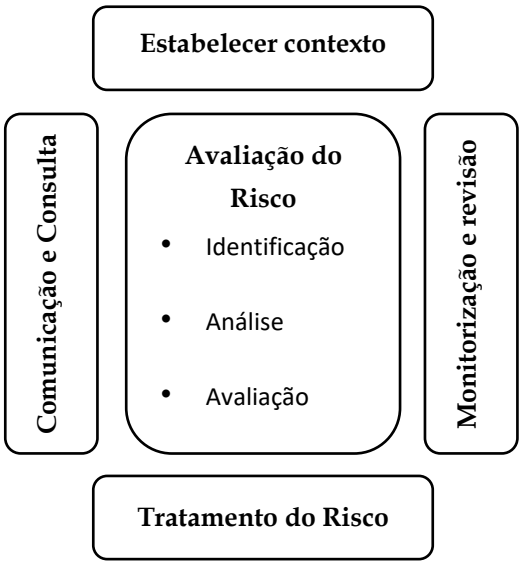


Figura 2.1 - Sistema de Gestão de Risco adaptado de (Oduoza, 2020)

O crescimento e desenvolvimento da gestão de risco potenciou a criação de regulação mais complexa para acompanhar as novas ferramentas e técnicas de gestão. Tal regulação é transversal a mais do que um país, isto é, anteriormente cada país tinha a sua legislação, que era muito desigual. À medida que a globalização aumentava, a necessidade de supervisão e regulação mais simétrica tornou-se mais premente (Cruz *et al*., 2015).

Dada a evolução da gestão de risco e dos seus conceitos, foi necessário criar regulamentação para que as instituições financeiras pudessem gerir o seu negócio em conformidade. Portanto, surgiu o regime Basileia, o regime de Solvência, o COSO (*Committee of Sponsoring Organizations)*, a ISO 31000, Cobit (*Control Objectives for Information and related Technology)*, entre outras.

A ISO 31000 é uma norma internacional de gestão de riscos que fornece diretrizes e princípios gerais para ajudar as organizações a identificar, avaliar e dar prioridade aos riscos, e a implementar medidas para mitigar esses riscos. A norma foi concebida para ajudar as organizações a compreender e gerir o risco de uma forma estruturada e sistemática (ISO, 2018).

A norma destina-se a ser utilizada em conjunto com outras normas de gestão, tais como ISO 9001 (gestão da qualidade) e ISO 14001 (gestão ambiental). Destina-se também a ser compatível com outros quadros de gestão de riscos, tais como o COSO ERM (*Enterprise Risk Management Framework*).

Basileia III é um quadro regulamentar internacional para bancos e outras instituições financeiras, que inclui requisitos para a gestão do risco operacional. Visa reforçar a capacidade dos bancos de resistir a choques causados por stress financeiro e económico. Também exige que os bancos detenham reservas de capital e liquidez para garantir que se mantenham

estáveis durante períodos de stress. A *framework* de Basileia III para a gestão do risco operacional inclui uma série de requisitos, tais como o desenvolvimento de um quadro para a identificação, avaliação e gestão dos riscos operacionais. Exige também que os bancos informem regularmente as autoridades de supervisão sobre os seus riscos operacionais e processos de gestão do risco. Algumas companhias de seguros utilizam Basileia III como referência para os seus quadros de gestão do risco operacional (Banco de Portugal, 2023).

COBIT (*Control Objectives for Information and related Technology*) é uma *framework* para a gestão do risco e da governação de Tecnologias de Informação (TI), publicada pela *IT Governance Institute of the Information Systems Audit and Control Association*, capaz de responder ao crescimento e aumento deste tipo de riscos, que são cada vez mais frequentes e presentes no quotidiano de cada um. COBIT fornece uma visão holística da gestão e governação de TI e cobre uma vasta gama de áreas, incluindo estratégia, arquitetura, desenvolvimento, operações e segurança de TI. É amplamente utilizado por organizações em várias indústrias para gerir os seus riscos e governação de TI de forma eficaz e eficiente (Amorim *et al*., 2021; Mangalaraj *et al*., 2014).

2.2 Risco Operacional

O risco operacional é tão antigo como o negócio. Cada indústria, cada atividade é confrontada com o risco operacional. A palavra operacional é equivalente a fazer, trabalhar e realizar, por esta razão, este risco está subjacente a todas as atividades (Franzetti, 2016).

Contudo, o risco operacional é o ramo mais novo dos três riscos mais importantes, sendo os outros riscos de crédito e risco de mercado (Cruz *et al*., 2015).

A atual definição de Risco Operacional é (Parlamento Europeu e do Conselho, 2009):

> O risco operacional é definido como "o risco de perdas resultantes de procedimentos internos inadequados ou deficientes, do pessoal ou dos sistemas, ou ainda de acontecimentos externos", desde ataques cibernéticos a falhas de prestadores subcontratados, fraudes e desastres naturais, que inclui os riscos de caráter jurídico (legal), mas exclui os riscos resultantes de decisões estratégicas e os riscos reputacionais.

Ao longo da história, existem registo de vários acontecimentos associados ao risco operacional. Os primeiros registos de fraudes de manipulação de títulos, que remetem para práticas grosseiras do risco operacional, têm origem na "*Dutch tulip Mania*" em 1636/37, na Holanda. Em 1717, há o exemplo do escândalo da *Mississipi Company,* em França. Pouco tempo depois, em 1720, há o escândalo da *South Sea Bubble* em Inglaterra (Toms, 2019).

Na década de 1920, ocorre a grande queda de Wall Street, nos Estados Unidos. Esta queda deve-se ao facto de os auditores não terem sido capazes de detetar fraudes. Os fraudulentos usavam estruturas de negócio complexas para esconder passivo e alterar valores da sua folha de contas. A ineficiência em verificar a legalidade dos negócios extremamente complexos e de elevada dimensão implicou numa enorme crise nos Estados Unidos (Toms, 2019).

Na Figura 2.2, é possível verificar os vários escândalos que aconteceram nas últimas décadas e, posteriormente entender as causas de alguns exemplos mais importantes e significativos que abriram precedentes no sistema financeiro e na preocupação do risco operacional.

- *Maxwell Bank*: Em 1991, Robert Maxwell desviou fundos de pensões, providenciou ativos como garantia para empréstimos adicionais, desviou ações e dinheiro de uma companhia para outras em seu controlo para dar falso lucros e comprometeu essas ações como garantia para mais empréstimos às suas empresas privadas (Abid & Ahmed, 2014).
- *Baring Bank*: Nick Leeson era um *trader* fez investimentos sem autorização no mercado asiático, com pouca supervisão superior. Resultando no colapso de um banco inglês com mais de 200 anos de história, dado que as negociações se mantiveram fora do radar da gestão (Chen, 2022; Cruz *et al*., 2015).
- Enron: Em 2001, Enron entrou em falência e admitiu irregularidades no reporte financeiro entre 1997 e 2000, onde utilizaram lacunas contabilísticas, entidades com fins especiais e relatórios financeiros deficientes para esconder a dívida do seu balanço (Abid & Ahmed, 2014).
- WorldCom: Um ano após a queda da Enron, a empresa de telecomunicações americana também tem o mesmo desfecho que a Enron. Descobriu-se que tinha inflacionado os seus ativos cerca de 11 biliões de dólares. A fraude foi descoberta quando se fez uma auditoria interna e se descobriu se cerca de 3.8 biliões de dólares em contas fraudulentas (Corporate Finance Institute, 2022; Hail & Wang, 2017).
- Parmalat: A fraude de Parmalat foi descoberta em 2003, quando a Parmalat entrou em falência numa emissão obrigacionista de 150 milhões de euros, apesar

de ter reportado mais de 4 mil milhões de euros em capital e equivalentes no seu balanço de contas (Rimkus, 2016).

- *Lehman Brothers*: *Lehman Brothers* era um dos maiores bancos de investimentos nos Estados Unidos, sediado em Nova Iorque. Em 2008, o banco entra em falência devido à elevada exposição ao risco que o banco, agravando a crise financeira de 2008 (Corporate Finance Institute, 2022)

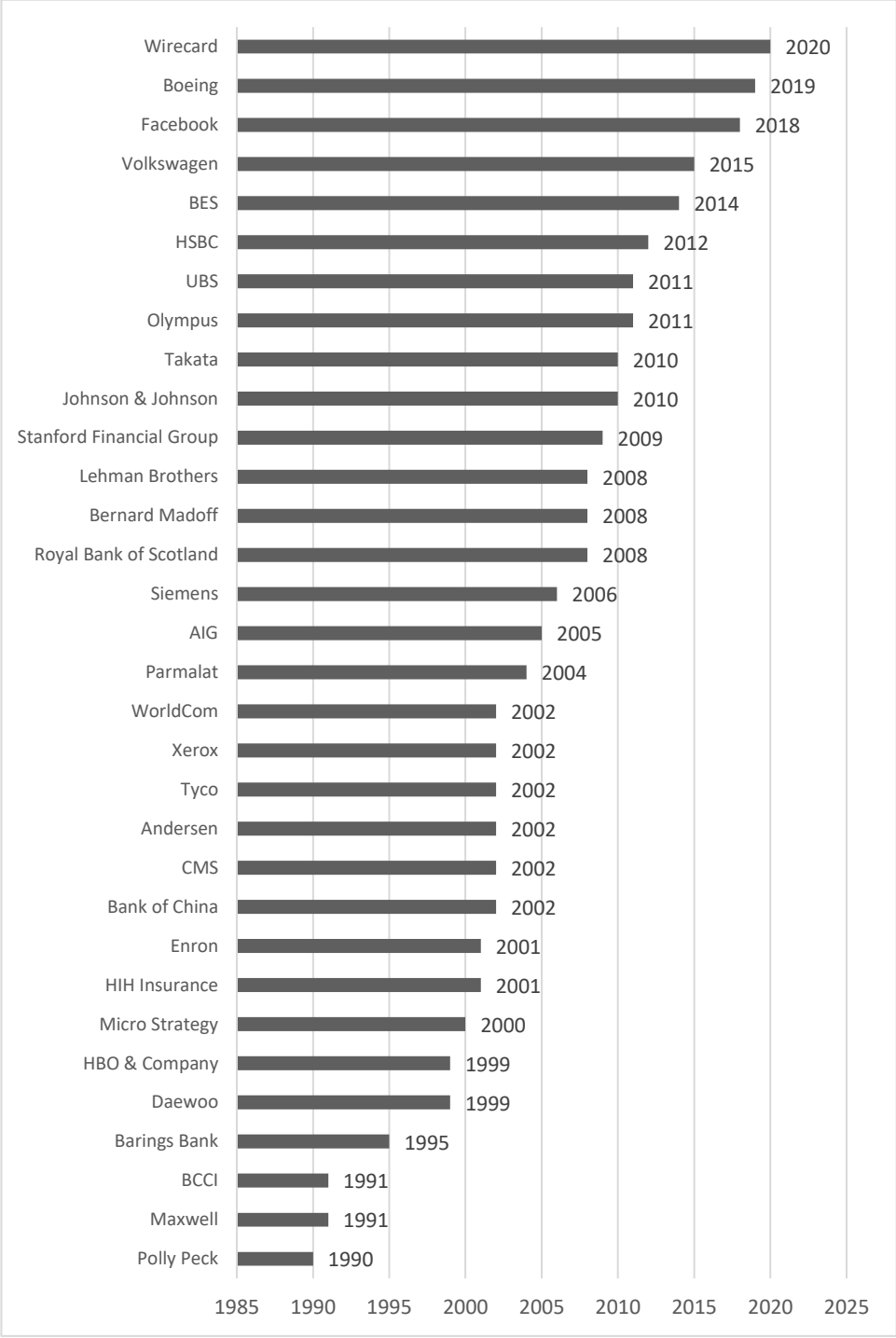


Figura 2.2 - Escândalos financeiros causados por perdas operacionais nas últimas 3 décadas adaptado de (Abid & Ahmed, 2014)

- BES (Banco Espírito Santo): Em 2014, ocorre a implosão do BES. Segundo uma auditoria externa solicitada pelo Banco de Portugal, identificaram-se irregularidades nas contas, onde o grupo omite cerca de 1,2 mil milhões de euros

do passivo. Deste modo, o Governo e o Banco de Portugal decidem dividir o BES em 2, o bom (Novo Banco) e o mau (BES), onde se declara falência do BES (Madeira, 2014; Oliveira *et al*., 2020).

Os escândalos acima são exemplos de má governação corporativa, que resultam em conspirações, gestão de risco ineficaz, de controlos internos inadequados e incapazes de detetar fraudes internas, arquivamento de documentos falsos.

Para além dos escândalos mencionados, existiram outros inúmeros casos, que forçaram as empresas a criar e a melhorar os seus sistemas de gestão de risco operacional, de modo a evitarem futuras insolvências, bem como atingir os seus objetivos estratégicos (Abid & Ahmed, 2014). Outras indústrias também mostraram elevadas perdas operacionais. A BP apresentou falhas operacionais muito críticas, levando ao derramamento de petróleo ao longo do Golfo do México. Na Indústria automóvel, a *Toyota e GM* não conseguiam corresponder às expectativas de segurança dos seus veículos (Walker, 2022). Devido à dimensão de alguns escândalos, originaram-se legislação/normas que forçassem as empresas a serem mais transparentes e que, deste modo, não deixar as empresas chegarem a um cenário mais extremo, como por exemplo, a impossibilidade de evitar a insolvência, devida à falta de mecanismos e processos adequados.

O termo Risco Operacional começa a ser mais usado e a ganhar mais visibilidade no caso *Barings*, em 1991. Na altura do *Barings*, a Indústria utilizava o termo risco operacional para situações onde havia a possibilidade de surgirem perdas. E como o que havia acontecido não era nem risco de mercado nem de crédito, aplicou-se a definição dada pelo Setor. Apesar de não ser considerada uma definição perfeita ou mais próxima da definição atual, ainda levou algum tempo até ser abandonada e a se propor uma definição mais adequada face à realidade (Cruz *et al*., 2015).

Considerar o risco operacional como tudo aquilo que não é crédito ou mercado, tornava a sua gestão ainda mais complicada. Em 1982, *Crockford* comenta que a pesquisa para a gestão de risco deparou-se logo com problemas iniciais de definição. Não se conhece muito bem as suas fronteiras e, por isso, era notório a falta de capacidade para formular uma definição (Cruz *et al*., 2015).

Em 1991, o *Committee of Sponsoring Organizations* (COSO) denominou o risco operacional como um conceito genérico. Os riscos desse caráter foram meramente classificados como "riscos de operações". Com o decorrer da década de 90, este conceito foi sendo trabalhado e generalizado, tendo, ao longo dos anos, surgido cada vez mais na literatura e até o surgimento

de novos cargos de trabalho, como é exemplo o cargo de gestor de risco operacional (Varela, 2016).

A *framework* do COSO é a estrutura subjacente que suporta os principais conceitos usados por todas as atividades envolvidas na gestão de risco, tais como: estratégia de risco, apetite de risco, perfil de risco, a sua medição, relatórios de exposição e muitos outros. O principal objetivo é fornecer uma forma de integrar a informação do risco nos processos estratégicos e de decisão da empresa. Deste modo, é possível para as organizações gerir os seus desempenhos, tendo em conta a quantidade de risco necessário para o atingir (Dupont *et al*., 2012).

A gestão de risco é vista como um processo operacional baseado em COSO II, providenciando decisores (gestores e diretores) com uma garantia razoável capazes de gerir os riscos tolerados na aplicação de objetivos estratégicos e dentro dos limites do apetite de risco. Sendo assim, permite gerir a incerteza, riscos e oportunidades e identificar eventos que podem vir a tornar-se riscos, bem como implementar sistemas de controlo interno (Dupont *et al*., 2012).

O desenvolvimento deste risco ao longo dos anos, veio salientar: que existem inúmeros riscos de caráter operacional e que têm vindo a aumentar nos últimos anos; a gestão de risco operacional deve ser vista como uma disciplina própria e não como algo secundário e inerente a outros riscos, como o risco de crédito ou de mercado; a importância da inclusão do risco operacional em qualquer sistema de gestão de riscos; o reconhecimento que este risco já merecia nas instituições financeiras e que com o avanço tecnológico era necessário a regulamentação do risco operacional. Para este efeito, as organizações colocam a responsabilidade de gerir o risco operacional a gestores nas unidades de negócio, sendo necessário desenvolver os sistemas e infraestruturas para as melhores práticas (Dupont *et al*., 2012; Torre-Enciso & Barros, 2012).

O risco operacional costuma refletir-se em eventos de perda, ou seja, a característica mais importante da definição é focar-se no impacto das perdas operacionais. Na Tabela 2.1, pode ser verificado as categorias do risco operacional e suas principais exposições:

Tabela 2.1 - Categorias Risco Operacional adaptado de (Vilas, 2015)

Categorias	**Descrição**
Risco de Pessoas	Possui vários compartimentos, tais como erros, acidentes, manipulação de mercados, ações legais, evasão de impostos, organizações de trabalho impróprias, etc.

Categorias	Descrição
Risco de Processos	Envolve ineficiência e falta de eficácia quando se realizam atividades e operações de negócio que podem incorrer em perdas. Ex.: Erros de cálculo, omissões, valores errados. Daí a importância de as organizações financeiras terem ativamente equipas a controlar transações.
Risco de Sistema	A tecnologia de informação tem as duas faces de uma moeda, tanto é boa como é má. As maiores perdas são causadas pelo *hacking, phishing*, vírus de computador, etc. É aconselhável às empresas regularem internamente os sistemas e investirem em IT.
Riscos Externos	São causados por eventos externos, não só por fatores económicos, fatores políticos e legais, mas também por fatores naturais, tais como desastres (incêndios, terramotos, etc.), que estão para lá do alcance da companhia.
Fraudes	As Fraudes podem ser divididas em fraudes internas e fraudes externas. Fraudes internas constituem as perdas incorridas devido a atos intencionais ou inapropriados realizados por colaboradores, que envolvem quebrar a lei, regulações ou políticas organizacionais. Fraudes externas constituem perdas relacionadas com o uso inapropriado de propriedade e fugas de informação.

O risco operacional é um risco diferente de todos os outros. A sua natureza peculiar revela uma dependência entre o risco operacional e os outros riscos, ou seja, o risco operacional condiciona os outros riscos, sobrepondo-se e agravando todos os outros tipos de riscos (Samad-Khan, 2008).

No entanto, a dependência não é bidirecional, uma vez que riscos como o de mercado, crédito, contraparte podem despoletar perdas operacionais, o inverso não acontece, as perdas operacionais não podem aumentar a exposição dos outros riscos (Kelliher *et al*., 2020). Na

ausência de problemas operacionais, os outros riscos são mais inofensivos (Samad-Khan, 2008).

Se uma instituição não achar interessante um investimento que tenha feito, ou acha que está muito exposta a uma determinada ação com um *rating* crítico, pode, simplesmente, reduzir a sua exposição por retirar o investimento. Por outro lado, se for detetada uma falha de sistema no momento da retirada do investimento, pode haver consequências graves para a instituição financeira.

2.2.1 Legislação

Derivado de vários escândalos e crises, a preocupação em controlar o risco operacional tem aumentado, pois tem consequências muito severas. 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).

As instituições financeiras tinham presente certos riscos, mas não sabiam a que categoria deveriam ser atribuídos, tendo como exemplo: o perigo ou incerteza, provenientes da imperfeição da tecnologia de informação e das infraestruturas da época, a fraude, as interrupções de negócio, etc. Com o surgimento da categoria Risco Operacional, estes riscos, até então não classificados, foram finalmente classificados (Varela, 2016).

As autoridades públicas internacionais têm vindo a implementar uma vasta quantidade de leis e regulamentos para prevenir a economia e, especialmente, o setor financeiro de sofrerem perdas operacionais no futuro, ou em casos mais extremos, colapsos financeiros como a crise de 2008 (Bauer, 2012).

A Figura 2.3 mostra as várias regulações que foram sendo implementadas ao longo do tempo, porque a gestão do risco operacional tem-se tornado cada vez mais desafiante e, cada vez mais importante, para evitar futuras insolvências como aconteceu a inúmeras empresas. A própria regulação do capital constitui uma proteção para a atividade que os clientes estabelecem com as seguradoras e as instituições financeiras. Como se pode verificar, houve um desenvolvimento significativo desta área nas últimas 2 décadas (Bauer, 2012).

Figura 2.3 - Legislação Risco Operacional adaptado de (Bauer, 2012)

No início do milénio, devido aos escândalos da *Enron, Tyco e Worldcom*, o governo americano introduziu o ato de *Sarbanes-Oxley* (SOX). O ato de *Sarbanes-Oxley* é obrigatório para todas as empresas listadas na bolsa de valores dos EUA, que fortaleceu os requisitos de reporte financeiro e a governação corporativa, tais como mecanismos de controlo interno e responsabilidades do auditor externo e introduziu sanções para atividades ilegais, como corrupção, fraude corporativa (Bauer, 2012; Hail & Wang, 2017).

Em 2001, O Comité de Basileia de Supervisão Bancária (CBSB) apresentou uma definição para este risco: "o risco de perda resultante de processos internos, pessoas e sistemas inadequados ou falhados, ou de eventos externos desfavoráveis" (Banco de Portugal, 2023).

A atribuição tardia de uma definição para este risco justifica-se muito à sua complexidade e, por muito tempo, ser considerado uma categoria residual de outros riscos. A complexidade do risco operacional torna difícil a sua medição, avaliação e quantificação, criando dificuldades na sua gestão, dado que está presente em todas as atividades, serviços e produtos de uma instituição. Nem sempre a mitigação/eliminação é tão simples como a de outros riscos (Varela, 2016).

A dificuldade sentida pelas instituições na complexidade e medição dos riscos conduziu à criação do Acordo Basileia II, que deu a importância devida ao risco operacional, ao longo da reformulação da regulação bancária (Varela, 2016). Em 2006, o Basileia II foi publicado pelo Comité de Basileia de Supervisão Bancária, através das Diretivas 2006/48/CE e 2006/49/CE. Desde 2007, é obrigatório para todos os bancos que possuem serviços

financeiros na União Europeia estarem em conformidade com a nova regulamentação. Este regime estabelece requisitos mínimos de capitais para bancos e introduz a famosa abordagem de três pilares, que para além das novas condições de capitais (Pilar I), prevendo a determinação de requisitos de capitais para risco operacional, introduz o pilar II e III, com novos procedimentos de supervisão e exigiu divulgação para garantir disciplina de mercado efetiva e transparência (Banco de Portugal, 2023; Bauer, 2012; Bryce *et al*., 2016).

Este acordo permitiu que fossem atribuídos determinados níveis de controlo ao risco, ou seja, as medidas de risco operacional que devem ser implementadas, de modo a ser possível a sua medição e quantificação, proporcionando uma gestão mais eficaz (Varela, 2016). A ligação existente entre o risco operacional e os requisitos mínimos de capital é um motivo para qual os bancos estão interessados na redução, transferência ou eliminação de riscos operacionais (Bauer, 2012).

Esta nova abordagem introduz o risco operacional como uma área autónoma das organizações que, pela primeira vez, teve de se mensurar, gerir e alocar capital aos riscos operacionais calculados (Bryce *et al*., 2016).

À semelhança da banca, a indústria seguradora também fez uma reestruturação das regulações, introduzindo o regime de Solvência II (Bryce *et al*., 2016). Esta diretiva também tem o intuito de incluir o risco operacional para determinar o requisito de capital de solvência (Bauer, 2012).

2.2.2 Regime prudencial do mercado segurador e ressegurador

O mercado segurador é um dos setores com mais peso no setor financeiro. A sua atividade baseia-se, de forma simplificada, no seguinte: é uma forma de gerir o risco. Um tomador de seguro adquire proteção contra perdas financeiras inesperadas em troca de prémios (pagamentos mensais). As apólices de seguros são utilizadas para cobrir o risco de perdas financeiras, grandes e/ou pequenas, que podem resultar de danos ao segurado ou à sua propriedade, ou da responsabilidade por danos ou prejuízos causados a terceiros (Kagan, 2023).

Os vários tipos de seguros estão divididos em 2 grandes ramos (Franca, 2015):

- Os Seguros Não Vida englobam todos os seguros que têm bens patrimoniais, objetos e seguros pessoais;
- Os seguros Vida engloba seguros de vida tradicionais (em caso de morte) associados à vida humana e seguros de capitais que incluem produtos de capitalização e aforro.

As principais operações elaboradas pelas companhias de seguros prendem-se quer com a subscrição de contratos de seguro quer com a obrigação de regularizar os sinistros ocorridos relativos a esses mesmos contratos, durante o período de vigência destes (Lages, 2010).

O primeiro regime a vigorar nas seguradoras foi a Solvência I, que entrou em vigor em 1973 (Clipici, 2012; Istrate & Badea, 2017). Esta diretiva à imagem do Basileia I (regime prudencial para o setor bancário), focava-se, essencialmente, na quantificação financeira. Considerado como um modelo flexível, simples e objetivo, apresentava lacunas, tais como: o caráter estático e inexistência de uma ponderação dos riscos assumidos, ignorando o perfil de risco da empresa, a gestão de risco não era vista como algo indispensável e, por fim, a falta de regras de supervisão e de transparência (Lages, 2010).

A volatilidade dos mercados financeiros e o aumento da dinâmica dos negócios eram uma grande ameaça para a segurança financeira das seguradoras e um dos problemas mais estritos que a solvência das empresas enfrenta. Apesar desses problemas continuarem a ser os mesmos (deficiências relacionadas com a subscrição, investimento e atividade de resseguro), a sua frequência e severidade vinha a aumentar. Deste modo, este regime apresentava inúmeras fragilidades na parte de governação (Clipici, 2012; Istrate & Badea, 2017).

Face a esta preocupação, a supervisão da UE veio introduzir novos parâmetros, tais como focar-se mais na parte legislativa, para avaliar e resolver os problemas de solvência dos mercados europeus das seguradoras, representando um passo em frente neste setor e, por sua vez, estabelecer um regime estável, harmonioso e consistente com as novas realidades sociais e económicas. Com o desenvolvimento da regulação da banca, as seguradoras utilizaram essas ideias para reestruturar o seu regime. Assim, a Comissão Europeia (CE) começa a rever o regime de solvência, em 2001 (Bauer, 2012; Clipici, 2012; Istrate & Badea, 2017).

Este projeto durou, aproximadamente, 15 anos até, finalmente, entrar em vigor, em 2016. Para apoiar este projeto, a Comissão Europeia criou instituições e estruturas de apoio e de supervisão. A principal entidade criada foi a CEIOPS (*Committee of European Insurance and Occupational Pensions Supervisors*), em que esteve a desenvolver e testar este processo entre 2003 e 2010 (Istrate & Badea, 2017). Entretanto, em 2011, a CEIOPS foi substituída pela EIOPA (*European Insurance and Occupational Pension Authority*) com o objetivo de restruturar a supervisão financeira europeia, devido à crise financeira (Istrate, 2017).

Em 2003, o Grupo de trabalho publica os "relatórios de controlo interno para companhias de seguro", em que se pretende estabelecer princípios na implementação ou avaliação dos sistemas de controlo interno (Istrate & Badea, 2017). Em 2004/05, a Comissão Europeia consultou a CEIOPS para o desenvolvimento do regime para companhias que

pratiquem vida e não-vida. Entre 2006 e 2011, a CEIOPS, sendo a autoridade responsável pela gestão deste processo, conduz uma série de testes e análises em seguradoras europeias, sendo divulgados nos relatórios de estudo de impacto quantitativo (QIS) (Istrate, 2017).

- QIS 1 - Relatório divulgado a 17 de março de 2006 relativo à informação do final do ano financeiro de 2004. Conta com a intervenção de 314 companhias de seguro e resseguro. Este estudo estava focado na implementação preliminar da diretiva, estando, principalmente, focada em obrigações Não-Vida, tais como provisões técnicas e no método de avaliação da melhor estimativa. A principal conclusão deste estudo foi que as melhores provisões técnicas estimadas eram inferiores aos níveis registados. Para além disso, havia informação insuficiente para o tratamento da dificuldade das margens de risco, risco financeiro e contabilização dos tratados de resseguro.
- QIS 2 - Divulgado a 26 de outubro de 2006, 514 empresas de 19 países europeus, que representavam cerca de 50% do mercado, participaram neste estudo. O principal objetivo foi a determinação do Requisito de Capital de Solvência (SCR), através da fórmula standard. Os resultados mostram que as provisões técnicas diminuíram, enquanto o capital necessário e o capital disponível aumentaram.
- QIS 3 - Realizado em novembro de 2007, com uma participação de 1027 companhias provenientes de 28 países europeus. Este estudo incluiu uma comparação com o regime de Solvência I. Este teste inclui introdução do Requisito de Capital Mínimo (MCR). Os resultados demonstram que as provisões técnicas tendem a diminuir, enquanto para a maioria das companhias (98%), não é necessário adicionar capital ao MCR. Um ponto importante foi a avaliação de ativos e passivos para o cálculo do SCR.
- QIS 4 – O objetivo deste teste foi utilizar uma fórmula standard mais refinada e apontada ao risco. Cerca de 98,8% dos participantes foram capazes de cobrir o MCR, mas 11% não conseguiram atingir o SCR necessário.
- QIS 5 – Permitiu testar os 3 pilares da diretiva. Realizado a 14 de março de 2011 e último estudo realizado antes de implementar o novo regime de solvência. Participaram 2520 companhias de seguro e resseguro, onde foram capazes de cobrir 95% das provisões técnicas e 85% dos prémios.

Em novembro 2009, o regime de Solvência II é aprovado, e que a diretiva tem de ser transposta para a legislação de cada estado-membro. A data prevista para a sua implementação era outubro de 2012. No entanto, o prazo foi estendido devido a alterações (Clipici, 2012).

Solvência II é um regime com um conjunto atualizado de requisitos regulamentares para as seguradoras, pertencentes à União Europeia. O presente regime foi adaptado das regulações do Basileia II (sistema prudencial do setor bancário) e a sua *framework* foi construída sob 3 pilares (Roth *et al*., 2013).

O pilar I tem o objetivo de calcular os requisitos de capital de solvência e mínimo (SCR/MCR), que podem ser interpretados como os limites mínimos de capitais próprios que uma companhia necessita ter disponível para mitigar o risco de insolvência. O pilar II pretende cumprir os requisitos de governação e, por isso, implementar medidas de controlo interno para a gestão do risco. O pilar III pretende divulgar a informação relativa à situação financeira e solvência da companhia, de forma transparente, na forma de relatórios (Roth *et al*., 2013; Vukovic, 2015).

A gestão da Solvência de uma empresa de seguros não pode ser só baseada no pilar I e, por isso, esse pilar não pode estar isolado do pilar II e III. A importância de ter um critério qualitativa e processos revistos sob o pilar II em conjunto com o reportar e divulgar das provisões sob o pilar III formam um sistema viável e coerente (Steffen, 2008).

2.3 Solvência II

Solvência II é o atual regime de solvência, à imagem do regime Basileia II (sistema prudencial do setor bancário), que passou a ser aplicável ao setor segurador, desde 1 de janeiro de 2016 (ASF, 2017a). O Parlamento Europeu e a Comissão Europeia aprovaram este novo regime de solvência através da Diretiva n.º 2009/138/CE de 25 de novembro, de forma a garantir a sua solvência, disponibilizando a quantidade de capital de solvência mínimo (Roth *et al*., 2013). A transposição para o Direito nacional da Diretiva Europeia foi efetuada pela Lei 147/2015, de 9 de setembro, que aprova o novo Regime Jurídico de Acesso e Exercício da Atividade Seguradora (RJASR). A Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) é a entidade portuguesa responsável pela regulação e supervisão da atividade seguradora, resseguradora, dos fundos de pensões e respetivas entidades gestoras e da mediação de seguros (ASF, 2017b; Fidelidade, 2022).

O principal foco do Solvência II é a proteção dos tomadores de seguros, seguradores e beneficiários. O balanço de contas deve-se basear na perspetiva do tomador de seguro, o que significa que as instituições financeiras precisam de reservar um nível de capital adequado para absorver as perdas sofridas pelos riscos das suas operações (Pitselis, 2009). Adotar sistemas dinâmicos de gestão de risco, que englobem os riscos mais significativos, para

permitir uma melhor adaptação ao perfil de risco. A supervisão é forçada a um processo transparente, permitindo intervenções no surgimento de problemas. Por fim, pretende promover a competitividade das seguradoras (Lages, 2010).

2.3.1 Os Três Pilares

A *framework* de Solvência II é construída sob 3 pilares, Figura 2.4.

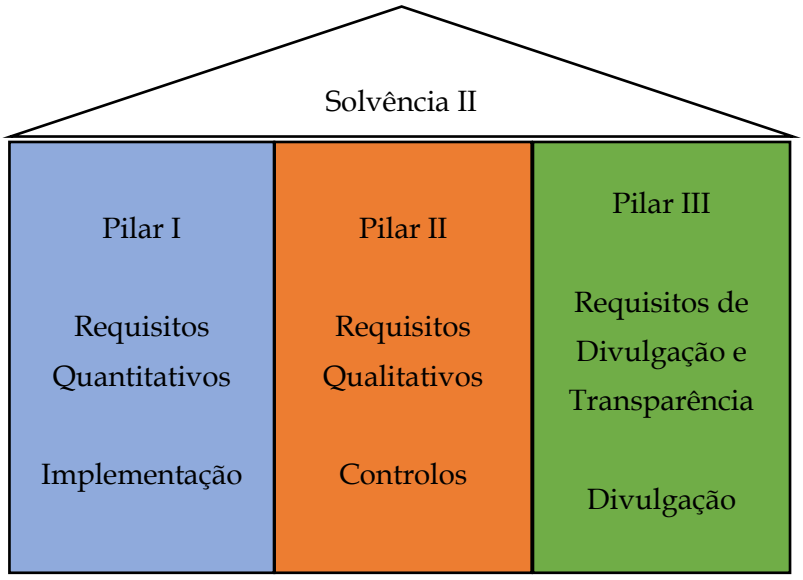


Figura 2.4 - *Framework* de Solvência II adaptado de (van Grinsven & Bloemkolk, 2009)

2.3.1.1 Pilar I

O pilar I, também denominado de **Requisitos Quantitativos de Capital,** introduz os critérios para a avaliação da posição de solvência das empresas de seguros dentro da União Europeia (UE). As instituições que avaliaram o seu apetite ao risco sob as novas regulações, podem ter de alterar as suas estratégias de negócio, de modo a atingir o rácio de Solvência II adequado.

Sob o regime de Solvência II, o capital deve estar disponível de modo a suportar os riscos apresentados no balanço de contas. Inclui Não-vida, Vida, saúde, bem como riscos de contraparte, de mercado e operacional. Assim, baseia-se numa análise abrangente dos riscos, levando em conta a interação entre ativos (ativos de resseguro, investimentos e outros ativos) e passivos (Provisões técnicas e outros passivos), mitigação de riscos e diversificação (Pitselis, 2009). Para além disso, o Solvência II considera que o ativo e o passivo (responsabilidades) de uma empresa devem ser avaliados, tendo em conta as flutuações de mercado. As normas IFRS (*International Financial Reporting Standards*) podem ser usadas como base para avaliar o capital disponível (diferença entre ativo e passivo) (Pitselis, 2009) (ASF, 2020).

Neste Pilar, a EIOPA descreve como os ativos e passivos de uma seguradora devem ser valorizados. Os elementos do ativo e do passivo (provisões técnicas) devem ser avaliados pelo montante por que podem ser transacionados entre as partes informadas agindo de livre vontade numa transação em condições normais de mercado. (Boonen, 2017; Parlamento Europeu e do Conselho, 2009).

No balanço de contas, todos os itens de capital (provisões técnicas, investimentos e fundos próprios elegíveis) devem ser avaliados, de acordo com o regime de Solvência II, Figura 2.5. As provisões técnicas correspondem ao montante atual que uma empresa de seguros teria de pagar se transferisse imediatamente as suas obrigações de seguro e resseguro para outra empresa de seguros ou resseguros. A quantidade elegível de capital próprio baseia-se na determinação dos fundos próprios de base e dos fundos próprios complementares que não constam no balanço de contas, da classificação dos fundos próprios e da sua elegibilidade, que correspondem essencialmente ao excesso do ativo sobre o passivo (Jornal Oficial da União Europeia, 2009; Pitselis, 2009).

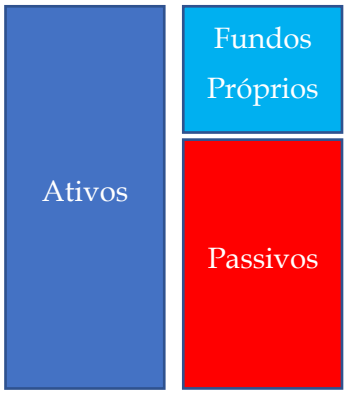


Figura 2.5 - Fundos Próprios adaptado de (EIOPA, 2014a)

Por outro lado, também são estabelecidos dois patamares de exigências de capital: o requisito de solvência mínimo (MCR) e o requisito de capital de Solvência (SCR).

O MCR estabelece um nível máximo de alerta, correspondendo ao montante de fundos próprios que deve ser sempre preservado, sob pena de colocar em risco o cumprimento das responsabilidades da seguradora. Também representa um limiar inferior ao qual o supervisor nacional interviria. O MCR destina-se a refletir um nível de confiança de 85% do valor em risco dos fundos próprios de base de uma empresa de seguros durante um período de um ano e

está limitado entre 25% e 45% do SCR da seguradora (DCWP, 2012; Parlamento Europeu e do Conselho, 2009).

O Requisito de Capital de Solvência, que é calculado abrangendo os riscos específicos de seguros, de mercado, de crédito e operacional, apresentados na árvore de sub-módulos de riscos da Figura 2.6 visa garantir a existência de fundos próprios elegíveis em montante suficiente para absorver perdas significativas decorrentes dos riscos a que uma empresa de seguros pode estar exposta. Deste modo, o SCR é a quantidade de capital disponível que permite absorver uma perda elevada (Steffen, 2008).

O Value-at-Risk (VaR) é um método de medição dos riscos que a indústria seguradora aplica para calcular a exposição de cada risco para fazer uma gestão bem-sucedida, segundo o regime de Solvência. Depende da severidade e da frequência do risco (Kenton, 2023). Por outras palavras, a exposição calculada para cada risco, o Valor em Risco, representa a perda máxima esperada num horizonte temporal de 1 ano, com um nível de confiança de 99,5%, ou seja, a probabilidade das perdas num ano serem superiores ao VaR calculado é de 1 em 200 anos.

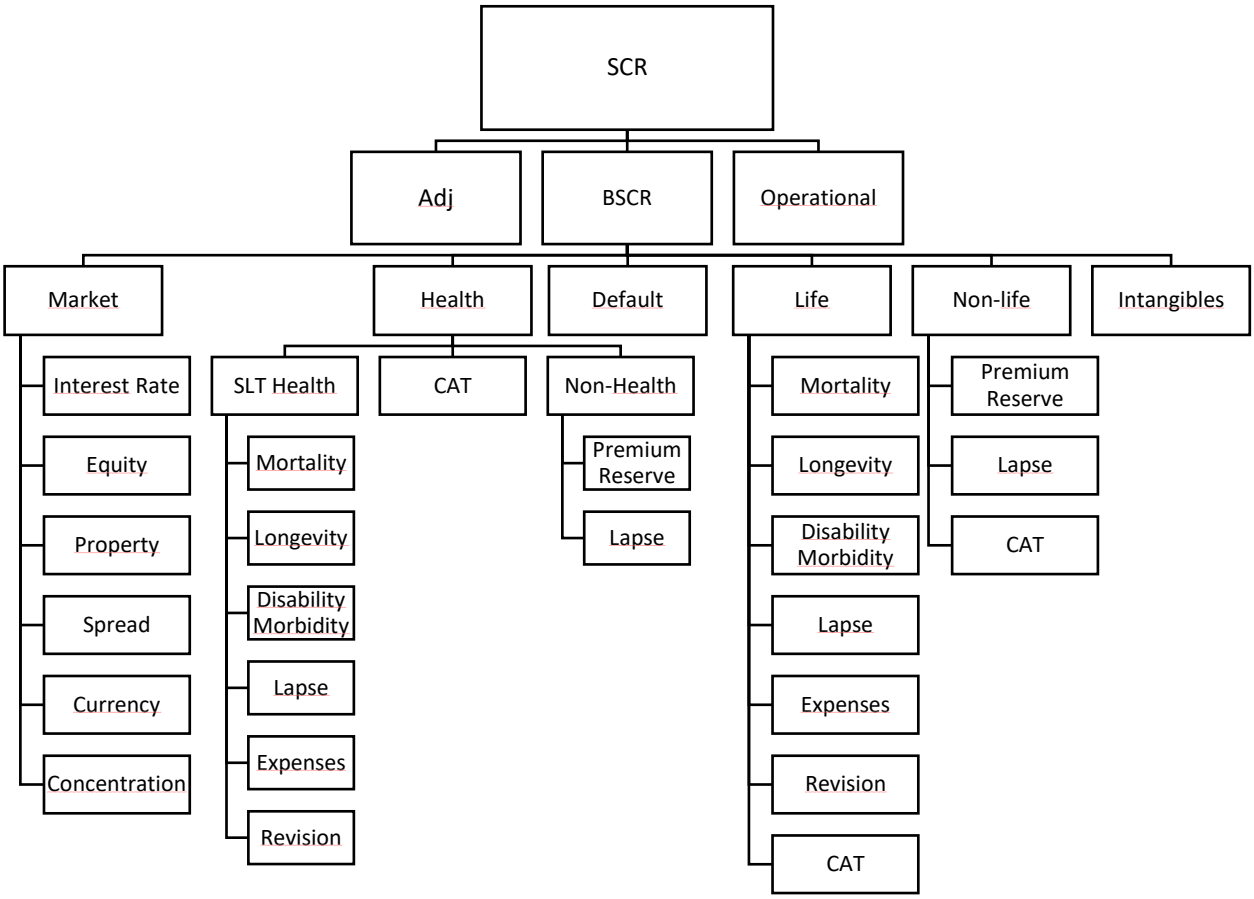


Figura 2.6 - Requisito de Capital de Solvência adaptado de (EIOPA, 2014a)

O SCR é o nível de capital, que corresponde ao VaR dos fundos próprios de base de uma empresa de seguros ou resseguros sujeitos a um nível de confiança de 99,5% para cobrir perdas inesperadas durante um período de um ano. Trata-se de um nível que se destina a ser suficiente para que a seguradora seja capaz de resistir a um evento de perda de 1 em 200 anos no prazo de um ano, com ativos suficientes para permitir a venda ou transferência dos seus passivos remanescentes para outra seguradora (Baranga, 2016; DCWP, 2012; Steffen, 2008). Este objetivo de calibração é aplicado a cada módulo de risco individual e sub-módulo.

A grande alteração deste pilar foi a valorização dos passivos no cálculo do SCR, algo que era desprezado pelo primeiro regime de solvência. Assim, é preciso estar constantemente a avaliar as provisões técnicas, dado que são importantes para determinar a quantidade de capital elegível para cobrir o SCR. A proporção entre capital disponível e o SCR são um indicador da capitalização da empresa. Deste modo, para a empresa estar numa situação favorável, requer que a quantidade de capital disponível seja, pelo menos, igual ao SCR, ou

seja, esse rácio deve ser superior a um, garantindo os requisitos de solvência das companhias de seguro (Pitselis, 2009). É de salientar que a necessidade de possuir uma quantidade de capital próprio serve para absorver perdas ocorridas pelos riscos das operações (Pitselis, 2009).

Segundo este regime, as instituições europeias devem optar pelo método da Fórmula-Padrão no cálculo do SCR ou usar um modelo interno Total ou Parcial aprovado pela autoridade de supervisão que seja capaz de fazer o mesmo ou que tenha mais em consideração a dimensão da seguradora, bem como o seu volume de negócio. Por esta razão, as organizações têm uma decisão importante a optar, em qual das abordagens se vão basear (ASF, 2017a). Os modelos internos parciais ou totais são semelhantes ao modelo partilhado pelo pilar I de Solvência II, mas que têm em conta o perfil de risco, sendo capazes de calcular requisitos de capitais mais adequados e até quantificar riscos com falta de informação (Baranga, 2016; Cantle *et al*., 2012).

A utilização da Fórmula-Padrão tem o objetivo de capturar os riscos materiais e quantificáveis em que a maioria das organizações está exposta. Contudo, não significa que cobra todos os riscos materiais de uma organização em específico. Como o próprio nome indica, a natureza e desenho do método de cálculo é normal ou comum, ou seja, não está desenhado/desenvolvido para situações ou riscos específicos. Desta forma, esta fórmula pode não refletir, efetivamente, o perfil de risco de uma organização e, consequentemente, a quantidade de capital próprio necessária para absorver um evento catastrófico, aumentando o risco de insolvência (EIOPA, 2014a).

Segundo a Fórmula-Padrão, o SCR, que é calculado através da equação (2.1), deverá corresponder à soma do Requisito de Capital de Solvência de Base (BasicSCR), calculado através da equação (2.2), Requisito de Capital para o Risco Operacional (SCR_op) e o Ajustamento das Provisões Técnicas e dos Impostos Diferidos em função da capacidade de absorção das respetivas perdas (Adj) (Lages, 2010).

$$SCR = BasicSCR + SCR_{op} - Adj \tag{2.1}$$

$$BasicSCR = \sqrt{\sum_{i,j} Corr_{i,j} * SCR_i * SCR_j} + SCR_{intangíveis} \tag{2.2}$$

2.3.1.2 Pilar II

A principal diferença do regime Solvência II para o regime anterior é a inclusão do pilar II, denominado de **Requisitos Qualitativas e Processo de Supervisão**. O pensamento por trás

do regime atual é parte de um processo de desenvolvimento mais amplo para a supervisão e reflete as ideias da *International Association of Insurance Supervisors (IAIS) e International Actuarial Association* (IAA) (Lavelle *et al*., 2010).

Uma das grandes dificuldades da implementação da nova Diretiva Europeia tem sido como interpretar e aplicar as regulações, devidamente, de modo a criar um processo de gestão de risco que vá ao encontro dos requisitos (Dupont *et al*., 2012).

No início de 2011, as organizações começaram a focar-se no pilar II de Solvência II, que as levou a desafiarem a sua própria cultura de risco, de modo a ser possível definir ou redefinir o risco de governação e de estratégia e considerar a implementação operacional da função de gestão de risco (Dupont *et al*., 2012).

O controlo de risco é um dos elementos-chave desta diretiva. Por esta razão, o *compliance* do pilar II levanta questões, tais como:

- O que é que as regulações de Solvência II requerem, exatamente?
- Como devem as provisões ser aplicadas à companhia?
- Que limitações ou fatores determinantes são usados para configurar um sistema de gestão de risco operacional o mais preciso possível?

O Pilar II tem a função de definir novos requisitos qualitativos para acautelar a existência e manutenção de sistemas de governação. Para além disso, também engloba todos os princípios e práticas de gestão de risco requeridos relacionados com o risco e o capital estimados abrangidos pelo pilar I. As provisões de Solvência II são baseadas somente nos princípios estipulados. Os reguladores querem que cada organização seja responsável por determinar a sua estrutura organizacional (Dupont *et al*., 2012). Na Tabela 2.2, é possível verificar as principais provisões do Pilar II:

Tabela 2.2 - Principais Provisões do Pilar II adaptado de (Dupont *et al*., 2012)

Provisões	**Descrição**
Governação de Risco (art.º 41 a 49)	Requisitos de governação gerais (Segregação de responsabilidades, gestão de conflitos de interesse, etc); Princípio de proporcionalidade do sistema de risco em relação à complexidade do perfil de risco;

Provisões	Descrição
	Definição de funções chave na gestão de risco e no âmbito do sistema de risco; Requisitos adequados para as principais funções de gestão de risco; Bons princípios de remuneração.
Novo processo de supervisão (art.º 27 a 39)	Novo processo de supervisão baseado no diálogo permanente com o regulador e em que a companhia carrega o "fardo da prova"; A opção do regulador de sancionar qualquer divergência quantitativa ou qualitativa dos padrões esperados com coimas.
Modelo Interno (art.º 120 a 126)	Requerimento para mostrar que o modelo interno é usado efetivamente na monitorização (alocação de capital, gestão de risco operacional). Avaliação concreta baseada em nove princípios (adoção por gestão, reflexão precisa do perfil de risco, etc) Processo de validação interna. Modelo de sensibilidade e testes de estabilidade.
ORSA (art.º 45)	Um dos elementos centrais deste Pilar é a realização de um exercício, pelo menos anual, de autoavaliação do risco e da solvência (ORSA). Através deste exercício, a empresa de seguros deve efetuar uma avaliação prospetiva sobre a suficiência do capital disponível para atingir os seus objetivos de negócio e estratégicos.

A Figura 2.7 apresenta os 7 principais componentes do sistema de governação dos riscos.

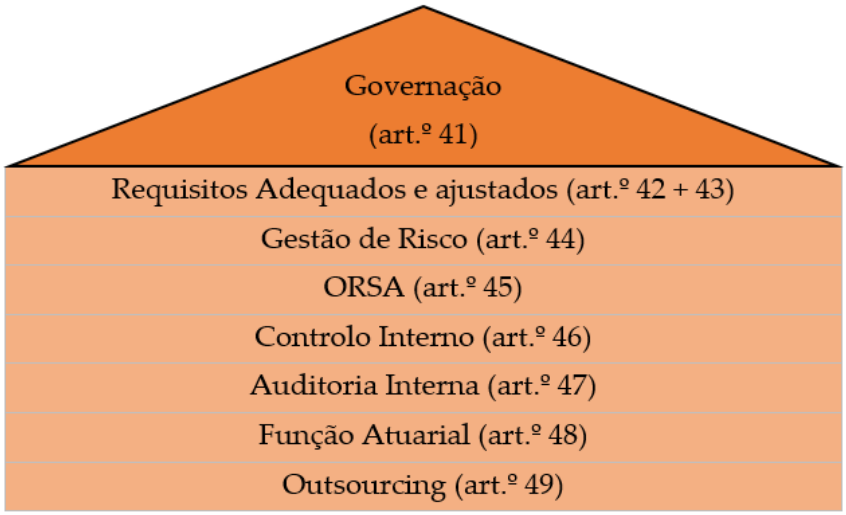


Figura 2.7 - Sistemas de Governação adaptado de (Dupont *et al*., 2012)

O Artigo 41 remete para os requisitos gerais de governação, sendo uma introdução para os seguintes artigos. Um bom sistema de governação é estabelecido, por regras fundamentais, como um sistema completo composto por funções e regras utilizadas pelos reguladores e modelos para procedimentos de decisão adequados (Dupont *et al*., 2012). Por outras palavras:

- Construir um sistema de governação eficaz de acordo com a Diretiva Solvência II que providencie uma gestão sã e prudente (EIOPA, 2014b);
- Construir um sistema de gestão de riscos eficaz que inclua estratégias, processos e procedimentos de reporte necessários para identificar, medir, monitorizar, gerir e reportar, de forma contínua, os riscos, a nível individual e a um nível agregado, aos quais estão ou podem estar expostos, e as suas interdependências;
- Fornecer informações qualitativas que permitam às autoridades nacionais competentes avaliar a qualidade do sistema de governação (EIOPA), 2014b).

Os Artigos 42 e 43 explicam a necessidade de garantir que as pessoas que governam a seguradora ou executam outras funções fundamentais ou caso existem alterações de cargos devem preencher os seguintes requisitos:

- As suas qualificações profissionais, conhecimentos e experiência são adequados para permitir uma gestão sã e prudente (*Fit*);
- São de boa reputação e integridade (*Proper*);

A EIOPA define ORSA (art.º 45) como um conjunto de processos e procedimentos para identificar, avaliar, monitorizar, gerir e reportar os riscos a curto e longo prazo que uma seguradora pode enfrentar e determinar os capitais próprios necessários para garantir as necessidades globais de solvência da empresa (Lavelle *et al*., 2010). Desta forma, este procedimento não é um simples exercício ou relatório, é uma parte fundamental da gestão de risco, ou seja, é definido como um processo documentado (Lavelle *et al*., 2010). A Figura 2.8 ilustra um exemplo de uma *framework* do ORSA, que as companhias de seguro utilizam.

Figura 2.8 - *Framework* ORSA adaptado de (Aon, 2012)

De acordo com o artigo 46, as companhias de seguro devem possuir um sistema de controlo interno efetivo, devendo incluir procedimentos administrativos e contabilísticos, disposições adequadas em termos de comunicação a todos os níveis da empresa e uma função de conformidade (CEIOPS, 2009b; Dupont *et al*., 2012; EIOPA, 2014b).

A auditoria interna, definida no artigo 47 (CEIOPS, 2009b; Dupont *et al*., 2012; EIOPA, 2014b), deve avaliar a adequação e eficácia do sistema de controlo interno e outros elementos do sistema de governação, sendo objetiva e independente das funções operacionais.

A função Atuarial (art.º 48) é descrita como uma função de avaliação, que tem o objetivo de coordenar o cálculo das provisões técnicas (CEIOPS, 2009b; Dupont *et al*., 2012; EIOPA, 2014b), da seguinte forma:

- Assegurar a adequação das metodologias e modelos subjacentes utilizados, bem como os pressupostos apresentados no cálculo das provisões técnicas;
- Avaliar a suficiência e a qualidade dos dados utilizados no cálculo das provisões técnicas; comparar as melhores estimativas com a experiência;
- Informar o órgão administrativo, de gestão ou de fiscalização da fiabilidade e adequação do cálculo das provisões técnicas;

- Supervisionar o cálculo das disposições técnicas, exprimir um parecer sobre a política global de subscrição;
- Exprimir uma opinião sobre a adequação das disposições relativas aos resseguros;
- Contribuir para a implementação eficaz do sistema de gestão de riscos.

O outsourcing, descrito no art.º 49 (CEIOPS, 2009b; Dupont *et al*., 2012; EIOPA, 2014b), determina e documenta se a função ou atividade subcontratada é uma função ou atividade crítica ou importante baseada no facto de esta função ou atividade ser essencial para o funcionamento da empresa, uma vez que não seria capaz de prestar os seus serviços aos tomadores de seguros sem a subcontratação, ou seja, não afetar negativamente a qualidade de serviço, sistemas de governação e a exposição ao risco operacional.

Segundo o art.º 44 da governação de risco, deve-se implementar na estrutura organizacional um sistema de gestão de risco eficaz composto por estratégias, processos bem documentados e procedimentos de comunicação necessários para identificar, medir, monitorizar, gerir e reportar, de forma contínua, os riscos ao nível do grupo e que define o apetite pelo risco do grupo e os seus limites globais de tolerância face ao risco (Dupont *et al*., 2012).

De acordo com a opinião da EIOPA (EIOPA, 2014b), a empresa deve estabelecer uma política de gestão de riscos que:

- Defina as categorias de risco e os métodos de mensuração dos riscos;
- Enuncie o modo como a empresa gere cada categoria de risco que seja relevante e qualquer potencial agregação de riscos;
- Descreva a articulação com as necessidades globais de solvência identificadas na autoavaliação prospetiva dos riscos com base nos princípios do ORSA, os requisitos de capital regulamentares e os limites de tolerância face ao risco da empresa;
- Especifique os limites de tolerância face ao risco em cada uma das categorias de risco relevantes em consonância com apetite pelo risco global da empresa;
- Descreva a frequência e o conteúdo dos testes de *stress* regulares e as situações em que se justifique a realização de testes de *stress ad-hoc*.

O sistema de governação é um parâmetro muito importante neste cenário. A companhia precisa de implementar um sistema que tenha em consideração o risco de perfil da companhia.

Assim, permite avaliar a adequação, conformidade com os artigos mencionados na Figura 2.7. E também rever ou atualizar a documentação da estrutura da organização, titulares de funções e objetivos e estratégias de negócio (Lavelle *et al*., 2010). É essencial reconhecer e definir as funções envolvidas na gestão de risco. Esta ação não é algo simples, porque a gestão envolve todos os níveis da companhia. Para isso, todos os níveis devem estar interligados e a cada nível o sistema deve integrar diferentes elementos: risco operacional, coordenação da tomada de riscos e supervisão da tomada de riscos (Dupont *et al*., 2012).

O modelo de "três linhas", representado na Figura 2.9, é um modelo de governação que se insere e se ajusta à *framework* de Solvência II, e garante a gestão eficaz dos riscos no setor segurador. O modelo consiste no seguinte (KPMG, 2017):

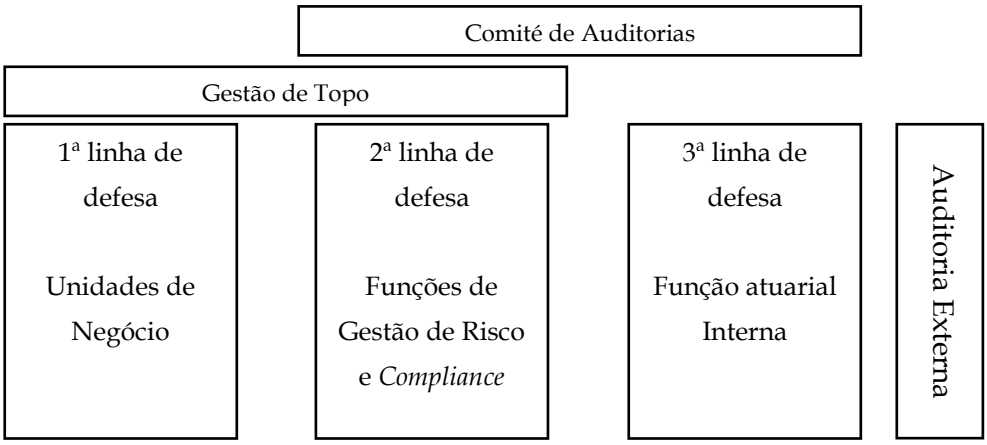


Figura 2.9 - Modelo três linhas adaptado de (Ferma/Eciia, 2010)

- A primeira linha de defesa é composta pelos funcionários da linha da frente, isto é, as atividades diárias realizadas nas áreas de negócio. São os principais responsáveis por identificar os riscos e pelas técnicas e processos de gestão em prática. Exige que os funcionários apliquem o controle interno no tratamento dos riscos associados às tarefas individuais.
- A segunda linha de defesa é constituída por um órgão especializado em funções de gestão de risco, de supervisão, que incluem controlo de riscos e conformidade. O seu papel é apoiar a primeira linha de defesa na gestão dos seus riscos, através de uma *framework* consistente, reduzindo a sua exposição ao risco.
- A terceira linha de defesa é composta pela função atuarial interna, que deve rever de modo sistemático e eficiente as atividades das duas primeiras linhas de defesa e contribuir para a sua melhoria contínua. As suas funções são realizadas de forma independente e assegura que as duas primeiras linhas de defesa executam

> os seus objetivos tal como foram propostas (Dupont *et al*., 2012). Por outras palavras, auxiliam as organizações a atingir seus objetivos, introduzindo abordagens sistemáticas para uma gestão e procedimentos eficazes de risco (Aloqab *et al*., 2018).

As empresas, que se apoiam por esta *framework*, costumam definir os principais objetivos para coordenar os vários processos envolvidos na tomada de riscos. Este modelo permite definir responsabilidades a cada nível no processo de gestão de risco. Tem o propósito de designar funções específicas de gestão de risco e responsabilidades de acordo com o perfil de risco (Dupont *et al*., 2012).

A integração de princípios da gestão da qualidade e da gestão de riscos, bem como a abordagem gestão total da qualidade, podem reforçar significativamente as três linhas de defesa, tornando a gestão de risco operacional mais eficiente, em instituições financeiras (Aloqab *et al*., 2018).

Para além da governação, também é importante implementar um sistema de gestão de risco e de controlo interno eficaz. Em relação à *framework* implementada, é preciso fazer uma avaliação interna ou externa dos processos utilizados na gestão de risco, tais como a cultura de risco, responsabilidades, plano de negócio, potenciais novas atividades, questionários de avaliação de riscos e controlos, testes de stress, utilização de sistemas certificados e, por fim, documentar os processos todos.

O teste de *stress* é um mecanismo efetivo para testar qualitativamente e quantitativamente o efeito sobre o capital e a solvência de alterações adversas nas condições financeiras, Figura 2.10 (Aon Benfield, 2012). O nível e a qualidade de capital entre as grandes organizações aumentaram com a introdução de testes de *stress* durante a crise financeira (Aloqab *et al*., 2018).

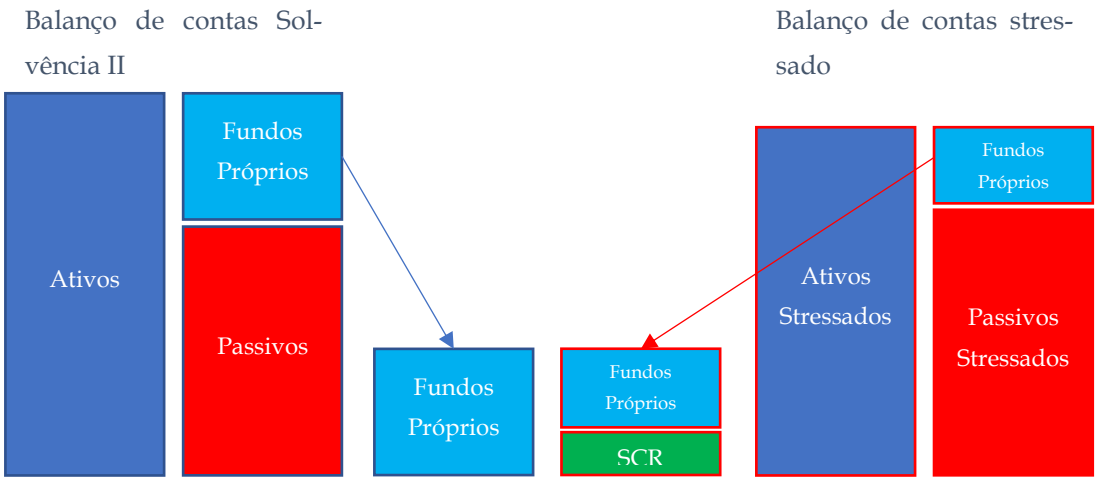


Figura 2.10 - *Stress Tests* adaptado de (EIOPA, 2014a)

A identificação e avaliação dos riscos é algo bastante importante, porque permite à companhia de seguros perceber os riscos existentes e possíveis futuros riscos (ex.: Contraparte, crédito, mercado, operacional, reputacional, etc.). Para tal, os gestores podem usar modelos para os avaliar, utilizar questionários que permitem quantificar esses riscos ou avaliar a materialidade desses mesmos riscos (Lavelle *et al*., 2010).

Por fim, é necessário relacionar a tolerância ao risco com a estratégia de negócio, a partir da revisão dos níveis de categoria dos riscos ou implementar processos que garantem que a companhia cumpre com os níveis de risco estabelecidos (Lavelle *et al*., 2010).

Em suma, o grande desafio do Pilar II está em avaliar como interpretar, adaptar e implementar essas *frameworks* e estratégias dentro de uma organização, uma vez que não são oferecidos exemplos práticos, o que implica que as seguradoras apliquem estes conceitos ao seu critério (Dupont *et al*., 2012). Para serem bem-sucedidos, essas *frameworks* devem estar ajustadas, corretamente calibradas e adaptadas às características específicas do seu negócio, à complexidade da sua estrutura organizacional e à sua "cultura de risco" (Dupont *et al*., 2012).

2.3.1.3 Pilar III

O presente pilar é conhecido por **Disciplina de Mercado**, que vem culminar e reforçar os requisitos dos outros pilares do regime de Solvência II. São estabelecidas novas obrigações de informação ao público e ao supervisor, nomeadamente, a obrigação de divulgação anual de um relatório sobre a solvência e a situação financeira da empresa de seguros (EIOPA), 2015; Lavelle *et al*., 2010).

Tem a missão de promover a disciplina de mercado e mecanismos de mercado para fornecer aos *stakeholders* toda a informação relevante sobre a situação financeira e solvência,

por exemplo, as atividades exercidas, o sistema de governação, perfil de risco, avaliação para efeitos de solvência, como a partilha do MCR e do SCR e a gestão de capital (Clipici, 2012).

No que diz respeito ao nível de prestação e divulgação da informação financeira e prudencial, esta deverá convergir o mais possível com as normas contabilísticas elaboradas pelo *International Accounting Standards Board* (IASB) (Lages, 2010).

Assim, a transparência e informação aberta destinam-se a ajudar a impor uma maior disciplina à indústria, de modo a proteger os tomadores de seguro e os beneficiários (Clipici, 2012).

2.4 Risco Operacional

Com o crescimento do mercado e o desenvolvimento de novos serviços de negócios para atrair clientes, o risco operacional tem-se tornado cada vez mais complexo, potencialmente mais devastador e cada vez mais complicado de prever e antecipar (van Grinsven & Bloemkolk, 2009).

O risco operacional é uma das maiores ameaças que o setor segurador enfrenta, só começou a ter a devida atenção há relativamente pouco tempo. Daí a importância da sua gestão e da implementação de modelos de governação sólidos e robustos. Por isso, o foco das seguradoras em relação ao risco operacional tem aumentado devido aos recentes desenvolvimentos na sua gestão, às orientações providenciadas pelos reguladores e ao novo regime de Solvência II (van Grinsven & Bloemkolk, 2009).

Um dos benefícios de uma abordagem formal de risco operacional é, sempre que possível, desenvolver incentivos suficientes para que os gestores das unidades de negócio adotem práticas de gestão de risco sãs através da alocação de capital, revisões de desempenho e outros mecanismos (Torre-Enciso & Barros, 2012)

Com a transição do regime de Solvência, o risco operacional foi uma das principais novidades, devido ao crescente interesse das autoridades reguladoras, (Torre-Enciso & Barros, 2012) e passou a ser considerado nos processos de uma empresa e a ter peso devido na estrutura de uma empresa (Vukovic, 2015). Este risco foi identificado como uma categoria separada dos outros riscos e as instituições financeiras estão a incluir informação sobre o risco operacional nos seus relatórios anuais de Solvência (Torre-Enciso & Barros, 2012).

Solvência II define o risco operacional como o risco de perdas resultantes de procedimentos internos inadequados ou deficientes, do pessoal ou dos sistemas, ou ainda de acontecimentos externos, incluindo riscos legais e jurídicos (Barriga & Rosengren, 2006).

Para analisar o risco operacional no setor segurador, é necessário dar atenção ao Pilar I e II. As seguradoras passaram a dedicar parte dos seus fundos próprios para cobrir a sua exposição ao risco operacional (Vukovic, 2015).

2.4.1 Requisito de capital para o Risco Operacional (Pilar I)

Estabelecer uma Fórmula-Padrão adequada para a regulação das empresas de seguros não é uma tarefa simples. É necessário ter conhecimento de diversos modelos de negócio e particularidades nacionais.

Segundo a fórmula providenciada pelo regime de Solvência II e os seus reguladores, a EIOPA insere a diversificação entre o risco operacional e os outros riscos financeiros de modo a reduzir o requisito de capital preciso para uma empresa de seguros (Baranga, 2016).

Para além dos pressupostos mencionados acima, ainda é de mencionar os seguintes pressupostos:

- O pressuposto geral no módulo de risco operacional é a presença de um certo nível padronizado de gestão de riscos.
- Para as empresas ligadas por unidades, as características são semelhantes às de outros produtos-vida. Portanto, os parâmetros evoluirão em linha com o parâmetro de vida.
- No que diz respeito à dimensão de volume de despesas para as atividades ligadas por unidades, presume-se que as despesas de aquisição se referem exclusivamente a intermediários de seguros, que não dão origem a qualquer risco operacional (Baranga, 2016; EIOPA, 2014a).

A equação (2.3) representa o cálculo do requisito de capital para o risco operacional (SCR_{op}) que aumenta juntamente com a dimensão da atividade do negócio da seguradora, uma vez que decorre de processos internos inadequados ou falhados, pessoal ou sistemas, ou de eventos externos a não ser que a organização esteja bem diversificada e gerida, correspondendo a uma percentagem do Requisito de Capital de Solvência Básico (BSCR) (EIOPA), 2014a). No que diz respeito às operações de seguros e de resseguros, o cálculo do coeficiente básico de risco operacional (OP_{lnul}) terá em conta o volume dessas operações, em termos de prémios adquiridos e de provisões técnicas detidas relativamente a essas obrigações de seguro e de resseguro. Neste caso, OP_{lnul} não deve exceder 30% do BSCR relativo a essas operações de seguro e de resseguro (CEIOPS, 2009b).

$$SCR_{op} = mín\{BSCR_{cap} * BSCR; OP_{lnul}\} + Ul_f * Exp_{ul}, \text{ onde } BSCR_{cap}=30\% \qquad (2.3)$$

A parcela Ul_f é o coeficiente a aplicar ao montante das despesas anuais (bruto de resseguro) incorridas em relação às operações associadas a unidades de negócio. Exp_{ul} refere-se ao valor total das despesas anuais (bruto de resseguro) incorridas nas mesmas unidades de negócio, que inclui despesas administrativas (exceto despesas de aquisição). O cálculo deve ser baseado nas despesas dos últimos anos e não em projeções de futuras despesas (Baranga, 2016; CEIOPS, 2009b).

A equação (2.4) representa o resultado obtido a partir do máximo entre as provisões técnicas e os prémios adquiridos (Baranga, 2016):

$$Op_{lnul} = máx(Op_{provisions}; Op_{Premiums}) \tag{2.4}$$

onde as equações (2.5) e (2.6), calculam as provisões técnicas e os prémios, respetivamente, e no anexo A é possível ver as descrições dos fatores (CEIOPS, 2009b):

$$\begin{aligned} Op_{Premiums} = {} & P_{life_f} * \left(Earn_{life} + Earn_{SLT\ Health} - Earn_{life-ul}\right) \\ & + P_{nl_f} * (Earn_{nl} + Earn_{Non-SLT\ Health}) \\ & + Max(0, P_{life_f} * (\Delta Earn_{life} - \Delta Earn_{life-ul})) \\ & + Max(0, P_{nl_f} * \Delta Earn_{non-life}) \end{aligned} \tag{2.5}$$

$$\begin{aligned} Op_{Provisions} = {} & TP_{life_f} * \left(TP_{life} + TP_{SLT\ Health} - TP_{life-ul}\right) \\ & + TP_{nl_f} * (TP_{nl} + TP_{Non-SLT\ Health}) \\ & + Max(0, TP_{life_f} * \left(\Delta TP_{life} - \Delta TP_{life-ul}\right)) \\ & + Max(0, TP_{nl_f} * \Delta TP_{non-life}) \end{aligned} \tag{2.6}$$

Onde:
P_{life_f}, P_{nl_f}, TP_{life_f}, TP_{nl_f} são os fatores a serem calibrados (Anexo A).

Δ= alteração nos prêmios ganhos ou nas provisões técnicas do ano t-1 para t superiores a 10%, sem diferenciação entre Vida e Não-Vida

2.4.2 Gestão de Risco Operacional (Pilar II)

A gestão de risco operacional envolve procedimentos, políticas, ações e ferramentas para gerir o risco e torná-lo aceitável. Deste modo, devem ser desenvolvidas diversas estratégias, que possibilitem evitar riscos, minimizar os efeitos adversos de enfrentar os riscos e aceitar, de alguma, as consequências provenientes do risco.

O conceito principal da sua gestão em Solvência II consiste em desenvolver e implementar funções de gestão de risco, definir estruturas organizacionais para todo o processo de gestão de riscos, abrangendo todas as funções, processos e organismos envolvidos na sua gestão (Dupont *et al*., 2012), implementando um sistema de controlo interno que a partir de ações tomadas de forma preventiva ou detetiva permita mitigar potenciais perdas originadas por falhas operacionais (EIOPA, 2014b).

No entanto, o regime atual imposto ao mercado segurador e ressegurador impõe/obriga as organizações a fazer a gestão do risco operacional, mas deixam ao seu critério o caminho a adotar. Desta forma, as instituições têm optado por desenvolver ao longo dos anos *framework*s internas que deem resposta aos requisitos regulamentares, e melhore a sua gestão.

A criação de uma *framework* de gestão de risco operacional é uma tarefa complexa, em especial numa organização com um histórico de processos, hábitos, organismos decisores estabelecidos, pois requer o envolvimento de todos os colaboradores e órgãos de decisão ao longo do processo. Por outro lado, a sua gestão deve ser integrada na organização, não só nas políticas e cultura da empresa, mas bem como na sua estrutura e processos (Epetimehin, 2013). Pretende que a tomada de decisões seja detalhada e informada sem detrimento do risco, para eliminar os efeitos provenientes de eventos perigosos e, por sua vez, reduzir a probabilidade da ocorrência desses eventos de perda (Oluwafemi, 2019).

A política de gestão de riscos operacional deve abranger, pelo menos, os seguintes pontos, no que respeita ao risco operacional:

- Identificação dos riscos operacionais a que está ou pode vir a estar exposta e avaliação da forma de os mitigar;
- Atividades e processos internos para gerir os riscos operacionais, incluindo o sistema de TI que os suporta;
- Limites de tolerância face ao risco nas principais áreas de risco operacional da empresa.
- Disposição de processos para identificar, analisar e comunicar eventos de risco operacional. Para tal, esta deve estabelecer um processo de recolha e monitorização de eventos de risco operacional (EIOPA), 2014b).

Em geral, as seguradoras e as instituições financeiras estão convencidas de que os programas de gestão de risco operacional protegem e valorizam o valor dos acionistas, porque é uma função interna distinta com os seus próprios processos, estruturas, ferramentas, estatísticas e estratégias de mitigação de riscos. Esta situação está a contribuir para o desenvolvimento de um processo formal e de uma maior transparência do risco operacional (Torre-Enciso & Barros, 2012).

No atual ambiente económico e regulamentar, *Chief Risk Officer* (CRO) tem o desafio de investir recursos com cuidado e prudência para aumentar as capacidades em sinergia com os requisitos de Solvência II (Dupont *et al*., 2012).

2.4.2.1 Dificuldades e desafios

A gestão do risco operacional levanta vários desafios, principalmente pela sua extensão, complexidade, subjetividade e a dificuldade em apurar a sua exposição.

A Formula-Padrão para o cálculo do SCR_{op} em Solvência II assume a presença do risco operacional em todos os outros riscos pela sua ligação ao BSCR que inclui os riscos de mercado, contraparte, saúde, vida e não-vida, por outro lado a sua limitação a 30% do BSCR revela alguma insegurança nos resultados obtidos pela fórmula para OP_{lnul}. Adicionalmente, se a informação reunida sobre de prémios adquiridos e provisões técnicos for imprecisa, pode levar a estimativas de capital incorretas. As calibrações dos fatores de risco operacionais têm sido uma tarefa particularmente desafiante devido à falta de informação disponível (CEIOPS, 2009b; EIOPA, 2014a).

O módulo de risco operacional baseia-se numa fórmula linear e, portanto, não é sensível às alterações do risco operacional nem aos fatores externos, tais como: fatores económicos, avanços tecnológicos e avanços regulatórios. A natureza estática da fórmula não permite captar todas as especificidades e dinamismo, bem como os processos e estruturas qualitativas usadas para mitigar o risco operacionais, não se adaptando ao perfil de risco de uma seguradora e, desta forma, não se foca no desenvolvimento de boas práticas de gestão de risco. Não reflete a elevada quantidade de riscos que se podem vir a materializar (CEIOPS, 2009b).

Assim, no que diz respeito às limitações da fórmula-padrão, a falta de mecanismos impostos pela regulamentação para uma avaliação quantitativa completa e robusta para o risco operacional, assim como a ausência de standards estabelecidos no mercado, influencia a gestão a complementar-se com abordagens e práticas qualitativas internas focadas no desenvolvimento da cultura de risco das organizações, desenhadas de acordo com a dimensão e as caraterísticas de cada organização.

Adicionalmente, as *framework*s de gestão de risco operacional que se estão desenvolvendo são na sua maioria compostas por um conjunto de ferramentas para identificação, avaliação e mapeamento do risco, indicadores e níveis de perda de dados. Ou seja, uma *framework* que inclua processos, ferramentas e estratégias de mitigação (Diehl & Weber, 2014).

2.5 Abordagens de Gestão de Risco Operacional

Face às dificuldades e desafios apresentados no capítulo anterior, a gestão necessita de incorporar processos nas suas atividades, que consigam ultrapassar estes obstáculos.

A gestão do risco operacional possui 2 vertentes/formas para estar ciente do risco operacional. Uma é mais direcionada para a exposição ao risco, onde se pretende quantificar o risco como um todo e não tanto mitigar a origem de cada risco e perceber se os métodos usados têm impacto na redução do risco.

Por outro lado, existe a vertente mais qualitativa, subjetiva, onde a seguradora não está tão focada no impacto económico que os riscos de caráter operacional terão. A companhia de seguro está mais interessada na análise do risco operacional, ou seja, pretende conhecer os seus riscos e perceber a sua origem e as formas que existem para mitigar os riscos, expondo, indiretamente, menos a empresa aos riscos. Por outras palavras, identificar, avaliar, reportar, monitorizar e melhorar a exposição do risco. Esta abordagem vai ser explorada no capítulo 4, com o desenvolvimento de um estudo de caso.

Por outro lado, o cumprimento das exigências impostas pelo pilar II e a necessidade de justificar aos reguladores que as empresas estão a usar mecanismos internos adequados para gerir o risco operacional e que uma estrutura de governação mais robusta permite uma melhor análise e recolha de informação. Assim, ao cargo da seguradora, pode notar-se um afastamento da abordagem standard, que permite às organizações adotarem um sistema de governação interno mais adequado para gerir o risco operacional (Cantle *et al*., 2012).

As seguradoras ao evoluírem no sentido de ter os seus próprios mecanismos internos e de efetuar uma gestão e melhoria contínua dos sistemas de gestão de risco operacional capazes de responder aos desafios impostos pelos reguladores e às necessidades do negócio, podem apoiar-se nas seguintes abordagens:

- Modelo baseado no histórico de eventos de risco operacional;
- Modelo baseado na Avaliação Prospetiva.

2.5.1 Histórico de eventos de risco operacional

Um histórico de eventos de risco operacional permite à organização construir uma imagem da sua exposição real ao risco operacional (The Institute of Operational Risk, 2021). Deste modo, a criação de uma base de dados de eventos de perda é um dos principais mecanismos na gestão de risco operacional (Roux, 2010).

A identificação de perdas operacionais pode ser determinada por dois parâmetros. Por um lado, em termos do seu impacto, severidade ou quantidade de perda, e por outro lado, depende da frequência com que o evento se repete ao longo de um período de tempo ou, dito de outra forma, a probabilidade de um evento ocorrer (Epetimehin, 2013).

De acordo com a Figura 2.11, é possível verificar a categorização das perdas, bem como a natureza dos eventos operacionais definida por uma função de ocorrência (frequência) e impacto (severidade). Podem ser definidos como recorrentes, os eventos com elevada frequência e baixa severidade, que também são aqueles mais conhecidos na gestão, como fraude em relatórios de sinistros. Enquanto, os eventos não-recorrentes são os mais perigosos, pois têm baixa frequência, porém elevada severidade, como por exemplo um incêndio ou um terremoto que leva à destruição de edifício (Epetimehin, 2013).

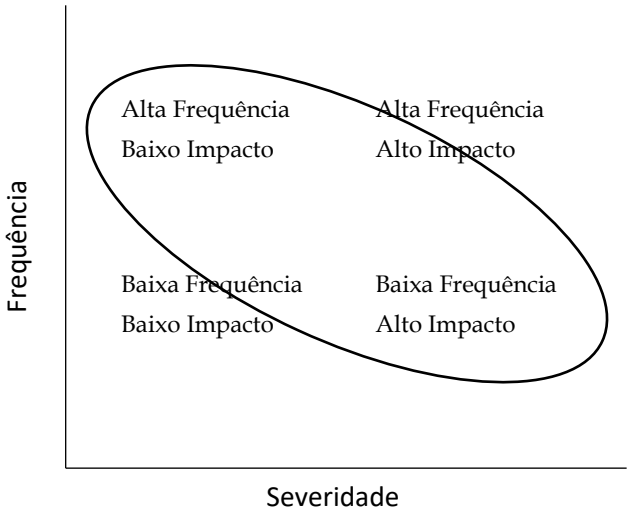


Figura 2.11 - Severidade vs Frequência adaptado de (Epetimehin, 2013)

Os dados de perdas internas são um elemento crítico na conceção de um modelo de medição interna, uma vez que representam melhor a estrutura do negócio, o sistema de controlo e a cultura de cada organização (Epetimehin, 2013). Desta forma, a existência de um

reportório de eventos de perda permite à empresa revelar novas exposições ao risco operacional, verificar como a exposição está a evoluir ao longo do tempo, identificar futuras ameaças e, assim, poder agir com conformidade. Para além disso, é importante incluir dados externos às bases de dados internas. O histórico de eventos de uma empresa pode não representar o espetro completo, sendo necessário a inclusão de eventos de perda externos de organizações semelhantes, que já tenham sofrido com essas perdas (The Institute of Operational Risk, 2021).

Assim, a existência de uma base dados central com o histórico de eventos de perda permite às empresas inúmeras vantagens (Roux, 2010), tais como:

- Determinar oportunidades de melhoria, consoante a análise das perdas colecionadas;
- Determinar se as medidas implementadas surtem efeito;
- Fornecer padrões entre atividades de negócio e determinar a sua influência na organização.
- Servir como plataforma para facilitar a gestão e controlo das perdas.

Na construção destas bases de dados pode-se incluir o seguinte:

- A identificação do departamento;
- O valor do impacto sofrido pela perda;
- A data de ocorrência da perda;
- A data de deteção da perda;
- A recuperação da perda;

Por norma, a coleção de eventos de perda requer perdas reais. No entanto, existem organizações que vão mais longe e colecionam "quase-perdas" ou recuperações. Uma quase-perda é um evento que ocorreu, mas que não resultou em qualquer perda devido possivelmente à eficácia de certos controlos, ex.: reembolso de uma fatura médica foi feito em duplicado. Uma recuperação

2.5.1.1 Limitações

Embora a abordagem dos eventos históricos de perda ofereça muitos benefícios na gestão do risco operacional, não está isenta de limitações. Estas incluem:

- **Falta de dados**: Nem todos os eventos de perda podem ter sido registados, especialmente se forem pequenos, tiverem ocorrido há muito tempo ou não tiverem sido reconhecidos como perdas operacionais na altura. Isto pode levar a uma compreensão incompleta da exposição ao risco operacional da organização.

- **Relevância dos dados históricos**: O passado nem sempre é um bom indicador do futuro, especialmente em ambientes em rápida mudança. Por exemplo, novas tecnologias podem introduzir novos tipos de riscos operacionais que não estavam presentes nos dados históricos.
- **Limitações dos dados externos**: Quando se utilizam dados externos, pode haver inconsistências devido a diferenças nas metodologias de recolha de dados, nos limites dos relatórios e nos processos empresariais das diferentes organizações. Também pode haver falta de acesso a dados externos pormenorizados sobre perdas devido a questões de confidencialidade.
- **Desvio na recolha de dados**: Pode haver enviesamentos na forma como as ocorrências de sinistro são comunicadas e registadas, em especial quando está envolvido o julgamento humano. Por exemplo, pode haver uma tendência para reportar certos tipos de perdas ou para dar demasiada importância a eventos recentes.
- **Dificuldade de quantificação do risco operacional**: Alguns tipos de risco operacional são difíceis de quantificar em termos monetários, o que torna difícil a sua incorporação na análise dos dados históricos de perdas.

2.5.2 Avaliação Prospetiva

A avaliação prospetiva do risco oferece uma perspetiva da empresa sobre a sua exposição futura ao risco e permite que uma empresa se possa proteger de acordo com os resultados obtidos, e tomar decisões proativas para prevenir ou minimizar o impacto.

Para tal, a avaliação prospetiva baseia-se em identificar, avaliar, monitorizar e mitigar potenciais riscos provenientes de causas operacionais (ISO, 2018). Permite à empresa preparar-se contra futuros eventos, em vez de apenas reagir a eventos de perda passados. Este processo segue as seguintes etapas:

2.5.2.1 Identificação do risco

Identificação do risco é um processo de encontrar, reconhecer e registar e, por sua vez, limitar potenciais riscos, que possam ter impacto para a empresa. O principal propósito desta atividade é identificar situações ou debilidades que possam ser um obstáculo para a obtenção de determinados objetivos empresariais (Roux, 2010). Informação atualizada, relevante e apropriada é um fator importante para identificar riscos (ISO, 2018).

De modo a realizar esta ação, é necessário fazer um levantamento das atividades e os possíveis riscos identificados. De seguida, saber se existem controlos e as suas finalidades e, por fim avaliar a sua eficácia.

Para realizar uma identificação adequada do risco, é preciso apoiar-se em mais do que uma técnica capaz de identificar os riscos inerentes à instituição, dos controlos criados para mitigar riscos e dos riscos residuais resultantes, tais como: Inventários de risco, mapeamento do risco, desde os processos, a controlos, a evidências, workshops/sessões com os colaboradores que percebem do negócio e estão em constante contacto com o risco, questionários de risco e controlos, comparar com a informação divulgada pelas outras organizações, entre muitos outros procedimentos (Roux, 2010).

2.5.2.2 Avaliação do Risco

Após esta fase inicial, prossegue-se para a compreensão da natureza do risco e avaliar a probabilidade de um evento ocorrer e o potencial impacto de um evento de perda, pois riscos medíveis podem ser controlados. Desta forma, é possível medir e avaliar a exposição dos riscos identificados com o objetivo de gerir e controlar os riscos que possam vir a ter impacto negativo na estratégia de negócio e o alcance dos objetivos.

A avaliação de potenciais impactos de um risco em particular não é uma tarefa fácil, pois existem inúmeros resultados possíveis ou o risco pode surgir várias vezes. Para além disso, o risco operacional contém particularidades que o tornam mais difícil de quantificar (Roux, 2010).

Um grande problema com qualquer tentativa de modelar perdas de risco operacional é a falta de dados. Os dados internos de eventos de baixa frequência raramente são suficientes para modelar as distribuições de perda com a precisão necessária. A utilização de distribuições de perdas paramétricas requer uma estimativa dos parâmetros com base nos dados existentes.

O desenvolvimento dos requisitos, o crescente foco na gestão dos riscos e mudanças na supervisão das instituições proporcionou o desenvolvimento de métodos para gerir o risco operacional. Até então, os métodos mais comuns eram lineares, tais como: modelos de séries temporais, modelos econométricos, modelos atuariais empíricos e teoria do valor extremo (Cowell *et al.*, 2007). Devido às limitações de dados e à interação complexa entre variáveis de risco operacional, são propostos vários métodos não lineares capazes de quantificar a exposição ao risco operacional.

O desafio do modelador é, desta forma, incorporar esta contribuição no quadro global de modelação de risco operacional. Verificou-se que a informação qualitativa, tais como decisões de gestão, competências e preferências, pode ser mais bem incorporada num quadro mensurável (e, portanto, qualitativo) utilizando métodos não lineares. Alguns deles incluem

LDA (Modelo de distribuição de perdas), simulação Monte Carlo, *Bayesian Networks*, entre outros, Tabela 2.3 (Cowell *et al*., 2007).

Tabela 2.3 - Métodos de avaliação do risco adaptado de (Assad, 2013; Cowell *et al*., 2007; Gabbay, 2010; Kang, 2015; Peters & Sisson, 2006; Vukovic, 2015)

Métodos	**Descrição**
LDA	O LDA é um método quantitativo amplamente utilizado na gestão do risco operacional. Este método modela a frequência e a gravidade das perdas devidas a eventos de risco operacional. Este método pode ser utilizado para estimar várias medidas de risco, tais como o valor em risco (VaR) para os requisitos de capital para o risco operacional. Ou seja, para estimar as reservas de capital que necessitam de constituir para potenciais perdas operacionais.
Monte Carlo	É um método estatístico utilizado para modelar a probabilidade de diferentes resultados em processos que são difíceis de prever devido à intervenção de variáveis aleatórias. Ao efetuar várias simulações, cada uma com diferentes entradas aleatórias, é possível obter uma distribuição de potenciais resultados. Os métodos de Monte Carlo são frequentemente utilizados em conjunto com o LDA para simular potenciais perdas operacionais. Ao simular vários cenários, as instituições podem obter uma melhor compreensão do intervalo e da probabilidade de perdas potenciais.
Bayesian Networks	As B*ayesian Networks* (BN) são modelos gráficos que representam as relações probabilísticas entre um conjunto de variáveis. São especialmente úteis quando existem interdependências complexas entre diferentes fatores de risco. Em contextos de risco operacional, as *Bayesian Networks* podem ser utilizadas para modelar e compreender as complexas inter-relações entre diferentes fatores de risco, prever a probabilidade de determinados eventos de risco operacional com base em dados observados e atualizar as avaliações de risco à luz de novos dados.

2.5.2.3 Mitigação do risco

Mitigação é essencial para a gestão de risco operacional. As estratégias de mitigação têm o objetivo de reduzir a probabilidade e o impacto dos riscos potenciais e podem ter uma variedade de aplicações de acordo com a natureza do risco e dos recursos e capacidades da empresa (Diehl & Weber, 2014).

Esta etapa permite desenvolver e implementar estratégias de resposta aos riscos identificados e quantificados, de forma a eliminar ou a reduzir os fatores que podem ter uma influência negativa nos objetivos estratégicos. Estas estratégias incluem implementar novos controlos e procedimentos, por exemplo controlos de acesso ou de autorização para prevenir que se realizem ações danosas ou desenvolver planos de contingência em caso de eventos disruptivos.

Para além disso, outro método de mitigação é a transferência de risco para outras empresas ou por outros mecanismos. Transferir para terceiros é útil para riscos difíceis de controlar diretamente, reduzindo o impacto financeiro da perda.

Por fim, estabelecer planos de mitigação de riscos e/ou alocar recursos para áreas de risco importantes para contenção, comunicação e recuperação, que ajudem na diminuição do impacto do evento.

2.5.2.4 Monitorização e reporte do risco

A última fase da avaliação prospetiva consiste em monitorizar continuamente os riscos, para garantir que se mantêm dentro das tolerâncias estabelecidas e avaliar continuamente o desempenho das ações da gestão do risco operacional, bem como as mudanças que possam advir do risco operacional. Para tal, é necessário coletar e reunir dados e informação sobre os eventos e as atividades (Diehl & Weber, 2014).

Adicionalmente, também é importante verificar a efetividade e o funcionamento dos controlos internos impostos e se a empresa está a cumprir a regulamentação aplicável.

Por fim, as principais descobertas dos dados recolhidos devem ser reportadas à gestão sénior e aos diretores, para que possam ajustar a estratégia de risco operacional e tomar as medidas necessárias para tornar a sua gestão o mais eficaz (Deloitte & Vw-Hsg, 2007).

2.5.3 Abordagem Mista

Juntar os modelos anteriormente descritos e optar por uma abordagem mista que permite cumprir a *framework* de gestão de risco operacional, envolve combinar a informação histórica com a análise prospetiva para identificar, analisar e mitigar os riscos operacionais

que podem pôr em causa o funcionamento do negócio, bem como os seus objetivos (Deloitte, 2019).

Por um lado, o modelo misto usa o histórico para identificar e avaliar incidentes passados e "quase-perdas", bem como identificar tendências e padrões que possa indicar futuros riscos. Por outro lado, a utilização de uma análise prospetiva possibilita antecipar potenciais riscos que possam surgir no futuro e, dessa forma, desenvolver estratégias para os mitigar.

A recolha de eventos de perda numa base de dados e o seu estudo vai permitir comparar periodicamente e calibrar os resultados retirados da avaliação do risco. Permite à área de gestão de risco elaborar juízos de valor sobre os controlos impostos e se é necessário alterar a sua estratégia face ao risco operacional (Deloitte, 2019). Para recolher eventos de perda eficazes no processo de calibração.

Adicionalmente, vai permitir priorizar os esforços na gestão e, por sua vez, alocar os seus recursos com maior precisão, ou seja, optar por uma perspetiva mais proativa capaz de perceber a que áreas esses recursos são mais urgentes.

A execução da incorporação das abordagens histórica e prospetiva num modelo híbrido de gestão de risco operacional requer um modelo de governação robusto, suportado por funcionários qualificados e apropriados, capazes de escalar problemas para os órgãos superiores, estabelecer processos de resolução de conflitos e implementar processos de melhoria contínua. A combinação destas duas metodologias pode envolver diferentes equipas e, por isso, a sua comunicação e colaboração é fundamental para o sucesso da gestão.

No entanto, dados históricos podem não ser sempre indicadores fiáveis de futuros riscos e uma análise prospetiva nem sempre é precisa a antecipar os riscos.

2.6 Sistema GRC

Os sistemas GRC (*Governance, Risk, and Compliance*) são essenciais para que as organizações possam gerir eficazmente os riscos operacionais. A importância de um sistema GRC na gestão do risco operacional pode ser compreendida através dos seguintes pontos (AWS, 2023; IBM, 2023):

- **Estrutura integrada**: Fornecem uma estrutura unificada que reúne iniciativas de governação, gestão de risco e conformidade, permitindo uma abordagem holística à gestão do risco operacional.

- **Processos padronizados**: Permitem que a organização padronize metodologias de avaliação de risco, classificações de risco e processos de mitigação, garantindo a consistência entre diferentes departamentos ou unidades de negócios.
- **Melhoria da tomada de decisão**: A gestão de topo e os *stakeholders* podem ter uma visão abrangente dos riscos operacionais, controlos. Os painéis de controlo e relatórios automatizados permitem a monitorização em tempo real e ajudam a tomar decisões estratégicas informadas.
- **Eficiência e produtividade**: A automatização das avaliações de risco, dos testes de controlo e dos processos de monitorização reduz o esforço manual, diminui as possibilidades de erros humanos e aumenta a eficiência e a produtividade globais.
- **Conformidade regulamentar**: Muitas indústrias operam sob diretrizes regulamentares rigorosas. Os sistemas GRC garantem que as empresas estão em conformidade, monitorizando continuamente as alterações nos regulamentos e ajustando as práticas da organização em conformidade.
- **Apetite e tolerância ao risco**: As organizações podem definir e comunicar a sua apetência pelo risco e níveis de tolerância de forma eficaz, assegurando o alinhamento com os objetivos empresariais.
- **Acompanhamento de eventos de perda**: Podem acompanhar e comunicar eventos de perda, ajudando as organizações a compreender as causas de raiz e a tomar medidas corretivas.
- **Gestão de incidentes**: Oferecem ferramentas para registar, gerir e analisar incidentes, facilitando respostas mais rápidas aos riscos operacionais e garantindo uma correção adequada.
- **Gestão de riscos de fornecedores e terceiros**: Muitos sistemas GRC incluem funcionalidades para avaliar e gerir os riscos associados a fornecedores e prestadores de serviços terceiros.
- **Escalabilidade**: À medida que uma organização cresce, os seus riscos operacionais podem tornar-se mais complexos. Os sistemas GRC são escaláveis e podem ser configurados para lidar com o cenário de riscos em constante mudança.
- **Mudança cultural**: A adoção de um sistema GRC pode promover uma cultura consciente dos riscos dentro da organização. Os funcionários tornam-se mais conscientes dos riscos associados às suas ações e da importância de aderir aos controlos e políticas.

- **Poupança de custos**: Ao longo do tempo, um sistema GRC bem implementado pode levar a poupanças de custos, reduzindo os impactos financeiros de perdas operacionais, multas regulamentares e simplificando os processos de gestão de riscos.

Em conclusão, um sistema GRC é vital para as organizações gerirem proactivamente e mitigarem os riscos operacionais de uma forma estruturada, consistente e eficiente. Não só garante que a organização está em conformidade com os regulamentos, mas também fornece uma estrutura para tomar melhores decisões comerciais e promover uma cultura consciente dos riscos.

3

METODOLOGIA DE INVESTIGAÇÃO E A APLICAÇÃO DO CICLO ROCI

O presente capítulo tem o objetivo de fundamentar a aplicação da metodologia de estudo de caso, bem como apresentar as etapas do Ciclo ROCI.

3.1 Metodologia de Investigação: Estudo de Caso

A metodologia de estudo de caso é uma estratégia de investigação utilizada em diversos campos, e os estudos de caso tratam de explorar processos e comportamentos novos ou pouco compreendidos. Logo, esta abordagem é particularmente útil para responder a questões sobre conjuntos de eventos atuais e pertinente (Leonard-Barton, 1990; Meyer, 2016).

Embora, na literatura, seja predominante uma corrente de pensamento que defende a aplicação da metodologia de estudo de caso a eventos de natureza qualitativa, existem autores (Stake, 1998) que defendem que o estudo de caso resulta da combinação de perspetivas qualitativas e quantitativas, mas sempre fundamentado em estratégias qualitativas (Beltran, 2003; Meirinhos & Osório, 2010).

Segundo Yin (2005), a metodologia de investigação de estudo de caso é um método que ainda não está sistematizado, logo as suas características variam de acordo com as abordagens de cada investigador, pelo que este a considera uma metodologia mais abrangente (Meirinhos & Osório, 2010). Podemos então considerar o estudo de caso como a abordagem e análise de um tema no seu contexto real guiado por uma lógica de construção de conhecimento que inclui a subjetividade do investigador, sendo apoiada por múltiplas fontes de evidência, que podem ser qualitativas e quantitativas (Meirinhos & Osório, 2010).

Yin (1993) classifica os estudos de caso relativamente ao seu objetivo de investigação, definindo três classificações de estudos de caso, descritivo, explanatório ou exploratório. Um

estudo de caso descritivo tem como objetivo descrever determinado evento dentro do seu contexto, um estudo de caso explanatório pretende relacionar causas e efeitos, tendo como ponto de partida uma determinada teoria, e um estudo de caso exploratório trata casos sobre os quais se sabe pouco, definindo hipóteses e proposições para trabalhos futuros (Meirinhos & Osório, 2010).

Nesta dissertação conduziu-se um estudo de caso exploratório com o objetivo de aumentar o conhecimento na área de avaliação do sistema de gestão de risco operacional e controlo interno, no contexto de uma empresa seguradora a operar no mercado Português. Esta investigação é apoiada em fontes de evidências qualitativas e quantitativas, suportadas na teoria revista no Capítulo 2 e adaptada à realidade em estudo, com dados concretos e envolvendo fontes quantitativas acerca de riscos, processos e controlos existentes. Para tal, aplicou-se o Ciclo ROCI (Risco Operacional e Controlo Interno) para garantir o cumprimento da *Framework* de gestão de Risco Operacional.

3.2 Ciclo ROCI

O Ciclo ROCI é um método para documentar e avaliar os sistemas de gestão de risco operacional e controlo interno. Por outro lado, permite consciencializar e sensibilizar os colaboradores sobre a cultura de gestão de risco

Este processo envolve o contacto e a colaboração das áreas em estudo na recolha de informação descritiva, qualitativa e quantitativa dos seus processos, riscos e controlos. Deste modo, elaboraram-se sessões entre a equipa de gestão de risco operacional e a unidade de negócio que pretende avaliar a sua exposição ao risco. Com estas sessões, pretende-se desenvolver as etapas que vão descritas posteriormente.

A 2º linha de defesa (equipa de gestão de risco) tem a função de dar apoio à 1ª linha de apoio (área de negócio) na componente metodológica e de registo no sistema GRC, sendo estes, últimos, responsáveis pelos resultados obtidos e pela sua manutenção.

De acordo com a Figura 3.1, o Ciclo ROCI é constituído pelas seguintes etapas:

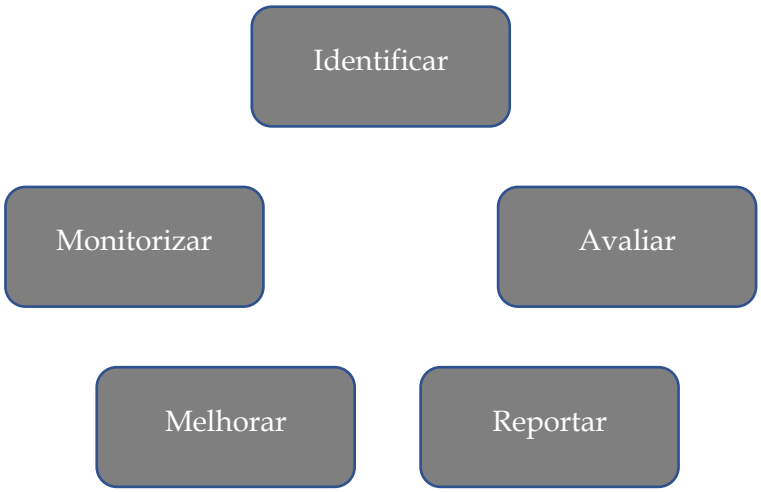


Figura 3.1 - Ciclo ROCI

3.2.1 Identificar

Esta etapa é responsabilidade da área de negócio com suporte da equipa de gestão de risco operacional identificam e documentam os processos, riscos inerentes e controlos utilizados para perceber e reduzir a exposição ao risco nessa área.

A documentação de todos os processos de negócio da Companhia é efetuada considerando uma "árvore" de processos pré-definida de três níveis (macroprocesso; processo; subprocesso), que representam as atividades de todas as áreas de negócio. A documentação e atualização dos processos de negócio das Companhias são um requisito aos sistemas de gestão de risco e controlo interno.

Para realizar este estudo são realizadas diversas reuniões entre a equipa de gestão de risco operacional e as várias áreas de negócio. Caso a unidade em estudo já tenha sido documentada, é feita uma revisão das atividades, dos riscos inerentes e dos controlos utilizados para a sua mitigação.

Este trabalho é realizado pela 2ª linha de defesa. Inicialmente, a equipa de risco operacional elabora um Excel, que é enviado à primeira linha de defesa para ser analisado. Na elaboração deste documento, constam os diversos processos, riscos, controlos e evidências, que possuem relações e dependências entre si. Estes objetos são extraídos a partir de listas, que estão disponíveis na plataforma GRC. Os riscos estão ligados aos processos, os controlos aos riscos e as evidências dos controlos aos controlos.

Ao longo de várias sessões, a área em estudo vai fazendo as retificações necessárias até se documentar as suas atividades e respetivas funções. No final, a 2ª linha de defesa faz as alterações em sistema para que se tenha a documentação mais atualizada.

3.2.2 Avaliar

Após a etapa identificar, prossegue-se para a avaliação dos riscos, onde a 1ª linha de apoio efetua a avaliação da exposição dos seus riscos, da qualidade do seu ambiente de controlo, e da adequação das medidas de mitigação existentes (atividades de controlo) com o apoio da equipa de risco operacional.

Deste modo, a 2ª linha de defesa providencia os questionários, onde a avaliação será realizada e fornece suporte no seu preenchimento. A avaliação dos riscos é quantitativa, tendo por base a frequência e a severidade de futuras perdas operacionais. Enquanto, o ambiente de controlo é qualitativa e pretende avaliar a perceção global da mitigação do risco tendo em conta fatores subjetivos que vão para além dos mecanismos de controlo formalmente implementados. As atividades de controlo também são avaliadas qualitativamente. A sua avaliação pretende avaliar a eficácia dos mecanismos de controlo formalmente implementados na mitigação do risco, a sua execução, e a manutenção de evidência.

Os questionários elaborados são referentes aos riscos e aos controlos. Existe um questionário para os riscos, que vai servir como base para calcular o VaR de cada risco. O cálculo do VaR é determinado com base num modelo estatístico suportado pelas respostas aos questionários pela 1ª linha de defesa. Nesta fase, a 1ª linha de defesa avalia a efetividade do ambiente de controlo, a frequência e a severidade dos diversos riscos em análise. O risco pode ser classificado nas seguintes categorias:

- **Risco Material com Avaliação**: Risco que permite determinar a perda a que a companhia está exposta.
- **Risco Imaterial**: Risco que não tem qualquer perda para a empresa.
- **Risco Material sem Avaliação**: Risco em que se sabe que uma perda pode ser materializada, mas não é possível determinar, pois não se sabe a frequência ou a severidade do mesmo.

Em relação aos questionários de controlo existem 2 tipos: questionário de controlo e questionário de controlo e evidências. A diferença entre cada um é se as evidências dos controlos são mantidas pela área que executa o controlo ou são mantidas por outra(s) área(s). Estes questionários de controlo avaliam o seguinte:

- **Execução do Controlo**: Perceção dos trabalhadores de como a sua experiência e envolvimento na realização das suas atividades podem contribuir para mitigar o risco implícito.

- **Eficácia do Controlo**: avaliação do nível de mitigação que os controlos têm, quando reduzem os riscos.

3.2.3 Reportar

Nesta fase, a 2ª linha de defesa reporta à 1ª linha de defesa e órgãos de administração os resultados e as conclusões retiradas nas fases anteriores, bem como as oportunidades de melhoria identificadas.

Desta forma, a equipa de risco operacional elabora relatórios com informações relevantes sobre as áreas de negócio, que são retiradas, a partir de *dashboards* do sistema GRC. Por sua vez, é feita uma apresentação, onde se expõe às unidades os resultados determinados e, possíveis oportunidades de melhoria, de modo a mitigar os riscos e a fortalecer os controlos implementados, de modo, a reforçar os sistemas de gestão de risco.

3.2.4 Melhorar

Após o reporte de oportunidades de melhoria por parte da 2ª linha de defesa, a 1ª linha de defesa vai avaliar a viabilidade e benefício na sua implementação, sempre com o apoio necessário da 2ª linha de defesa.

Esta etapa pretende que este estudo seja sempre contínuo, de modo que haja uma melhoria contínua dos sistemas de gestão de risco operacional e controlo interno. Desta maneira, pretende-se que a 1ª linha de defesa identifique oportunidades de melhoria, continuamente e que proceda à sua implementação, sempre que se seja justificado.

Só a melhoria contínua dos sistemas de gestão de risco operacional e controlo interno permite à Companhia reduzir a sua exposição ao risco operacional e a tornar os seus sistemas de gestão do risco operacional e controlo interno mais robustos, garantindo a proteção dos seus *stakeholders.*

Após a viabilização da oportunidade de melhoria, esta é carregada no sistema GRC e a sua implementação monitorizada pela 2ª linha de defesa.

3.2.5 Monitorizar

A monitorização é imprescindível na identificação de falhas nos sistemas de gestão de risco operacional e controlo interno, funcionando, muitas vezes, como um alerta atempado a novas exposições.

Existem 3 mecanismos, que ajudam a etapa da monitorização:

- Registo de eventos de risco operacional;
- Indicadores Chave de Risco (KRIs);

- Monitorização de melhorias.

3.2.5.1 Eventos de Risco Operacional

O registo de eventos de risco operacional é um dos mecanismos mais importantes para a monitorização da adequação dos seus sistemas de gestão de risco operacional e controlo interno, o que permite a deteção de falhas sucessivas e inequívocas. Permite detetar riscos não identificados, reavaliar um risco quando as perdas ultrapassam de forma significativa o número esperado de ocorrências e/ou o impacto financeiro estimado e identificar fragilidades no sistema de controlo interno, bem como oportunidades de melhoria.

O registo de eventos de risco operacional é o processo pelo qual a 1ª linha de defesa reporta a ocorrência de eventos de perda direta ou indireta, quantificável, ainda que apurada de forma estimada ou potencial, resultante de falhas internas (procedimentos, pessoas ou sistemas) ou eventos de natureza externa (por exemplo: serviços de outsourcing, ações da natureza, vandalismo, fraude).

De acordo com a Figura 3.2, este mecanismo é constituído pelo seguinte:

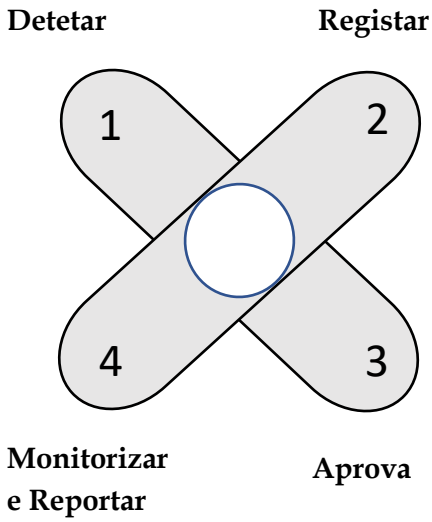


Figura 3.2 - Etapas de Eventos de Risco Operacional

- **Detetar**: A deteção de eventos de risco operacional é uma responsabilidade de todos os colaboradores. É também responsabilidade de todos os colaboradores, após a deteção de um evento de risco operacional, sempre que possível, tomar todas as ações que estejam disponíveis no seu campo de ação no sentido de minimizar, ou se possível recuperar, a perda financeira decorrente do evento.

- **Registar**: O registo de eventos de risco operacional é uma responsabilidade de todos os colaboradores, devendo quem detetou, salvo se outro procedimento estiver estabelecido, registar o evento no sistema de GRC da Companhia, podendo sempre que necessário solicitar apoio à 2ª linha de defesa. A quem regista eventos de risco operacional no sistema de GRC da Companhia não é exigida a caracterização completa do evento, sempre que a mesma não seja do seu conhecimento. Compete à 2ª linha de defesa proceder às ações necessárias à obtenção da caracterização completa do evento de forma a possibilitar a sua aprovação.
- **Aprovar**: A validação e aprovação da caracterização do evento de risco operacional no sistema de GRC da Companhia é da responsabilidade da 1ª linha de defesa, nomeadamente a área exposta ao risco presente no evento, devendo sempre que necessário solicitar apoio à 2ª linha de defesa no sentido de obter as condições necessárias à aprovação do evento.
- **Monitorizar e Reportar**: Cabe à 2ª linha de defesa a responsabilidade de monitorizar o registo de eventos de risco operacional e reportar regularmente à 1ª linha de defesa e órgãos de administração qualquer evento ou conjunto de eventos que considere relevante para a garantia da adequação dos sistemas de gestão do risco operacional e controlo interno da Companhia.

3.2.5.2 KRIs

Os indicadores chave de risco (KRIs) é um mecanismo que permite alertar a 1ª linha de defesa de forma imediata para um possível aumento da exposição ao risco, sendo possível agir em conformidade na sua mitigação. A 1ª linha de defesa tem o dever de identificar os indicadores chave de risco relevantes para monitorizar o risco da sua atividade, uma vez que as atividades variam de unidade para unidade e, por sua vez, os sistemas de risco operacional e controlo interno.

Compete à 2ª linha de defesa apoiar a 1ª linha de defesa na implementação e operacionalização dos indicadores chave de risco identificados no sistema de GRC da Companhia.

3.2.5.3 Monitorização de melhorias

A monitorização das oportunidades de melhoria é um mecanismo de melhoria contínua, que permite monitorizar a aplicabilidade e analisar os impactos esperados e adversos na implementação de uma oportunidade.

Compete à 1ª linha de defesa ser responsável verificar a eficácia das medidas implementadas com o apoio da 2ª linha de defesa.

4

ESTUDO DE CASO

No presente capítulo é caracterizado o contexto em que a presente dissertação foi desenvolvida com especial ênfase às práticas de gestão de risco operacional realizadas na Fidelidade – Companhia de Seguros, S.A. Através da realização de um estágio curricular no âmbito foi possível adquirir conhecimentos relativos a esta área.

O presente capítulo pretende dar uma breve apresentação da empresa, o funcionamento da Departamento de Gestão de Risco Operacional (DGRO) e o conjunto de atividades realizadas desde a identificação à monitorização para reduzir a exposição da empresa ao risco.

Após o desenvolvimento realizado nos capítulos anteriores, é fundamental perceber o enquadramento prático do risco operacional numa empresa e os sistemas de gestão utilizados, bem como os métodos que são utilizados no seu controlo. Para entender melhor a gestão do risco operacional, foi realizado um estágio na empresa Fidelidade. Assim, foi possível ter uma visão mais concreta dos processos utilizados para efetuar uma gestão eficaz.

4.1 Apresentação da Empresa

A Fidelidade – Companhia de Seguros, S.A. foi fundada em 1808, com sede em Lisboa, Portugal. É uma sociedade anónima, resultante da fusão das seguintes empresas: Fidelidade, Mundial Confiança, Império e Bonança, com lançamento da marca única Fidelidade em 2013.

Em 2014, o Grupo Fidelidade foi privatizado e adquirido pelo Grupo Fosun, iniciando uma nova etapa marcada pela consolidação da liderança em Portugal e pela expansão internacional. O Grupo Fosun detém 84,99% do portfolio, através da Longrun Portugal, SGPS, S.A., a Caixa Geral de Depósitos, S.A. (CGD) detém 15,00% e o restante é detido por colaboradores e ações próprias.

O Grupo Fidelidade, em Portugal, é composto pelas seguintes companhias: Fidelidade, Multicare, Fidelidade Assistência, Via Directa, Companhia Portuguesa dos resseguros (anexo

B). No mercado internacional atua através de sucursais – em Espanha e França – e através de empresas subsidiárias – Fidelidade Angola, Fidelidade Moçambique, Garantia Cabo Verde, Fidelidade Macau, La Positiva (Perú), Alianza (Bolívia), Alianza Garantia (Paraguai) e Fid Chile.

O Grupo Fidelidade disponibiliza uma vasta gama de produtos e serviços aos seus clientes, que resulta de uma sólida experiência e constante aposta na diversificação e inovação. Desta forma, tem vindo a desenvolver uma oferta integral no negócio segurador, mas também a reafirmar o seu propósito de se posicionar, cada vez mais, como um parceiro dos seus clientes na prestação de serviços de proteção e assistência.

No âmbito do negócio segurador, o Grupo Fidelidade tem uma oferta alargada de produtos, que abrangem a generalidade dos ramos Vida e Não-Vida, desde seguros automóveis, multirriscos (habitação, incêndios), saúde, acidentes de trabalho, Vida Financeiro (produtos de poupança com diferentes maturidades e objetivos), entre outros produtos. Através das empresas do Grupo são prestados também serviços em diversas áreas como a Saúde, Assistência, Imobiliário, Gestão de Ativos, Peritagens e Reparação Automóvel.

4.2 Sistemas de Governação de Risco Operacional

Como mencionado nos capítulos anteriores, fazer uma gestão quantitativa do risco operacional não é suficiente para controlar este risco tão extenso e complexo. Então, a Fidelidade opta por também realizar uma gestão mais qualitativa, onde pretende conhecer melhor o risco e perceber a sua origem e possíveis consequências se não tentarem reduzir a sua exposição.

A companhia possui uma direção somente direcionada para o tratamento do risco operacional, denominada de Departamento de Gestão de Risco Operacional (DGRO).

A gestão do risco operacional visa:

- Identificar e monitorizar os riscos a que a empresa está ou possa vir a estar exposta, sejam estes de natureza interna ou externa;
- A implementação de um sistema de controlo interno eficaz e eficiente que auxilie na mitigação de riscos e na redução das perdas decorrentes para a Companhia;
- O tratamento de eventos de risco operacional, incluindo também o registo, reporte e monitorização dos mesmos;
- Fornecer à gestão de topo informação de suporte à tomada de decisão e à implementação de melhorias.

Através destes processos, a Companhia vê o seu sistema de gestão do risco operacional mais robusto, proporcionando uma imagem mais próxima da realidade no que diz respeito à sua exposição ao risco operacional.

Para tal, a *framework* de gestão de risco operacional baseia-se em 4 premissas importantes, Tabela 4.1.

Tabela 4.1 - *Framework* de Gestão de Risco Operacional

Premissas	Descrição
Conhecer os riscos e a sua mitigação	Para qualquer sistema de gestão de risco é fundamental conhecer os riscos a que a organização se encontra exposta e a forma como os mesmos são mitigados. Esta premissa é a base fundamental de qualquer sistema de gestão de risco operacional e controlo interno.
Conhecer as fraquezas	A identificação das fragilidades dos sistemas de gestão de risco operacional e controlo interno, permite à organização focar-se nas situações mais críticas, identificar oportunidades de melhoria significativas e preparar-se de forma defensiva e reativa contra possíveis ameaças.
Melhoria Contínua	Através da implementação da melhoria contínua nos seus processos de negócio, a organização procura diminuir o nível de exposição aos riscos operacionais, nomeadamente através da redução da frequência e/ou severidade de futuras perdas financeiras. A melhoria contínua permite à organização preparar-se melhor para a evolução da exposição dos riscos atuais e futuros.
Monitorização	Por fim, a monitorização permite avaliar a adequação das 3 primeiras premissas dos sistemas de gestão de risco operacional e controlo interno.

Cumprir as premissas descritas acima é essencial para a obtenção de sistemas de gestão de risco operacional e controlo interno completos, eficazes e eficientes.

4.2.1 Modelo de Governação

A gestão de risco operacional pretende identificar e monitorizar os riscos a que a empresa está exposta. A função de gestão de riscos deve ter um papel preponderante na implementação de sistemas de gestão de risco. Deste modo, segundo o Regulamento Delegado (UE) 2015/35, a sua função deve contemplar as seguintes responsabilidades:

- a assistência à Comissão Executiva e outras funções que possam ser relevantes no âmbito do funcionamento eficaz do sistema de gestão de riscos;
- a monitorização do sistema de gestão de riscos;
- a monitorização do perfil de risco geral da empresa como um todo;
- a comunicação de informações pormenorizadas sobre exposições ao risco e aconselhamento à Comissão Executiva em matéria de gestão de riscos, incluindo questões estratégicas, como a estratégia empresarial, fusões e aquisições e grandes projetos e investimentos;
- a identificação e avaliação dos riscos emergentes.

Também é importante cooperar estreitamente com a função atuarial, mesmo sabendo que têm funções independentes entre si.

4.2.1.1 Modelo de 3 linhas de defesa

O sistema de gestão de risco operacional assenta no modelo de governação das 3 linhas de defesa.

- **1ª linha de defesa**: Esta linha é composta pelas Áreas de Negócio, tendo a função de identificar, documentar, avaliar e mitigar os riscos da atividade. De modo, a resolver as deficiências no sistema de controlo interno devem ser implementadas as medidas de mitigação adequadas e as ações corretivas necessárias ao risco operacional da Companhia. Por sua vez, cada área tem a responsabilidade de eleger um representante dos temas de risco operacional, denominado de Focal Point, colaborando diretamente com a 2ª linha de defesa.
- **2ª linha de defesa**: A Função de Gestão de risco, nomeadamente a DGRO, é considerada a 2ª linha de apoio. Tem a responsabilidade de apoiar a 1ª linha de defesa e, por isso, de monitorizar e controlar que as atividades propostas à 1ª linha de defesa são executadas e auferem a qualidade necessária. Assim, garantir que a 1ª linha de defesa identifica, avalia e reporta corretamente os riscos da sua atividade e a adequação do sistema de controlo.

- **3ª linha de defesa**: É constituída pela Função de Auditoria Interna. Esta deve rever de modo sistemático e eficiente as atividades das duas primeiras linhas de defesa e contribuir para a sua melhoria contínua. As suas funções são realizadas de forma independente e assegura que as duas primeiras linhas de defesa executam os seus objetivos tal como foram propostas.

4.2.2 Política de Gestão de Risco Operacional

A Política de Gestão de Risco Operacional é aplicada à Fidelidade - Companhia de Seguros S.A. e a todas as empresas de seguros e resseguros do Grupo, cuja atividade se exerça sob regime de Solvência II, enquadrando-se segundo os Artigos 41º - Requisitos gerais em matéria de governação, 44º - Gestão de Riscos, 46º - Controlo Interno e 246º - Supervisão do sistema de governação das empresas. Enquanto as restantes empresas de seguros e de resseguros do Grupo regem-se sob as políticas a adotar em relação ao risco operacional, definidas pela *International Governance Policy*.

Para além disso, também se encontra regida em consonância com a legislação vigente no Regulamento Delegado (UE) 2015/35, concretamente no Artigo 266o - Sistema de Controlo Interno, e com as Orientações relativas ao sistema de governação EIOPA-BoS-14/253, nomeadamente a Orientação 21 - Política de gestão do risco operacional (secção 4), a Orientação 38 - Ambiente de controlo interno e a Orientação 39 - Monitorização e prestação de informação.

A Política tem o objetivo de consciencializar as áreas e os seus colaboradores sobre os potenciais riscos operacionais que possam ter inerentes às suas atividades, bem como os seus respetivos controlos. Assim, mostrar que esta identificação é benéfica para uma gestão mais eficiente dos processos e dos recursos da empresa.

Em relação ao risco operacional, esta política abrange o seguinte:

- A identificação dos riscos operacionais a que a empresa está ou poderá estar exposta e avaliação das suas formas de mitigação e/ou controlo;
- A identificação dos processos/atividades para a gestão do risco;
- A identificação, análise e reporte de eventos de risco operacional;
- A definição de limites de tolerância ao risco;
- A elaboração de análises baseadas em cenários.

A definição dos limites de tolerância ao risco da empresa e de análises baseadas em cenários permite à Fidelidade - Companhia de Seguros S.A estabelecer os mecanismos necessários para fornecer um nível de segurança aceitável à Comissão Executiva de forma a não inviabilizar o cumprimento dos seus objetivos estratégicos.

4.2.3 Funções e Responsabilidades

Apresentam-se de seguida, as principais funções e responsabilidades por linha de defesa e respetivos intervenientes, Tabela 4.2.

Tabela 4.2 - Funções e Responsabilidades

	Responsabilidades				
	1ª Linha de defesa				2ª Linha de defesa
Atividades	Todos os colaboradores	Aprovadores de eventos de risco operacional	*Focal Point*	Diretor de 1ªlinha	DGRO
Gestão documental dos sistemas de gestão de risco operacional e controlo interno	●		●	●	●
Avaliação da exposição ao risco operacional	●		●	●	●
Deteção de eventos de risco operacional	●				
Registo de eventos de risco operacional	●		●		●
Validação/aprovação de eventos de risco operacional		●	●		●
Melhorias nos sistemas de gestão de risco operacional e controlo interno	●		●	●	●
Reporte dos sistemas de gestão de risco operacional e controlo interno				●	●

● Aprova ● Ratifica ● Apoia ● Executa

4.2.3.1 *Focal Point*

O *Focal Point* é o interlocutor na comunicação entre as duas primeiras linhas de defesa. É eleito um representante por cada área de negócio. Este representante tem a função de

facilitador na manutenção dos sistemas de gestão de risco operacional e controlo interno da sua unidade de negócio, funcionando "quase como um mediador". Sendo sempre apoiado pela 2ª linha de defesa no cumprimento das suas responsabilidades.

4.2.3.2 Aprovador de eventos de risco operacional

Para além da designação de um *Focal Point*, também se designa um aprovador de eventos. Este tem o objetivo de validar e completar a caracterização de eventos com impacto na sua unidade de negócio, bem como proceder à sua aprovação no sistema de GRC designado para o efeito. Sempre que for necessário, deve solicitar apoio ao *Focal Point* da sua área de negócio ou à 2ª linha de defesa.

Todas as unidades de negócio deverão possuir aprovadores definidos no sistema de GRC da Companhia. Compete à direção de gestão de risco operacional realizar a gestão dos aprovadores de eventos de risco operacional.

4.3 Requisito de Capital de Solvência Operacional

O Grupo Fidelidade aplica a fórmula-padrão para calcular o requisito de capital de Solvência (SCR), não aplicando qualquer modelo interno. A Figura 4.1 representa a variação do requisito de capital para o risco operacional desde 2017. Só a partir de 2021, é que se começou a divulgar o SCRop para o Grupo Consolidado, até então era só individualmente para a Fidelidade.

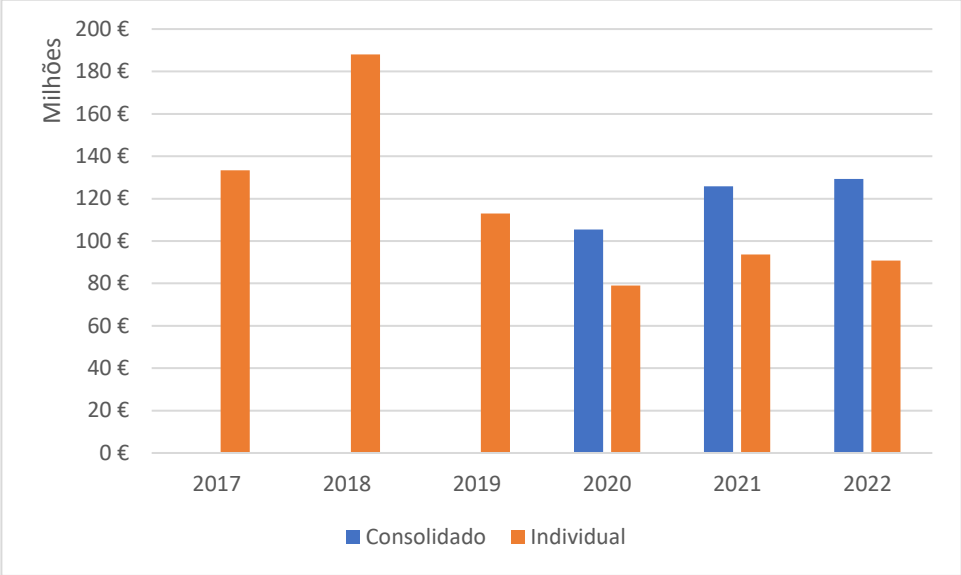


Figura 4.1 - Requisito de Capital de Solvência Operacional

4.4 Aplicação do Ciclo ROCI

A realização deste estudo teve por base o trabalho desenvolvido na Fidelidade, através da aplicação do Ciclo ROCI. Iniciou-se com a realização de um estágio, que permitiu compreender o processo, desde a fase de identificação à fase de monitorização do risco.

Deste modo, através de workshops de auscultação das diversas áreas em estudo, realizou-se um levantamento dos principais processos dessas áreas e dos riscos associados à realização dessas atividades. Para tal, foi necessário o apoio dos responsáveis de cada área.

Após este mapeamento inicial, avaliou-se os riscos e os controlos associados para determinar o VaR (*Value-at-Risk*) e eficácia dos mecanismos de controlo, respetivamente. De seguida, analisou-se a exposição da empresa ao risco e que medidas de melhoria foram necessárias tomar.

4.4.1 Caracterização da amostra

A determinação da exposição da empresa ao risco operacional teve como base uma amostra de 17 áreas de negócio da Fidelidade Espanha (anexo F). Na Tabela 4.3, é possível visualizar os subprocessos e os riscos materiais por unidade de negócio. Adicionalmente, também se pode observar exposição do risco mais alto por área, bem como a exposição acumulada.

Tabela 4.3 - Exposição das áreas

Área	Subprocessos	Riscos materiais com avaliação	Riscos materiais sem avaliação	VaR mais alto	VaR acumulado
A1	10	1	6	253 €	253 €
A2	8	1	7	1 282 €	1 282 €
A3	7	8	5	41 430 €	168 832 €
A4	14	4	0	170 968 €	228 700 €
A5	11	22	3	44 119 €	291 324 €
A6	8	3	32	1 427 €	3 396 €
A7	9	1	8	3 944 €	3 944 €
A8	8	0	15	- €	- €
A9	8	0	18	- €	- €
A10	6	8	5	225 520 €	638 264 €
A11	17	8	7	1 175 €	4 368 €
A12	7	1	14	2 695 €	2 695 €
A13	12	5	49	66 930 €	158 885 €
A14	10	20	0	949 906 €	1 938 700 €
A15	5	1	10	5 906,00 €	5 906 €
A16	3	0	1	- €	- €
A17	4	0	13	- €	- €
Total	**147**	**83**	**193**		**3 446 544 €**

4.4.2 Processos

De acordo com a Tabela 4.4, foram identificados os principais macroprocessos e subprocessos de negócio, bem como a quantidade de riscos associados a cada macroprocesso. Analisaram-se 12 macroprocessos com 147 subprocessos de negócio. Foram identificados 414 riscos, dos quais 81 são relacionados com "Vendas", 72 com "Contabilidade" e 56 com "Governação", que representam cerca de 50% dos riscos identificados.

Tabela 4.4 - Exposição dos Macroprocessos

Macroprocessos	Subprocessos	Riscos	VaR acumulado
Vendas	28	81	78 501 €
Resseguro	4	12	594 430 €
Cobranças	8	13	134 405 €
Sinistros	14	39	1 845 850 €
Investimentos	1	5	0 €
Contabilidade	12	72	7 678 €
Gestão de Recursos	23	35	174 512 €
Processos complementares	14	34	380 821 €

Macroprocessos	Subprocessos	Riscos	VaR acumulado
Processos transversais	14	34	47 327 €
Governação	19	56	183 020 €
Funções Chave	8	33	0 €
Sistemas de Informação	2	0	0 €
Total	**147**	**414**	**3 446 544 €**

Para além disso, foi possível verificar o VaR acumulado de cada macroprocesso, excluindo os riscos que apresentam um VaR superior a 1M, com um valor total de 3 446 544 €, em que os macroprocessos "Investimentos", "Funções Chave" e "Sistemas de Informação não apresentam VaR. A Figura 4.2 representa a distribuição dos riscos por macroprocesso.

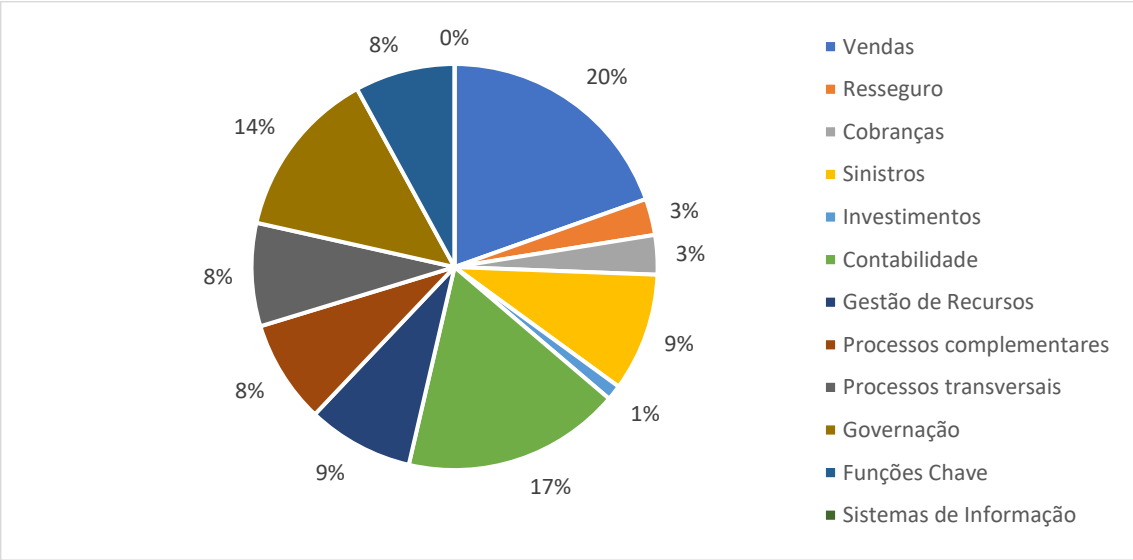


Figura 4.2 - Distribuição dos Riscos por macroprocesso

A Tabela 4.5 enumera a quantidade de riscos associados aos macroprocessos, categorizados por riscos materiais e imateriais, que representam 279 e 135 riscos, respetivamente. Os Riscos materiais são compostos pelos riscos materiais sem avaliação, riscos materiais com avaliação e riscos materiais com VaR superior a 1M. Dos 414 riscos, apenas 86 tiveram a sua exposição avaliada.

Tabela 4.5 - Distribuição dos Riscos por Macroprocesso

Macroprocessos	Riscos	Riscos materiais	Riscos sem avaliação	Riscos com avaliação	Riscos VaR>1M	Riscos imateriais
Vendas	81	79	69	10	0	2
Resseguro	12	9	3	6	0	3
Cobranças	13	13	7	6	0	0
Sinistros	39	34	14	17	3	5
Investimentos	5	1	1	0	0	4
Contabilidade	72	40	35	5	0	32
Gestão de Recursos	35	17	5	12	0	18
Processos complementares	34	23	1	22	0	11
Processos transversais	34	21	18	3	0	13
Governação	56	20	18	2	0	36
Funções Chave	33	22	22	0	0	11
Sistemas de Informação	0	0	0	0	0	0
Total	**414**	**279**	**193**	**83**	**3**	**135**

A Tabela 4.6 lista a descrição de 3 riscos com um VaR superior a 1 milhão de euros, que face à sua dimensão são analisados individualmente. Por sua vez, estes riscos estão relacionados com o macroprocesso "Sinistros", desde a sua Abertura ao Encerramento. Por fim, estão referidos os níveis dos ambientes de controlo (avaliação qualitativa ao risco), bem como a área onde foram identificados.

Tabela 4.6 - Riscos com VaR superior a 1M

Área	Processo	Risco	Ambiente de Controlo
A14	04.01.02. Abertura de processos de sinistros	1.2.2 Falhas na aceitação de assistências	Médio Alto
A14	04.01.03. Gestão de processos de sinistros	4.1.1 Fraude externa	Médio
A14	04.01.04. Encerramento de processo de sinistros	4.1.1 Fraude externa	Médio

A Tabela 4.7 lista todos os riscos que possuem um evento de risco operacional, bem como os processos e áreas onde ocorreram.

Tabela 4.7 - Correlação Eventos de Risco Operacional e Riscos Operacionais

Área	Processo	Risco	Evento de Risco Operacional	Ambiente de Controlo
A13	01.01.03 Gestão de produtos	3.6.3 Falhas na execução das operações	Erro no ficheiro dos ativos do PIAS.	Médio Alto
A14	04.02.01 Pagamentos a sinistrados/ tomadores/ lesados	3.6.2 Falhas nos pagamentos ou liquidações	Ordem de pagamento com erro no destinatário	Médio
A12	04.02.01 Pagamentos a sinistrados/ tomadores/ lesados	3.6.2 Falhas nos pagamentos ou liquidações	Pagamento a uma entidade incorreta	Alto
A11	06.02.01 Pagamentos	3.6.3 Falhas na execução das operações	Devolução incorreta de recibo na transferência PIAS OUT	Alto
A11	06.02.01 Pagamentos	3.4.2 Falhas no fornecimento de bens e serviços	Destinatário do pagamento errado	N/A
A6	06.02.01 Pagamentos	3.5.1 Falhas no desempenho de contrapartes	Pagamento em duplicado do banco	N/A
A6	06.02.01 Pagamentos	3.6.2 Falhas nos pagamentos ou liquidações	-Montante transferido para uma conta incorreta; -Pagamento em duplicado ACENS - retrocessão recusada; -Registo da mesma fatura duas vezes por ter sido registada com caracteres diferentes; -Recibo bancário não processado - PIAS; -Recibos pagos em duplicado	Alto
A6	06.03.01 Obrigações fiscais	3.6.8 Erros de registo ou afetação contabilística	Cancelamento de erros NRC 2023-01	Alto
A5	08.05.03 Faturação de prestadores/ fornecedores	3.6.3 Falhas na execução das operações	Incumprimento do procedimento - Faturas pagas por Avda. América de +8000€ para o período de junho a Set. 2021 sem assinatura do Diretor Geral	Alto
A5	08.05.03 Faturação de prestadores/ fornecedores	3.7.2 Falhas na prestação de serviços de serviços subcontratados	Fornecedor cobra valor superior ao correto	Alto

Na Tabela 4.8, é possível observar os impactos máximo e líquido e o valor de perda dos eventos de perda recolhidos, bem como comparar com o VaR calculado para cada risco associado. O evento "Montante transferido para uma conta incorreta; Pagamento em duplicado ACENS - retrocessão recusada; Registo da mesma fatura duas vezes por ter sido registada com caracteres diferentes; Recibo bancário não processado - PIAS; Recibos pagos em duplicado" apresenta um impacto líquido semelhante ao VaR, 1332,60€ e 1427,00€, respetivamente.

Tabela 4.8 - Impacto dos Eventos de Risco Operacional

Risco	VaR do Risco	Impacto Máximo	Valor da perda	Impacto Líquido	Tipo de Perda
3.6.3 Falhas na execução das operações	7 470,00 €	2 000,00 €	0,00 €	0,00 €	Quase-perda
3.6.2 Falhas nos pagamentos ou liquidações	167 168,00 €	855,09 €	855,09 €	0,00 €	Recuperação
3.6.2 Falhas nos pagamentos ou liquidações	Sem avaliação	90,75 €	90,75 €	90,75 €	Perda
3.6.3 Falhas na execução das operações	339,00 €	120,00 €	120,00 €	0,00 €	Recuperação
3.4.2 Falhas no fornecimento de bens e serviços	Risco identificado no Evento de perda	40 122,59 €	40 122,59 €	0,00 €	Recuperação
3.5.1 Falhas no desempenho de contrapartes	Risco identificado no Evento de perda	153,04 €	153,04 €	0,00 €	Recuperação
3.6.2 Falhas nos pagamentos ou liquidações	1427,00 €	2 480,56 €	2 480,56 €	1 332,60 €	Perda
3.6.8 Erros de registo ou afetação contabilística	Sem avaliação	19 209,61 €	19 209,61 €	0,00 €	Recuperação
3.6.3 Falhas na execução das operações	12 956,00 €	0,00 €	0,00 €	0,00 €	N/A
3.7.2 Falhas na prestação de serviços de serviços subcontratados	5 634,00 €	43,38 €	43,38 €	0,00 €	Recuperação
Total	**194 994,00 €**	**65 075,02 €**	**63 075,02 €**	**1 423,35 €**	

4.4.3 Controlos Internos

Para complementar a identificação e avaliação do risco, procedeu-se à identificação dos controlos, que possibilitam mitigar o risco e, por sua vez, promover um sistema de gestão robusto. A Tabela 4.9 demonstra a quantidade de controlos em uso, dos quais 185 são manuais e 19 são relativos a sistemas aplicativos. Por outro lado, na Tabela 4.10, pode-se observar a caracterização dos 204 controlos em detetivos ou preventivos.

Tabela 4.9 - Natureza dos controlos

Natureza	Controlos
Manuais	185
Aplicacionais	19
Total	**204**

Tabela 4.10 - Caracterização dos controlos

Caracterização	Controlos
Detetivo	112
Preventivo	92
Total	**204**

Na Tabela 4.11 e na Tabela 4.12, estão mencionadas as tipologias dos controlos. Os controlos manuais estão divididos em próprios (controlos de uma área aplicados nessa mesma área) e em terceiros (controlos de uma área aplicados a outra área). É de salientar que o controlo "validação pelos colaboradores" representa cerca de 44% dos controlos.

Tabela 4.11 - Controlos Manuais

Controlos Manuais	Próprios	Terceiros
Validação pelos colaboradores	89	1
Análise periódica	37	0
Reconciliação	18	0
Autorização de Operações	16	0
Segregação de funções	9	0
Outras tipologias	15	0
Total	**184**	**1**

Tabela 4.12 - Controlos Aplicacionais

Controlos Aplicacionais	#
Alertas de Sistema	8
Restrições de Sistema	8

Controlos Aplicacionais	#
Perfis de Acessos	3
Total	**19**

Foram estudados os controlos que apresentavam deficiências a nível de execução, eficácia e evidência, onde se identificaram 49, anexo D. A Tabela 4.13 expressa a quantidade de controlos com falhas de execução, eficácia e evidência, 7, 30 e 21, respetivamente. A Tabela 4.14 enumera a natureza dos controlos com deficiências. Adicionalmente, identificaram-se que 15 áreas possuem controlos com deficiências, Tabela 4.15.

Tabela 4.13 - Controlos com deficiências na Execução, Eficácia e Evidência

	Controlos com deficiências
Execução	7
Eficácia	30
Evidência	21

Tabela 4.14 - Natureza dos controlos com deficiências

Tipo	Controlos com deficiências
Manual	46
Automático	3

Tabela 4.15 - Áreas com controlos com deficiências

Área	Controlos com deficiências
A3	2
A11	11
A12	3
A14	8
A10	2
A8	4
A5	1
A4	4
A7	1
A2	3
A6	1
A15	3
A13	2
A3	2

Na Tabela 4.16, é possível verificar-se os riscos materiais que não possuem controlos. É de salientar que, apesar de os riscos não possuírem controlos, as áreas atribuem uma avaliação qualitativa em relação ao ambiente de controlo (avaliação subjetiva) de cada risco, que indica a perceção que a área tem em relação à exposição do risco.

Tabela 4.16 - Riscos materiais sem controlos

Área	Risco	Ambiente de controlo	VaR
A14	3.6.4 Atrasos na execução de operações	Médio	949 906,00 €
A14	3.6.2 Falhas nos pagamentos ou liquidações	Médio Alto	167 410,00 €
A14	3.6.2 Falhas nos pagamentos ou liquidações	Médio	167 168,00 €
A14	3.6.3 Falhas na execução das operações	Médio Baixo	40 325,00 €
A14	3.6.4 Atrasos na execução de operações	Médio Baixo	40 249,00 €
A10	3.6.3 Falhas na execução das operações	Médio Alto	29 665,00 €
A14	3.6.9 Erros de cálculo	Baixo	19 812,00 €
A5	3.6.4 Atrasos na execução de operações	Alto	11 811,00 €
A14	3.6.4 Atrasos na execução de operações	Médio Alto	10 552,00 €
A14	3.6.3 Falhas na execução das operações	Médio	4 899,00 €
A7	3.6.3 Falhas na execução das operações	Médio Alto	3 944,00 €
A5	3.6.3 Falhas na execução das operações	Alto	1 487,00 €
A5	3.6.4 Atrasos na execução de operações	Alto	771,00 €
A11	3.6.3 Falhas na execução das operações	Médio	632,00 €
A11	3.6.3 Falhas na execução das operações	Alto	339,00 €
A11	3.6.3 Falhas na execução das operações	Alto	62,00 €
A13	3.4.2 Falhas no fornecimento de bens e serviços	Baixo	N/A
A15	3.6.3 Falhas na execução das operações	Baixo	N/A
A11	3.6.4 Atrasos na execução de operações	Baixo	N/A
A16	3.6.11 Falhas em processos judiciais ou litígios	Médio	N/A
A9	3.6.9 Erros de cálculo	Médio Alto	N/A
A9	3.6.4 Atrasos na execução de operações	Médio Alto	N/A
A9	3.6.4 Atrasos na execução de operações	Médio Alto	N/A
A9	3.6.4 Atrasos na execução de operações	Médio Alto	N/A
A9	3.6.4 Atrasos na execução de operações	Médio Alto	N/A
A9	3.6.5 Falhas de comunicação na instituição	Médio Alto	N/A
A9	3.6.6 Falhas de comunicação de terceiros	Médio Alto	N/A
A9	3.6.3 Falhas na execução das operações	Médio Alto	N/A
A8	3.6.3 Falhas na execução das operações	Médio Alto	N/A
A8	3.6.3 Falhas na execução das operações	Médio Alto	N/A
A8	3.6.3 Falhas na execução das operações	Médio Alto	N/A
A10	3.6.3 Falhas na execução das operações	Médio Alto	N/A
A9	3.6.4 Atrasos na execução de operações	Alto	N/A
A1	3.6.3 Falhas na execução das operações	Alto	N/A
A7	3.6.4 Atrasos na execução de operações	Alto	N/A
Total			**1 449 032,00 €**

Cerca de 69% dos riscos sem controlos, possuem um ambiente de controlo Médio Alto ou Alto. Também é possível verificar que 19 riscos dos 35 riscos sem controlos são riscos materiais sem avaliação e que os restantes 16 contabilizam, aproximadamente, 1,5M€ do VaR estimado.

A Tabela 4.17 expressa a quantidade de riscos imateriais sem controlos associados que se dividem pelas diversas categorias de risco.

Tabela 4.17 - Riscos Imateriais sem controlos

Risco	#
3.3.1 Falhas na apresentação de informações	5
3.4.2 Falhas no fornecimento de bens e serviços	1
3.6.3 Falhas na execução das operações	7
3.6.4 Atrasos na execução das operações	3
3.6.5 Falhas de comunicação na instituição	2
3.6.9 Erros de cálculo	3
7.3.3 Deficiências na gestão dos recursos humanos	1
Total	**22**

A Tabela 4.18 lista os riscos que possuem um ambiente de controlo deficiente, ou seja, um ambiente Médio Baixo ou Baixo, com 7 e 12 riscos, respetivamente. Os riscos que possuem controlos representam 53% dos riscos com um ambiente de controlo deficiente. A área A14 possui 9 riscos com um ambiente de controlo deficiente. Para além disso, é possível verificar que existem 9 riscos materiais com avaliação, 9 riscos materiais sem avaliação e 1 risco imaterial com deficiências nos seus ambientes de controlo.

Tabela 4.18 - Riscos com ambiente de controlo deficiente

Área	Risco	Ambiente de controlo	Controlos	VaR
A14	3.6.9 Erros de cálculo	Baixo	0	19 812,00 €
A13	3.4.2 Falhas de fornecimento de bens e serviços	Baixo	0	N/A
A15	3.6.3 Falhas na execução das operações	Baixo	0	N/A
A11	3.6.4 Atrasos na execução de operações	Baixo	0	N/A
A16	3.4.2 Falhas no fornecimento de bens e serviços	Baixo	0	Imaterial
A13	5.1.1 Fraude interna	Baixo	1	N/A
A11	4.1.1 Fraude externa	Baixo	1	N/A
A14	3.6.4 Atrasos na execução de operações	Médio Baixo	0	949 906,00 €

Área	Risco	Ambiente de controlo	Controlos	VaR
A14	3.6.3 Falhas na execução das operações	Médio Baixo	1	86 554,00 €
A14	3.4.2 Falhas no fornecimento de bens e serviços	Médio Baixo	2	55 555,00 €
A14	3.6.3 Falhas na execução das operações	Médio Baixo	0	40 325,00 €
A14	3.6.4 Atrasos na execução de operações	Médio Baixo	0	40 249,00 €
A14	1.2.2 Falhas na aceitação sinistros	Médio Baixo	2	14 139,00 €
A14	3.6.3 Falhas na execução das operações	Médio Baixo	1	3 767,00 €
A14	3.3.1 Falhas no reporte de informação	Médio Baixo	1	2 917,00 €
A13	5.1.1 Fraude interna	Médio Baixo	2	N/A
A7	3.6.4 Atrasos na execução de operações	Médio Baixo	1	N/A
A13	3.6.3 Falhas na execução das operações	Médio Baixo	2	N/A
A16	3.6.11 Falhas em processos judiciais ou litígios	Médio Baixo	0	N/A
Total	**19**			**1 213 224,00 €**

4.4.4 Oportunidades de Melhoria

Após a avaliação dos riscos e dos controlos, foram identificadas 67 oportunidades de melhoria para mitigar o risco operacional, demonstrado no anexo E. Selecionaram-se 31 oportunidades de melhoria, que foram registadas no sistema GRC para futura implementação.

A Tabela 4.19 mostra onde é que as oportunidades de melhoria foram aplicadas.

Tabela 4.19 - Oportunidades de melhoria

	Oportunidades de melhoria
Risco com Var superior a 1M €	7
Risco Material com avaliação	14
Risco Material sem avaliação	7
Risco Imaterial	9
Controlos com deficiências	46
Risco material sem controlo	11
Riscos com ambiente de controlo deficiente	9
Riscos com Eventos de Riscos Operacional registados	2

5

DISCUSSÃO DE RESULTADOS

Neste capítulo, pretende-se analisar os resultados obtidos no capítulo anterior, de modo a perceber a importância de perceber em maior detalhe a exposição da empresa ao risco operacional, com o auxílio da aplicação do Ciclo ROCI.

5.1 Resultados da aplicação do Ciclo ROCI

Diante da aplicação do Ciclo ROCI, foi possível calcular a exposição da empresa ao risco operacional. A Figura 5.1 é uma representação gráfica da exposição para cada uma das áreas de negócio em estudo. Verificou-se que as áreas: A3, A4, A5, A10, A13 e A14 são as áreas com maior peso, onde a área A14 representa mais de 50% da exposição acumulada para os riscos avaliados. Por outro lado, as restantes áreas possuem uma exposição muito residual, inferior a 1% para os riscos avaliados.

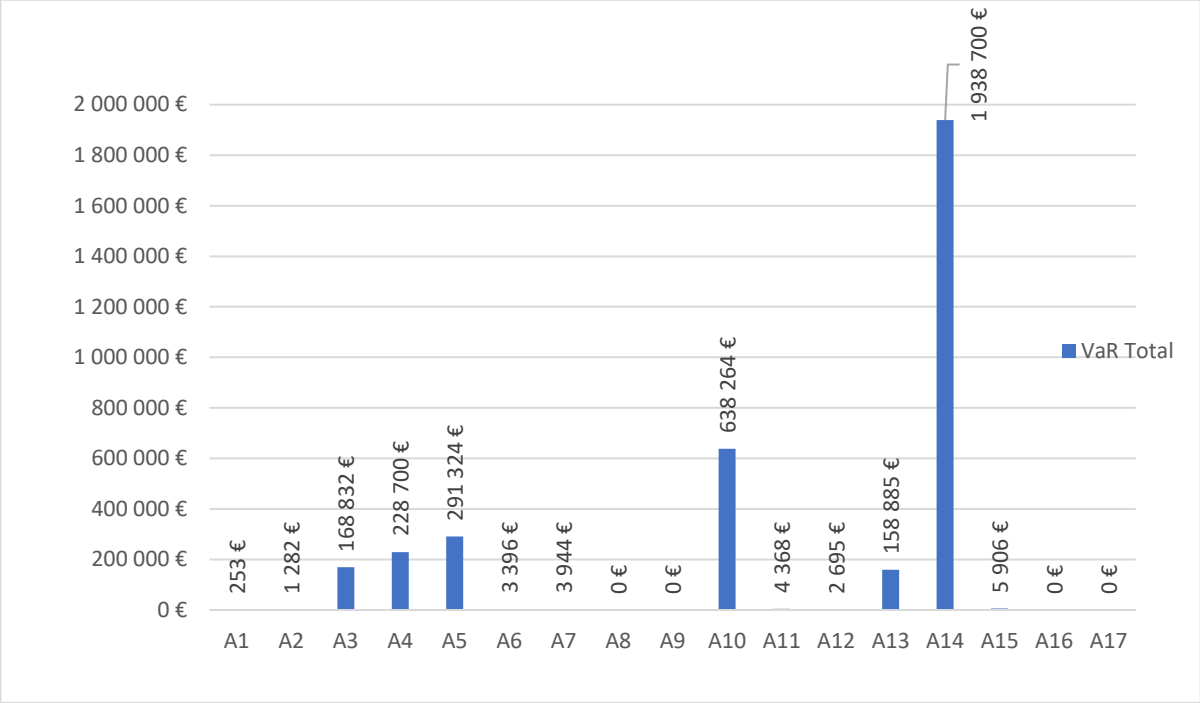


Figura 5.1 - Exposição das áreas

De acordo com a Tabela 5.1, verificou-se que, aproximadamente, 21% dos riscos foram avaliados quantitativamente. Também se notou que os riscos materiais sem avaliação representam a maior categoria de riscos, aproximadamente 46,6% de todos os riscos identificados. Para além disso, observou-se que 193 riscos dos 279 riscos materiais não possuem avaliação, o que corresponde aproximadamente a 70% dos riscos materiais.

Tabela 5.1 - Quantidade de Riscos por tipologia

Riscos		
Risco material com avaliação	83	20,1%
Risco material sem avaliação	193	46,6%
VaR > 1M	3	0,7%
Imateriais	135	32,6%
Total	**414**	

A Figura 5.2 demonstra graficamente a quantidade de riscos distribuídos pelos diversos macroprocessos da empresa. Os macroprocessos "Vendas", "Contabilidade" e "Governação" possuem o maior número de riscos identificados, representando 51%, mas apenas representam 7,8% do VaR acumulado. O macroprocesso "Sinistros" apenas representando 9% dos riscos

identificados, tem o maior peso do VaR acumulado de 1 845 850 €, cerca de 54% do valor total, como se pode ver na Figura 5.3.

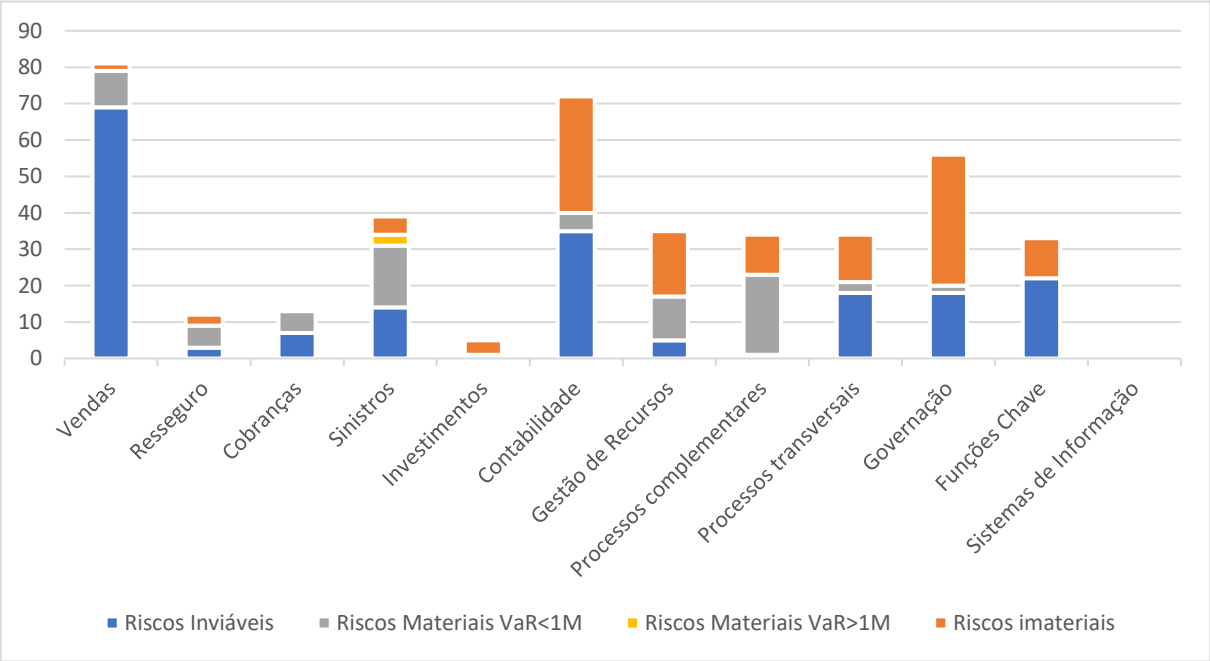


Figura 5.2 - Categoria de Riscos por macroprocesso

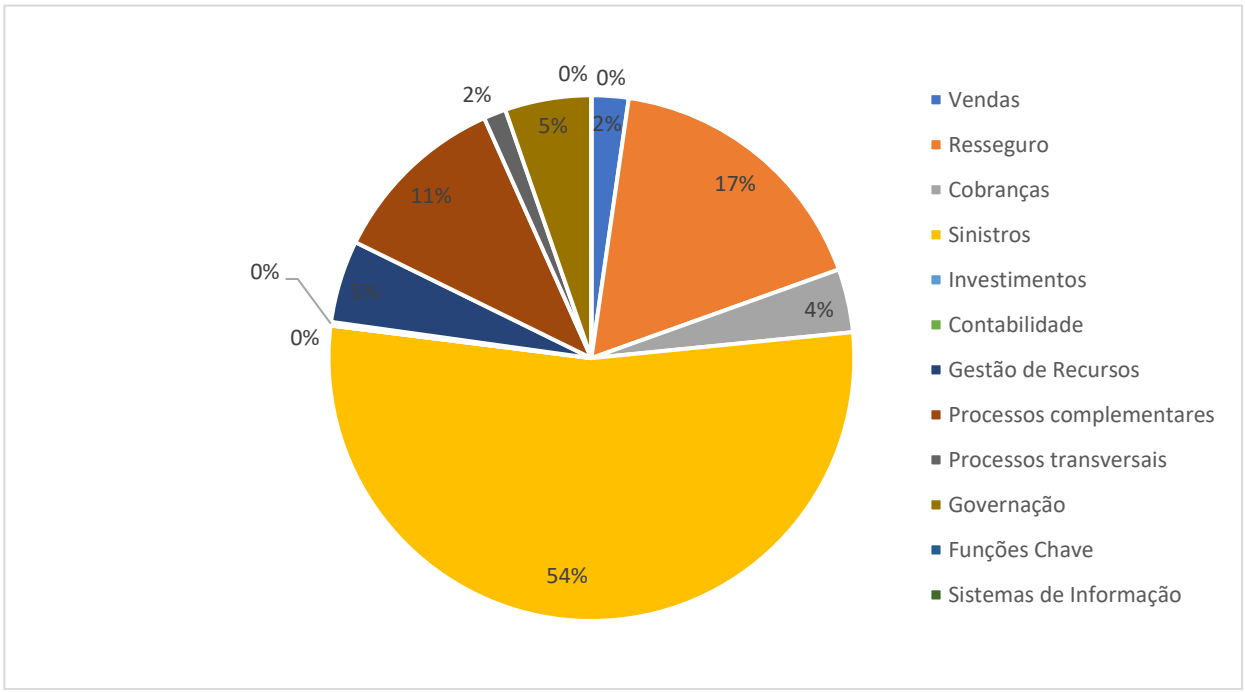


Figura 5.3 - Exposição dos Riscos por macroprocesso

No anexo C, é possível verificar que 18 riscos dos 83 riscos materiais com avaliação (21,7%) representam mais de 80% do VaR acumulado, 2 786 767 € de 3 446 554 €.

A Tabela 5.2 demonstra a exposição estimada dos riscos que possuem eventos, com um valor de 194 994 €. Por outro lado, esses eventos registaram um impacto máximo de 65 075 €, onde 2 000 € representam uma quase-perda. No entanto, o impacto líquido (o verdadeiro prejuízo da empresa) representa, aproximadamente, 1 423 €, cerca de 2% do impacto máximo calculado, havendo uma recuperação superior a 60 000 €. Deste modo, tinha-se avaliado a exposição desses riscos para um determinado valor, mas o impacto máximo dos eventos recolhidos representa 33% do VaR acumulado.

Tabela 5.2 - Exposição e Impactos de Eventos de Perda Operacional

VaR acumulado	**194 994,00 €**
Impacto Máximo	**65 075,02 €**
Valor da perda	**63 075,02 €**
Impacto Líquido	**1 423,35 €**

A área A6 é a área com o maior número de eventos registado. As áreas A14 e A5 possuem os riscos com maior VaR acumulado, 167 168 € e 18 590 €, respetivamente. No entanto, são as áreas A11 e A6 que têm o maior impacto máximo, representando mais de 95,4% do valor total, que por sua vez, apresentam uma exposição inferior a 2 000 €, Tabela 5.3.

Tabela 5.3 - Eventos de Risco operacional por área

Áreas	Evento de Risco Operacional	Controlos	VaR acumulado	Impacto Máximo	Impacto Líquido
A5	2	3	18 590,00 €	43,38 €	0,00 €
A11	2	0	339,00 €	40 242,59 €	0,00 €
A14	1	0	167 168,00 €	855,09 €	0,00 €
A12	1	2	0,00 €	90,75 €	90,75 €
A13	1	4	7 470,00 €	2 000,00 €	0,00 €
A6	3	9	1 427,00 €	21 843,21 €	1 332,60 €

Na Tabela 5.4, observa-se que o Processo "06.02.01. Pagamentos" apresentou no total um impacto máximo de 42 876 € em perdas operacionais, pelo que só tinha sido estimado um VaR de 1 766 €. No entanto, o impacto líquido foi ligeiramente ao valor que se tinha estimado. O evento de risco operacional associado ao Processo "06.03.01. Obrigações fiscais" surgiu de um

risco inviável, ou seja, não se sabia determinar a sua exposição, que se refletiu num evento com um impacto máximo próximo dos 20 000 €.

Tabela 5.4 - Eventos de Risco Operacional por Processo

Processos	Evento de Risco Operacional	Controlos	VaR acumulado	Impacto Máximo	Impacto Líquido
01.01.03. Gestão de produtos	1	4	7 470,00 €	2 000,00 €	0,00 €
04.02.01. Pagamentos a sinistrados/ tomadores/ lesados	2	2	167 168,00 €	945,84 €	90,75 €
06.02.01. Pagamentos	4	4	1 766,00 €	42 876,19 €	1 332,60 €
06.03.01. Obrigações fiscais	1	5	0,00 €	19 209,61 €	0,00 €
08.05.03. Faturação a fornecedores	2	3	18 590,00 €	43,38 €	0,00 €

A Tabela 5.5 enumera os controlos com deficiências. O controlo manual validação por colaboradores representa 45% dos controlos com deficiências.

Tabela 5.5 - Controlos com deficiências por tipologia

Controlos com deficiências	
Validação por colaboradores	22
Reconciliação	7
Análise periódica	6
Restrições de sistema	2
Segregação de funções	2
Alertas do sistema no Outlook	2
Alerta de sistema	2
Autorização de operações	2
Alertas de sistema sobre prazos	1
Repositório de entidades	1
Requisitos legais e regulamentares	1
Reuniões semanais com o prestador de serviços multirrisco	1
Total	**49**

A Figura 5.4 representa graficamente a distribuição dos riscos sem controlos, um total de 57 riscos, e que os riscos imateriais representam 39% dos riscos. A categoria Médio Alto é a categoria que possui mais riscos sem controlos, representando 51% dos riscos, Tabela 5.6.

Tabela 5.6 - Riscos sem controlos por Ambiente de Controlo

Tipo de Ambiente	Riscos	Riscos Materiais com avaliação	Riscos Materiais sem avaliação	Imateriais	%
Alto	15	5	3	7	26%
Médio Alto	29	4	12	13	51%
Médio	4	3	0	1	7%
Médio Baixo	4	3	1	0	7%
Baixo	5	1	3	1	9%
Total	**57**	**16**	**19**	**22**	**100%**

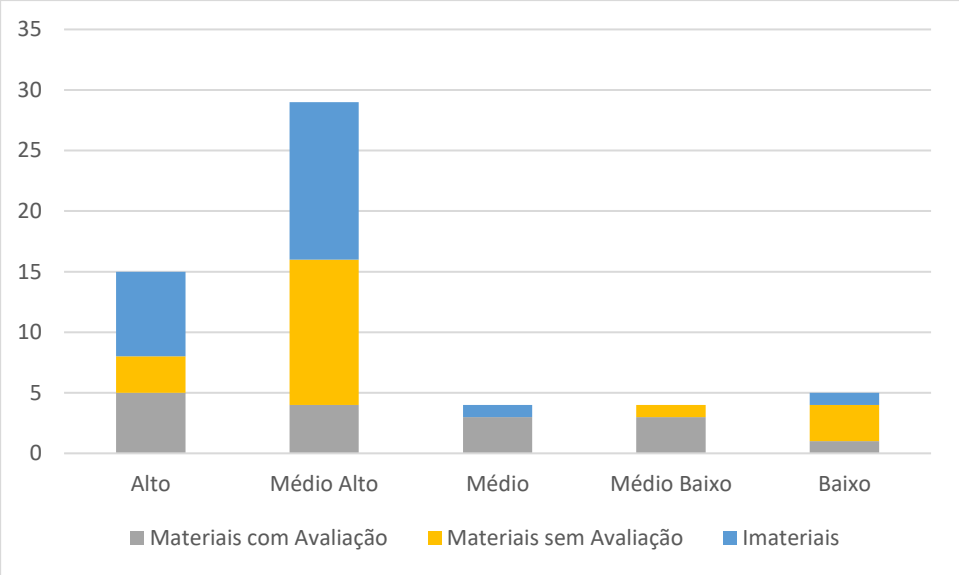


Figura 5.4 - Riscos sem controlos por ambiente de controlo

De acordo com a Figura 5.5, observa-se os riscos com ambientes de controlo deficiente, nomeadamente, Baixo e Médio Baixo. A categoria Baixo apresenta 5 riscos sem quaisquer controlos, enquanto a categoria Médio Baixo apresenta 8 riscos com controlos associados, cerca de 42% dos riscos. Para além disso, existem 8 riscos materiais com avaliação com ambiente de controlo Médio Baixo e existem 5 riscos materiais sem avaliação com ambiente de controlo Baixo.

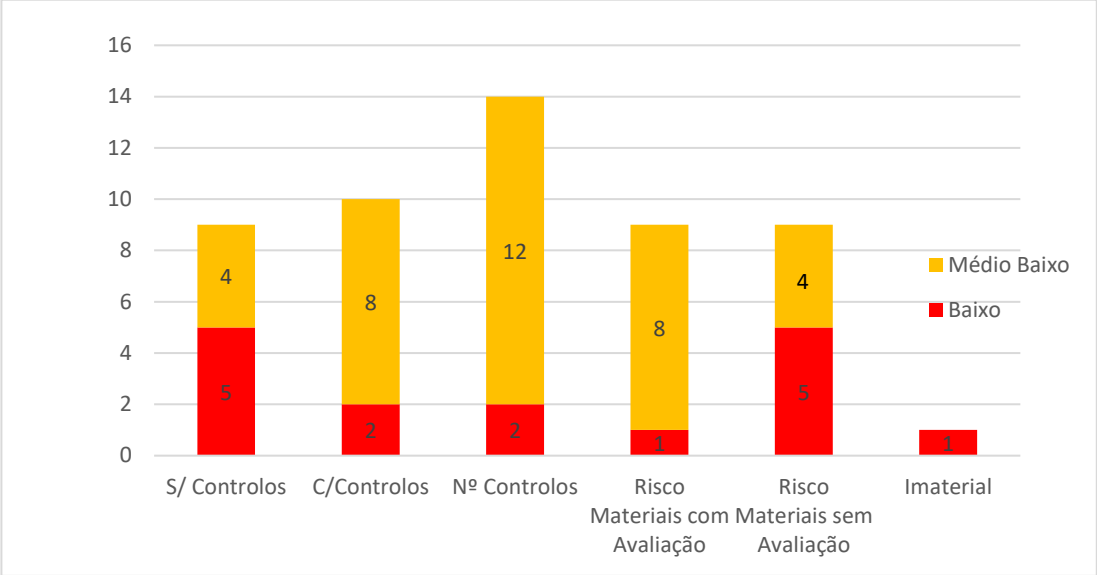


Figura 5.5 - Riscos com ambiente deficiente

Na Figura 5.6, as áreas A14, A4, A7, A11 possuem 16, 10, 10, 9 oportunidades de melhoria identificadas, respetivamente. As restantes áreas representam 33% das oportunidades de melhoria identificadas.

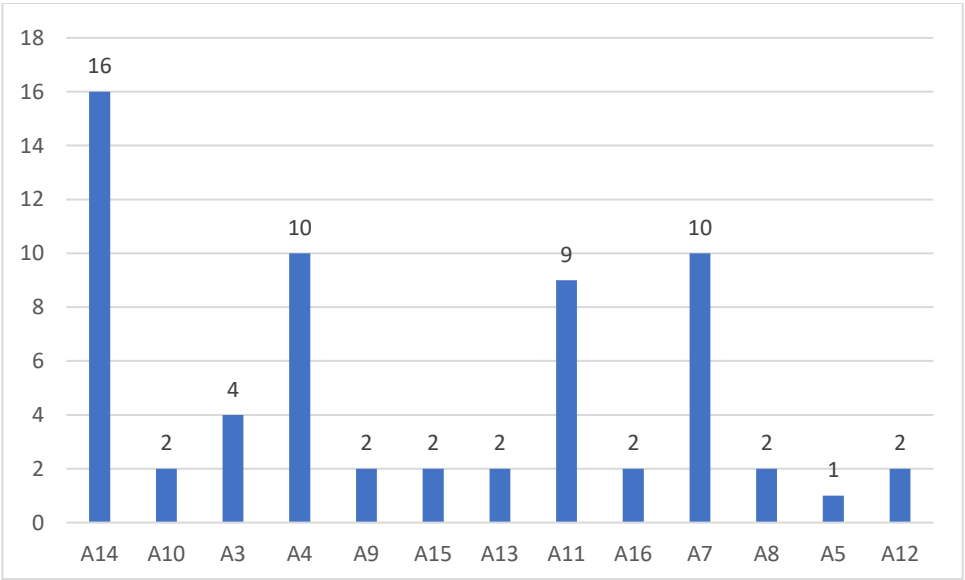


Figura 5.6 - Oportunidades de Melhoria por área

De acordo com a Figura 5.7, as oportunidades de melhoria tiveram mais foco na mitigação de controlos com deficiências, em que foram identificadas no total 46 oportunidades. Apesar de existirem apenas 3 riscos com VaR superior a 1M, foram identificadas 7 oportunidades de melhoria.

Relativamente aos eventos de perda, identificaram-se 2 oportunidades de melhoria, no qual uma das melhorias permite mitigar um risco relativo a um evento que possui um VaR de 167 168 €.

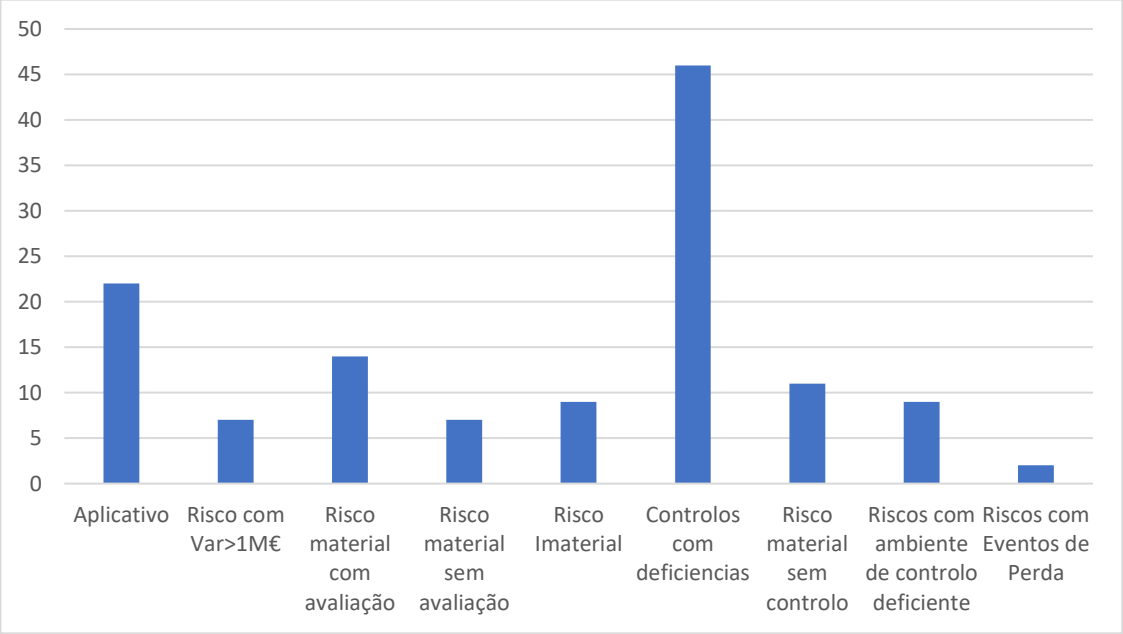


Figura 5.7 - Oportunidades de melhoria por categoria

5.2 Comparação da avaliação dos riscos face aos eventos de perda operacional

Para determinar se a avaliação dos riscos está bem estimada e se os mecanismos de controlos implementados estão a ser eficazes, procede-se à comparação dos riscos com o impacto dos eventos de risco registados.

De acordo com a Tabela 4.8, o registo de 2 eventos, com um impacto máximo de 40 122,59 € e 153,04 €, originaram 2 novos riscos com falhas no fornecimento de bens e serviços e falhas no desempenho de contrapartes. Para além disso, houve um risco com erros de registo ou afetação contabilística que teve 1 evento associado com um impacto máximo de 19 209, 61 €. Por outro lado, os restantes riscos tinham a sua exposição avaliada, no que resultou em eventos com um impacto máximo inferior a 6 000 €. Ou seja, cerca de 91% do impacto máximo surgiram de 2 riscos que não estavam previamente quantificados.

Na Tabela 5.7, é possível comparar a exposição estimada para cada tipologia de risco com o impacto dos eventos de risco recolhidos. Verifica-se que 3 tipos de risco não tinham

qualquer avaliação, mas registaram eventos com um impacto máximo de 40 122 €, 19 209 € e 153 €. Registaram-se 3 eventos nos riscos 3.6.2 Falhas nos pagamentos ou liquidações, que por sua apresentam a maior exposição estimada, 168 595 € e que representaram prejuízos de 1 423 € para a empresa.

Tabela 5.7 - Eventos de Risco Operacional por Tipologia de Risco

Riscos	Evento de Risco Operacional	VaR	Impacto Máximo	Valor da perda	Impacto Líquido
3.4.2 Falhas no fornecimento de bens e serviços	1	0,00 €	40 122,59 €	40 122,59 €	0,00 €
3.5.1 Falhas no desempenho de contrapartes	1	0,00 €	153,04 €	153,04 €	0,00 €
3.6.2 Falhas nos pagamentos ou liquidações	3	168 595,00 €	3 426,40 €	3 426,40 €	1 423,35 €
3.6.3 Falhas na execução das operações	3	20 765,00 €	2 120,00 €	120,00 €	0,00 €
3.6.8 Erros de registo ou afetação contabilística	1	0,00 €	19 209,61 €	19 209,61 €	0,00 €
3.7.2 Falhas na prestação de serviços de serviços subcontratados	1	5 634,00 €	43,38 €	43,38 €	0,00 €

Deste modo, é importante salientar a importância de identificar antecipadamente os vários riscos, avaliar a sua exposição e calibrar com os eventos de risco operacional registados. Assim, é possível analisar se o exercício realizado e as medidas de mitigação e de melhoria estão a surtir o efeito desejado.

6

CONCLUSÃO

No presente capítulo serão apresentadas as conclusões do trabalho desenvolvido. Inicia-se com uma secção relativa à revisão da literatura, seguida de uma breve síntese conclusiva sobre aplicação do Ciclo ROCI, as contribuições da investigação para a teoria e para a prática das organizações e, no final, serão apresentadas as limitações e as sugestões de trabalho futuro a ser desenvolvido.

6.1 Conclusão

Face aos objetivos e às necessidades das instituições financeiras e seguradoras, é cada vez mais importante incorporar a gestão do risco operacional nas suas estruturas organizacionais e envolver todos os colaboradores na mesma missão: reduzir a exposição ao risco operacional.

Historicamente, as instituições financeiras focavam-se principalmente na gestão de risco de crédito e de mercado. No entanto, nas últimas décadas, os diversos escândalos financeiros mostraram que os riscos operacionais podem resultar em perdas financeiras severas e danos à reputação, enfatizando a necessidade de uma supervisão e gestão mais rigorosas desses riscos, destacando a importância do risco operacional. Deste modo, a existência de determinados problemas financeiros e a elaboração de legislação impulsionou e impôs o desenvolvimento de sistemas de governação, que se traduzem na implementação de mecanismos e práticas úteis para efetuar uma gestão eficaz. Assim, permite às organizações não sofrerem tanto do impacto de perdas operacionais.

No entanto, foi possível verificar ao longo da revisão literária que o risco operacional possui características que dificultam a sua gestão. A maioria das dificuldades sentidas pela gestão justificam-se pela sua abrangência, extensão e a falta de mecanismos eficientes, que se costumam traduzir em perdas inesperadas para o mercado segurador.

Um sistema de gestão de riscos eficaz não se limita apenas à identificação e avaliação dos riscos, mas também se foca na implementação de controlos e estratégias de mitigação. Ao rastrear e avaliar sistematicamente os riscos, as empresas podem abordar proactivamente potenciais problemas e/ou perdas, protegendo seus ativos e reputação. Em essência, a gestão de riscos operacional passou a ser uma necessidade.

Solvência II, com a sua abordagem de três pilares, representa uma mudança significativa na regulamentação das empresas de seguros e resseguros na União Europeia. O principal objetivo é estabelecer um conjunto de requisitos de capital e desenvolver sistemas gestão de riscos em toda a UE para aumentar a proteção dos segurados.

O Pilar I da Solvência II define os requisitos quantitativos, como o capital que as empresas de seguros e resseguros devem manter. No entanto, reconhece-se que o Pilar I e aplicação da fórmula-padrão, por si só, tem algumas limitações ao nível do cálculo do Requisito de Solvência Operacional (SCRop). O valor obtido não é realista e preciso da exposição da empresa e não reflete o seu perfil de risco, visto que a fórmula não tem a consideração as características da empresa e não há nada que indique que se está a reduzir a sua exposição ao risco operacional. Deste modo, o Pilar I não pode atuar isolado do Pilar II. O Pilar II aborda os aspetos qualitativos do sistema financeiro global de uma instituição. Ele enfatiza a importância da governação e supervisão, destacando a necessidade de uma estrutura robusta de gestão de riscos operacionais. Complementando os requisitos quantitativos do Pilar I com as disposições qualitativas do Pilar II, a Solvência II oferece uma abordagem mais holística à gestão de riscos, combatendo efetivamente algumas das falhas inerentes ao Pilar I.

A abordagem histórica de gestão de riscos operacionais, baseada em incidentes e perdas passadas, oferece informações valiosas, mas nem sempre são indicativas de futuras ameaças, especialmente num ambiente de negócios em rápida mudança. Por outro lado, uma abordagem prospetiva enfatiza a previsão e antecipação de riscos futuros, garantindo que as empresas se mantenham à frente das mudanças. Desta forma, a sinergia destas duas abordagens vai permitir comparar periodicamente e calibrar os resultados retirados da avaliação do risco com os eventos recolhidos. Assim, a área de gestão de risco pode elaborar juízos de valor sobre os controlos impostos e se é necessário alterar a sua estratégia face ao risco operacional

Mediante o processo de revisão de literatura constatou-se a existência de um gap na literatura. Assim, para analisar os sistemas de gestão de risco operacional e controlo interno,

a realização deste estudo contribui colmatar a lacuna existente, através da análise do Ciclo ROCI, método desenvolvido pela Fidelidade.

No início do estudo, identificaram-se os principais processos e riscos inerentes às atividades das áreas em estudo, e determinar a exposição da empresa aos diversos riscos, através do cálculo do VaR. Além disso, verificar a eficácia dos controlos para mitigar a exposição do risco operacional. Por fim, identificaram-se oportunidades de melhoria a serem implementadas.

Primeiramente, foram identificados os macroprocessos e subprocessos associados a 17 áreas. Deste modo, prosseguiu-se para a identificação dos riscos, bem como para a determinação da exposição de cada risco com o auxílio da perceção dos intervenientes de cada área. Conclui-se que a exposição acumulada dos 414 riscos identificados tem, aproximadamente, um valor de 3,5M €. A área A14 e o macroprocesso "Sinistros" apresentam a maior exposição acumulada da empresa, 1,94M € e 1,85M €, respetivamente.

Relativamente aos riscos, neste ciclo só foi possível obter a exposição para 30% dos riscos materiais, e dos quais 3 possuem um VaR superior a 1 milhão de euros (VaR>1M). É de notar que os riscos imateriais correspondem a 32,6% dos riscos identificados.

No que diz respeito aos eventos de perda, foram identificados 10 eventos de perda, onde foi possível correlacionar o impacto dos eventos com a exposição estimada dos riscos relacionados com essas perdas. Ao comparar a exposição estimada para esses riscos e o impacto máximo dos eventos de perda, concluiu-se que as perdas ocorridas têm enquadramento com o VaR obtido. Adicionalmente aos riscos identificados no Ciclo ROCI, a análise de registo de eventos de risco operacional permitiu a identificação de 2 outros riscos. Por fim, os riscos associados a Falhas no fornecimento de bens e serviços, sem avaliação, possuem eventos com um impacto acumulado de 40 122 €. Assim, esta comparação permitiu calibrar a avaliação dos riscos e agir de forma a mitigar futuras perdas para a empresa.

No que diz respeito à eficácia dos controlos, foram identificados 204, dos quais 49 apresentam deficiências. Na sequência, analisou-se o ambiente de controlo associado aos riscos sem controlos. Determinou-se que apesar de não possuírem controlos, 67% dos riscos apresentam um ambiente de controlo Médio Alto e Alto. No caso dos riscos com um ambiente de controlo deficiente, identificaram-se 19 riscos, onde 9 não possuem quaisquer controlos associados.

Por fim, foram propostas 67 oportunidades de melhoria para mitigar as lacunas identificadas nos riscos e nos controlos. Verificou-se que 46 oportunidades estavam associadas a controlos deficientes e que 37 oportunidades estavam associadas aos vários tipos de risco.

Por conseguinte, a aplicação deste método colmata a gap na literatura, dando uma visão mais holística e integrada dos sistemas de gestão de risco operacional. Assim, destaca-

se a eficácia da metodologia aplicada, no setor segurador, tendo em conta a determinação da exposição do risco operacional, bem como os métodos para a sua mitigação.

6.2 Contribuições da Investigação

É igualmente importante reconhecer a maturidade do método e os seus potenciais contributos, teóricos e práticos, para colmatar algumas das limitações da literatura, principalmente, a nível do Pilar I e o cumprimento dos requisitos do Pilar II.

6.2.1 Contributos para a Construção da Teoria

Teoricamente, este método pode fornecer informações e melhorias às *frameworks* de gestão de risco operacional, permitindo uma compreensão mais precisa da categorização e priorização do risco. O método pode servir de base para o desenvolvimento de novos modelos e teorias que respondam de forma mais adequada às complexidades do risco operacional no setor segurador e ressegurador. As limitações da aplicabilidade da fórmula-padrão, por ser imprecisa e pouco sensível ao risco operacional, remetem para a necessidade de implementar sistemas de governação robustos. No entanto, o Pilar II não específica a forma como devem construir os sistemas de gestão de risco, tais como identificar, avaliar e monitorizar o risco, apenas salienta a necessidade de o fazer. Desta forma, o Ciclo ROCI permite responder a essa necessidade e criar um sistema de gestão de riscos robusto e eficaz, com elevada sensibilidade ao risco.

6.2.2 Contributos para a Gestão

Dada a sua aplicação por uma das maiores companhias de seguros portuguesas, este método pode servir de *benchmark* para as práticas de gestão do risco operacional no setor. Pode orientar o desenvolvimento de melhores práticas e *standards* que podem ser adotados por outras companhias de seguros que procuram melhorar a sua gestão do risco operacional e o cumprimento da regulamentação Solvência II.

Em termos práticos, a aplicação deste método pode ajudar a satisfazer os requisitos do Pilar II relativamente ao Solvência II, assegurando que a empresa emprega práticas eficazes de gestão de risco. Isto pode melhorar a conformidade regulamentar da empresa e reduzir a probabilidade de sanções regulamentares. Pode contribuir significativamente para a identificação, avaliação e gestão da exposição dos riscos operacionais, permitindo a implementação de estratégias eficazes de mitigação do risco e, por sua vez, ajudar na afetação

de recursos, na priorização de riscos e no desenvolvimento de estratégias de resposta a riscos específicos. Por outro lado, ajuda a gerir as incertezas e vulnerabilidades operacionais inerentes à atividade seguradora, melhorando assim a resiliência e a estabilidade globais da empresa.

No que diz respeito à adoção do Ciclo ROCI, é necessário adaptá-lo à dimensão, natureza, características da empresa, pois a realidade da Fidelidade difere da realidade das outras empresas de seguro. Por fim, pode servir como um catalisador para a inovação nas práticas de gestão de risco, inspirando outras empresas a aperfeiçoar as suas abordagens e a contribuir para o avanço do setor como um todo.

6.3 Limitações do Estudo

É importante salientar que ao longo do desenvolvimento da presente dissertação, surgiram algumas limitações que podem ter impacto nos resultados obtidos.

O método baseia-se predominantemente na perceção dos colaboradores para identificar e avaliar os riscos, o que tem um impacto significativo na qualidade da gestão dos riscos. As perspetivas dos colaboradores sobre o risco podem ser subjetivas, variadas e podem não estar necessariamente alinhadas com a exposição real ao risco, conduzindo a potenciais imprecisões na identificação e avaliação do risco. A variabilidade na experiência, conhecimento e consciência dos riscos operacionais por parte dos trabalhadores pode criar discrepâncias na avaliação da gravidade e probabilidade dos eventos de risco, afetando assim a eficácia global da estratégia de gestão do risco.

O método é limitado pela existência de um montante substancial de riscos materiais sem avaliação, sendo por isso, apesar do desconhecimento da sua exposição, fundamental a sua gestão. A incapacidade de detetar todos os riscos é outra das limitações, podendo afetar tanto a sua estabilidade financeira como a sua reputação.

Por fim, a recolha de eventos de risco operacional é crucial para uma compreensão e gestão holística dos riscos operacionais. O reporte e registo dos eventos depende da vontade e da capacidade dos trabalhadores de as comunicarem. Esta dependência introduz uma variabilidade substancial e um potencial enviesamento nos dados recolhidos. Os trabalhadores podem ter relutância em comunicar os eventos de perda devido ao receio de repercussões, à falta de sensibilização ou à perceção da complexidade do processo de comunicação. A deficiência ou a falta de dados exatos sobre os eventos de risco operacional complica a comparação das avaliações de risco com os eventos, impedindo assim a calibração da avaliação e a validação e o aperfeiçoamento e desenvolvimento de estratégias de gestão do risco.

Consequentemente, após o Ciclo ROCI, a organização permanece vulnerável a perturbações operacionais imprevistas e a perdas financeiras inesperadas, sendo por isso a gestão do risco operacional um processo contínuo de melhoria.

6.4 Sugestões de trabalho futuro

Ao longo deste estudo, mergulhámos profundamente nas complexidades do risco operacional e nas ferramentas e metodologias que o enquadram. Com base nos pontos supracitados, emerge um caminho claro para futuras investigações e aplicações práticas.

Primeiramente, assume-se como pertinente a necessidade de difundir a cultura de risco operacional de forma mais abrangente. A integração desta cultura nas diversas camadas organizacionais é crucial, através de planos e estratégias direcionados para este fim. Quando os colaboradores estão plenamente cientes da sua exposição e das implicações associadas, torna-se mais viável não só identificar riscos, mas também adotar práticas que os mitiguem eficazmente.

Em relação ao Ciclo ROCI, é evidente que a sua eficácia está intrinsecamente ligada à perceção dos intervenientes. Uma compreensão profunda e precisa da exposição ao risco por parte de todos os envolvidos nas diversas áreas é indispensável. Trabalhos futuros poderiam explorar maneiras de afinar esta perceção, talvez através de formações específicas ou simulações práticas, para minimizar as chances de falhas e imprecisões no ciclo.

Por fim, e talvez um dos avanços mais promissores para a área, é a integração de inteligência artificial (IA) na gestão do risco operacional. Com a capacidade da IA de analisar grandes volumes de dados, pode ser possível identificar correlações na forma como os riscos são percebidos e geridos. Assim, permitiria identificar *root-causes* e antecipar potenciais ameaças e/ou perdas significativas, podendo proporcionar às organizações uma vantagem importante na gestão dos riscos operacionais.

Em síntese, embora se tenha feito avanços significativos no domínio do risco operacional, o caminho à frente está repleto de oportunidades para inovação. Com a integração de tecnologias emergentes, a gestão do risco operacional pode aumentar a sua eficiência e eficácia.

BIBLIOGRAFIA

Abid, G., & Ahmed, A. (2014). *Failing in corporate governance and warning signs of a corporate collapse. Pakistan Journal of Commerce and Social Science,* Vol. 8 (3), 846-866. Available at SSRN: Failing in Corporate Governance and Warning Signs of a Corporate Collapse by Ghulam Abid, Alia Ahmed :: SSRN

Aloqab, A., Alobaidi, F., & Raweh, B. (2018). Operational risk management in financial institutions: An overview. *Business and Economic Research*, *Vol. 8(2)*, 11–32. Available at: Operational Risk Management in Financial Institutions: An Overview | Aloqab | Business and Economic Research (macrothink.org)

Amorim, A. C., Mira da Silva, M., Pereira, R., & Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. *Information Systems*, *101*, 101496. Available at: Using agile methodologies for adopting COBIT - ScienceDirect

Aon Benfield. (2012). *CRO guide to solvency II -The journey from complexity to best practice*. October, 1-40. Aon plc Global Media Relations.

Assad, A. M. (2013). Aplicação da metodologia LDA para gestão do risco operacional de companhia seguradora. Dissertação apresentada ao Programa de Pós-Graduação em Administração de Empresas, Universidade Presbiteriana Mackenzie. São Paulo, Brasil. Available at: Aplicação da metodologia LDA para gestão do risco operacional de companhia seguradora (mackenzie.br)

Assi, M. (2021). *Gestão de riscos com controles internos*. Saint Paul Editora. Available at: Gestão de riscos com controles internos - Marcos Assi - Google Livros

Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF). (2020). *IFRS 17 – Apresentação PCES*. Available at: Apresentação do PowerPoint (asf.com.pt)

Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF). (2017a). *ASF - Enquadramento*. Available at: ASF - Enquadramento

Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF). (2017b). *ASF - Solvência II*. Available at: ASF - Solvência II

Amazon Web Services (AWS). (2023). *O que é GRC? – Explicação sobre governança, risco e conformidade – AWS*. Amazon Web Services, Inc. Available at: O que é GRC? – Explicação sobre governança, risco e conformidade – AWS (amazon.com)

Banco de Portugal. (2023). Regras prudenciais | Banco de Portugal. Available at: Regras prudenciais | Banco de Portugal (bportugal.pt)

Barangă, L. P. (2016). Similarities and differences between the operational risk covered by Basel III and Solvency II and trends in this area. *Theoretical and Applied Economics*, Vol. XXIII, Special issue (I), 19-28. Available at: Microsoft Word - Garda.docx (researchgate.net)

Barriga, L., & Rosengren, E. S. (2006). Overview of Operational Risk Management at Financial Institutions (Chap 8). In Karyl B. Leggio, David L. Bodde, Marilyn L. Taylor (Eds). *In Elsevier Global Energy Policy and Economics Series, Managing Enterprise Risk, Elsevier Science* Ltd, 119-133, ISBN 9780080449494, Available at: Overview of Operational Risk Management at Financial Institutions - ScienceDirect

Bauer, S. (2012). A literature review on operational IT risks and regulations of institutions in the financial service sector. *In The Proceedings of International Conference on Information Resources Management* 58 (CONF-IRM). Available at: "A Literature Review on Operational IT Risks and Regulations of Institu" by Stefan Bauer (aisnet.org)

Beltran, A. L. (2003). *La investigación-acción: Conocer y cambiar la práctica educativa*. Ediciones Grao. Available at: La investigación-acción: Conocer y cambiar la práctica educativa - Antonio Latorre Beltran - Google Livros

Boonen, T. J. (2017). Solvency II solvency capital requirement for life insurance companies based on expected shortfall. *European Actuarial Journal*, Vol. *7*(2), 405–434. Available at: Solvency II solvency capital requirement for life insurance companies based on expected shortfall | European Actuarial Journal (springer.com)

Bryce, C., Webb, R., Cheevers, C., Ring, P., & Clark. G. (2016). Should the insurance industry be banking on risk escalation for solvency II? *International Review of Financial Analysis,* Vol. 46, 131-139. Available at: Should the insurance industry be banking on risk escalation for solvency II? - ScienceDirect

Cantle, N., Clark, D., Kent, J., & Verheugen, H. (2012). A brief overview of current approaches to operational risk under Solvency II. *Milliman White Paper*. Available at: current-approaches-operational-risk.ashx (milliman.com)

Chen, J. (2022). Barings Bank: Its collapse, acquisition, lessons learned. Investopedia. Available at: Barings Bank: Its Collapse, Acquisition, Lessons Learned (investopedia.com)

Clipici, E. (2012). Solvency II–the new EU solvency regime on the insurance market. *Scientific Bulletin-Economic Sciences*, Vol. *11*(2), 112-119. Available at: Microsoft Word - Buletin_2012_2.doc (psu.edu)

Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS). (2009a). CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: System of

Governance, CEIOPS-DOC-29/09, October. Available at: CEIOPS-DOC-29-09-L2-Advice-on-Governance (europa.eu)

Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS). (2009b). CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula—Article 111 (f) Operational Risk, CEIOPS-DOC-45/09, October. Available at: CEIOPS-DOC-45-09-L2-Advice-Standard-Formula-operational-risk (europa.eu)

Corporate Finance Institute. (2022). *Top Accounting Scandals*. *Corporate Finance Institute.* Available at: Accounting Scandals - List of Top 10 Scandals in Past Decades (corporatefinanceinstitute.com)

Cowell, R. G., Verrall, R. J., & Yoon, Y. K. (2007). Modeling operational risk with bayesian networks. *Journal of Risk and Insurance*, Vol. *74*(4), 795–827. Available at: Modeling Operational Risk With Bayesian Networks - Cowell - 2007 - Journal of Risk and Insurance - Wiley Online Library

Cruz, M. G., Peters, G. W., & Shevchenko, P. V. (2015). *Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk*. John Wiley & Sons. Available at: Fundamental Aspects of Operational Risk and Insurance Analytics: A Handbook ... - Marcelo G. Cruz, Gareth W. Peters, Pavel V. Shevchenko - Google Livros

Deloitte. (2019). Establishing an operational risk framework in banking. Lessons learned in operational risk management. Available at: Establishing an Operational Risk Framework in Banking | Deloitte US

Deloitte, & Vw-Hsg. (2007). *Management of Operational Risks in Insurance*. Available at: untitled (actuaries.ie)

Dependencies and Calibration Working Party (DCWP). (2012). Solvency II Standard Formula and NAIC Risk-Based Capital (RBC). In Casualty Actuarial Society E-Forum, Fall 2012 - Vol. 2, 1-38. Available at: Internet Electronic Journal of (casact.org)

Diehl, C., & Weber, E. (2014). Gestão de riscos operacionais: Um estudo bibliográfico sobre ferramentas de auxílio. *Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ*, Vol. *19*, 41–58. Available at: Webwe (atena.org.br)

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, Vol. *16*(2), 147–166. Available at: Risk Management: History, Definition, and Critique - Dionne - 2013 - Risk Management and Insurance Review - Wiley Online Library

Dupont, E., Zou, J., & Nguyen Dao, Q. (2012). *Pillar 2 – Operational issues of risk management*. 60. Available at: Challenging your own risk culture (pwc.com)

Epetimehin, F. (2013). Managing the Impact of Operational Risk on the Solvency of Insurance Companies. *OIDA International Journal of Sustainable Development*, Vol. *5*(12), 69-78. Available at: Managing the Impact of Operational Risk on the Solvency of Insurance Companies by Festus Epetimehin :: SSRN

European Insurance and Occupational Pensions Authority (EIOPA). (2020). Solvency II. Available at: Solvency II (europa.eu)

European Insurance and Occupational Pensions Authority (EIOPA). (2015). Orientações relativas aos relatórios de supervisão e à divulgação pública. EIOPA-BoS-15/109 PT. Available at: eiopa_pt_public_disclosure_gl.pdf (europa.eu)

European Insurance and Occupational Pensions Authority (EIOPA). (2014a). The underlying assumptions in the standard formula for the Solvency Capital Requirement calculation. EIOPA-14-322, July. Frankfurt, Germany. Available at: Date: (thomsonreuters.com)

European Insurance and Occupational Pensions Authority (EIOPA). (2014b). Guidelines on system of governance. EIOPA-BoS-14/253 EN. Available at: EIOPA-BoS-14-253_GL on system of governance_revised_clean (europa.eu)

Fidelidade. (2022). Relatório sobre a Solvência e a Situação Financeira. 1-119. Available at: Microsoft Word - Fidelidade_SFCR_PT_2022.docx

Franca, L. M. P. V. (2015). *Mercado segurador - o ramo dos seguros de vida em Portugal: os determinantes da sua procura.* Dissertação apresentada ao Instituto Politécnico de Bragança para a obtenção do Grau de Mestre em Contabilidade e Finanças. Associação de Politécnicos do Norte (APNOR) Instituto Politécnico de Bragança. Available at: Biblioteca Digital do IPB: Mercado segurador - o ramo dos seguros de vida em Portugal: os determinantes da sua procura

Franzetti, C. (2016). *Operational risk modelling and management*. CRC Press. Available at: Operational Risk Modelling and Management - Claudio Franzetti - Google Livros

Gabbay, A. M. (2010). Simulação de Monte Carlo para mensuração do risco operacional: aplicação do modelo LDA. Dissertação apresentada ao Programa de Pós-Graduação em Administração de Empresas, Universidade Presbiteriana Mackenzie. São Paulo, Brasil. Available at: content (mackenzie.br)

Hail, L., & Wang, C. (2017). Corporate Scandals and Regulation: Appendix on Data Collection for Historical Time-Series from 1800 to 2015. *Institute for New Economic Thinking.* Paper nº 71. Available at*: SSRN 2960069.* Corporate Scandals and Regulation: Appendix on Data Collection for Historical Time-Series from 1800 to 2015 by Luzi Hail, Ahmed Tahoun, Clare Wang :: SSRN

Hoyle, D. (2007). *Quality Management Essentials*. Routledge. ISBN 9780750667869. Available at: Quality Management Essentials - David Hoyle - Google Livros

IBM. (2023). *What is GRC? | IBM*. Available at: What is GRC? | IBM

Islam, M. A., & Tedford, D. (2012). Implementation of risk management in manufacturing industry- An empirical investigation. In The Proceedings of Islam 2012 Implementation of Risk Management in Manufacturing Industry, Vol. *2*(3), 258-267. Available at: Microsoft Word - 6. Risk_Management__Final_Dr._Islam-Final-2.doc (psu.edu)

ISO. (2018). ISO 31000:2018(en), Risk management—Guidelines. Available at: ISO 31000:2018(en), Risk management — Guidelines

Istrate, C. A. (2017). Comparative analysis of evaluation models in insurance solvency. *Theoretical & Applied Economics*, *24*. Available at: Microsoft Word - Garda.docx (ectap.ro)

Istrate, C., & Badea, D. (2017). Financial management of insurance companies in the context of the new regime Solvency II. In the *Proceedings of the International Conference on Business Excellence*, Vol. *11*(1), 625-636. Available at: Financial management of insurance companies in the context of the new regime Solvency II (sciendo.com)

Kagan, J. (2023). Insurance: Definition, How It Works, and Main Types of Policies. Investopedia. Available at: Insurance: Definition, How It Works, and Main Types of Policies (investopedia.com)

Kang, S. W. (2015). Quantification of Operational Risk within an Insurance company. Master Actuariat de Dauphine, Université Paris-Dauphine, Available at: b70927361fe2ffede706ffadadf12696.pdf (institutdesactuaires.com)

Kelliher, P. O. J., Acharyya, M., Couper, A., Maguire, E., Nicholas, P., Pang, N., Smerald, C., Stevenson, D., Sullivan, J., & Teggin, P. (2020). Operational risk dependencies. *British Actuarial Journal*, *25*, e5, 1-21. Available at: Operational risk dependencies | British Actuarial Journal | Cambridge Core

Kenton, W. (2023). Understanding Value at Risk (VaR) and How It's Computed. Investopedia. Available at: Understanding Value at Risk (VaR) and How It's Computed (investopedia.com)

KPMG. (2017). *Operational Risk Management (ORM)*. Available at: KPMG Screen template (worldbank.org)

Lages, V. F. V. (2010). *Solvência II – Aplicação a uma companhia de seguros Não Vida*. Tese de Mestrado em Finanças, ISCTE-Instituto Universitário de Lisboa. Available at: Repositório do Iscte – Instituto Universitário de Lisboa: Solvência II: aplicação a uma companhia de seguros Não Vida (iscte-iul.pt)

Lavelle, D., O'Donnell, A., Pender, D., Roberts, D., & Tulloch, D. (2010). The Solvency II ORSA Process. *Society of Actuaries* in Ireland, 1-29. Available at: Microsoft Word - SolvencyII-OrsaProcess_20101123.doc (actuaries.ie)

Leonard-Barton, D. (1990). A Dual Methodology for Case Studies: Synergistic Use of a Longitudinal Single Site with Replicated Multiple Sites. *Organization Science*, 1(3), 248–266. Available at: A Dual Methodology for Case Studies: Synergistic Use of a Longitudinal Single Site with Replicated Multiple Sites | Organization Science (informs.org)

Madeira, J. (2014). Como os Espírito Santo foram à falência. Jornal SOL, 4 de Agosto Available at: Como os Espírito Santo foram à falência (sapo.pt)

Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT Governance Frameworks and COBIT - A Literature Review. In *AMCIS*. Available at: IT Governance Frameworks and COBIT - A Literature Review (core.ac.uk)

Meirinhos, M., & Osório, A. (2010). O estudo de caso como estratégia de investigação em educação. *EDUSER: Revista de Educação*, 2(2), 49–65. Available at: O estudo de caso como estratégia de investigação em educação | EduSer (ipb.pt)

Meyer, C. B. (2016). A Case in Case Study Methodology: *Field Methods*. Available at: A Case in Case Study Methodology - Christine Benedichte Meyer, 2001 (sagepub.com)

Moosa, I. A. (2007). Operational risk: a survey. *Financial markets, institutions & instruments*, Vol. *16*(4), 167–200. Available at: Operational Risk: A Survey - Moosa - 2007 - Financial Markets, Institutions & Instruments - Wiley Online Library

Oduoza, C. F. (2020). Framework for sustainable risk management in the manufacturing sector. *Procedia Manufacturing*, Vol. *51*, 1290–1297. Available at: Framework for Sustainable Risk Management in the Manufacturing Sector - ScienceDirect

Oliveira, M., Ferreira, C., Crisóstomo, P., & Ferreira, V. (2020). A história da queda do BES | PÚBLICO. Available at: A história da queda do BES | PÚBLICO (publico.pt)

Oluwafemi, A. K. (2019). *Accessing the effectiveness of operational risk management amongst Portuguese banks*. Dissertation presented as the partial requirement for obtaining a Master's degree in Statistics and Information Management. NOVA Information Management School Instituto Superior de Estatística e Gestão de Informação Universidade Nova de Lisboa. Available at: RUN: Accessing the effectiveness of operational risk management amongst portuguese banks (unl.pt)

Parlamento Europeu e do Conselho. (2009). Directiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, relativa ao acesso à actividade de seguros e resseguros e ao seu exercício (Solvência II). *Jornal Oficial da União Europeia*, 1-155. Available at: Directiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, relativa ao acesso à actividade de seguros e resseguros e ao seu exercício (Solvência II) (europa.eu)

Peters, Gareth and Sisson, Scott, Bayesian Inference, Monte Carlo Sampling and Operational Risk. (2006). Peters G.W. and Sisson S.A. (2006) "Bayesian Inference, Monte Carlo Sampling and Operational Risk". *Journal of Operational Risk*, Vol. *1*(3). Available at SSRN: Bayesian Inference, Monte Carlo Sampling and Operational Risk. by Gareth Peters, Scott Sisson :: SSRN

Pitselis, G. (2009). Solvency supervision based on a total balance sheet approach. *Journal of Computational and Applied Mathematics*, Vol. *233*(1), 83–96. Available at: Solvency supervision based on a total balance sheet approach - ScienceDirect

Rimkus, R. (2016). Financial scandals, scoundrels & crises. Available at: Parmalat - Financial Scandals, Scoundrels & Crises (econcrises.org)

Roth, S., Hauder, M., & Khosroshahi, P. (2013). Impact of solvency II on the enterprise architecture of insurances: A qualitative study in Germany. *Multikonferenz Wirtschaftsinformatik, Paderborn,* 1-12. Available at: (PDF) Impact of Solvency II on the Enterprise Architecture of Insurances: A Qualitative Study in Germany (researchgate.net)

Roux, M. C. L. (2010). Operational risk management in the short-term insurance industry and risk-based capital. Research Report. University of South Africa (UNISA). Available at: Microsoft Word - Research Report.docx (core.ac.uk)

Samad-Khan, A. (2008). *Modern operational risk management. Emphasis,* Vol. *2,* 26-29. Available at: Emp8-2_6-3-08.qxp (sbp.org.pk)

Scherer, M., & Stahl, G. (2021). The standard formula of Solvency II: A critical discussion. *European Actuarial Journal*, Vol. *11*(1), 3–20. Available at: The standard formula of Solvency II: a critical discussion | European Actuarial Journal (springer.com)

Siva, V., Gremyr, I., Bergquist, B., Garvare, R., Zobel, T., & Isaksson, R. (2016). The support of Quality Management to sustainable development: A literature review. *Journal of Cleaner Production*, Vol. *138*, 148–157. Available at: The support of Quality Management to sustainable development: a literature review - ScienceDirect

Stake, R. E. (1998). *Investigación con estudio de casos*. Ediciones Morata.

Steffen, T. (2008). Solvency II and the Work of CEIOPS. *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. *33*(1), 60–65. Available at: Solvency II and the Work of CEIOPS | SpringerLink

The Institute of Operational Risk. (2021). Operational Loss Events: Internal and External Data. The Institute of Operational Risk, Sound Practice Guidance. Available at: Operational Loss Events – Institute of Operational Risk (ior-institute.org)

Toms, S. (2019). Financial scandals: A historical overview. *Accounting and Business Research*, Vol. *49*(5), 477–499. Available at: Full article: Financial scandals: a historical overview (tandfonline.com)

Torre-Enciso, M. I. M., & Barros, R. H. (2012). Operational Risk Management for Insurers. *International Business Research*, Vol. *6*(1), 1. Available at: Operational Risk Management for Insurers | Torre-Enciso | International Business Research | CCSE (ccsenet.org)

van Grinsven, J., & Bloemkolk, R. (2009). Solvency II: Dealing with operational risk. *FSI magazine*. Available at: Solvency-II-Dealing-with-Operational-Risk-FSI-Magazine.pdf (vgc.nl)

Varela, V. L. A. (2016). *Apresentação de uma metodologia para a avaliação do impacto de variáveis de negócio nos níveis de risco operacional das Instituições financeiras portuguesas.* Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Estatística e Gestão de Informação, Especialização em Análise e Gestão de Informação. NOVA Information Management School. Instituto Superior de Estatística e Gestão de

Informação. Universidade Nova de Lisboa. Available at: RUN: Apresentação de uma metodologia para a avaliação do impacto de variáveis de negócio nos níveis de risco operacional das Instituições financeiras portuguesas (unl.pt)

Vilas, S. M. (2015). *A implementação da gestão de risco operacional numa instituição financeira portuguesa tendo como base a abordagem de medição avançada: Processo, desafios e oportunidades.* 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. NOVA Information Management School. Instituto Superior de Estatística e Gestão de Informação. Universidade Nova de Lisboa. Available at: RUN: A implementação da gestão de risco operacional numa instituição financeira portuguesa tendo como base a abordagem de medição avançada: processo, desafios e oportunidades (unl.pt)

Vukovic, O. (2015). Operational Risk Modelling in Insurance and Banking. *Journal of Financial Risk Management*, Vol. *4*(03), 111. Available at: Operational Risk Modelling in Insurance and Banking (scirp.org)

Walker, R. (2022). The increasing importance of operational risk in enterprise risk management. *The Journal of Enterprise Risk Management,* Vol. *1*(1), 82-96. Available at: 61_operational_risk_ERM.pdf.pdf (actuaries.ie)

Wicher, E. W., Chaves, S., Campello, M., Machado, F. M., Silveira, F. da, Ortiz, L. C. V., Mello, V. D., Vidolin, A. C., Santos, F. B. dos, Jesus, I. N. de, Correa, J. C., Barbosa, T. da S., Weersma, L. A., Barros, J. L. C., Barros Júnior, E. de A., Coimbra, D. B., Oliveira, M. de L. M. C. de, Moser, D. D. N., Amaro, E. S. D. de M., Andrade, D. F. (2018). Gestão pela Qualidade—Vol. *3*. 10.5935. Available at: GQ_volume3.pdf (poisson.com.br)

Williams, R., Bertsch, B., Dale, B., van, der W. T., van, I. J., Smith, M., & Visser, R. (2006). Quality and risk management: What are the key issues? *The TQM Magazine*, Vol. *18*(1), 67–86. Available at: Quality and risk management: what are the key issues? | Emerald Insight

Yin, R. K. (1993). *Applications of Case Study Research*. SAGE Publications. Available at: Applications of case study research. (apa.org)

Yin, R. K. (2005). *Estudos de caso: Planeamento e métodos*. Bookman. Available at: Repositório de Informação Acessível: Estudos de caso : planejamento e métodos (ufrn.br)

ANEXO A

FATORES DO RISCO OPERACIONAL

Fatores de Calibração	Descrição
TP_{life}	Total de provisões técnicas de seguro de vida (bruto de resseguro), com um limite mínimo igual a zero. Isto também incluiria obrigações unitárias de negócios e de vida, tais como anuidades.
$TP_{SLT\ Health}$	Provisões técnicas correspondentes ao seguro de saúde (resseguro bruto) correspondentes ao SLT de Saúde com um piso igual a zero
$TP_{life-ul}$	Total de provisões técnicas de seguro de vida para negócios ligados a unidade (resseguro bruto), com um piso igual a zero.
TP_{nl}	Total das provisões técnicas de seguros não vida (resseguro bruto), com um piso igual a zero (excluindo obrigações de vida, tais como obrigações em contratos não vida, tais como anuidades).
$TP_{Non-SLT\ Health}$	Provisões técnicas correspondentes a seguros de saúde correspondentes à Saúde Não SLT (resseguro bruto), com um piso igual a zero.
$Earn_{life}$	Total de prémios adquiridos do ramo Vida (resseguro bruto), incluindo negócios ligados a unidades.

$Earn_{SLT\ Health}$	Prémios totais obtidos correspondentes ao seguro de saúde correspondente ao SLT de Saúde (resseguro bruto).
$Earn_{life-ul}$	Prémio total vitalício para negócio ligado a unidade (resseguro bruto)
$Earn_{nl}$	Prémios totais não vitalícios (resseguro bruto)
$Earn_{Non-SLT\ Health}$	Prémios totais auferidos correspondentes ao seguro de saúde correspondente à Saúde Não SLT (resseguro bruto)
P_{life_f}	Prémios - seguro de vida, que indica um fator de carga ou um fator de ajustamento da taxa aplicado aos prémios de base das apólices de seguro de vida
P_{nl_f}	Prémios - seguro não-vida, que indica um fator que é aplicado aos prémios das apólices de seguro não-vida

ANEXO B

GRUPO FIDELIDADE

Marca	Descrição
FIDELIDADE	Fidelidade - Companhia de Seguros, S.A., é a sociedade que encabeça o Grupo Fidelidade e a empresa líder do mercado de seguros português, disponibilizando uma vasta gama de produtos nos ramos Não-Vida e Vida, contando, como acima já se referiu, com operações em diversas geografias. Marca sob a qual são comercializados os Produtos Vida e Não-Vida (exceto seguros de saúde). Marca de referência presente em todos os canais de distribuição
MULTICARE	A Multicare – Seguros de Saúde, S.A., é a seguradora do grupo vocacionada para os seguros de doença, gerindo a marca líder do ramo saúde em Portugal, com mais de um milhão de clientes. Dispõe da maior rede privada de prestadores de saúde em Portugal (com cerca de 5 mil prestadores de cuidados de saúde) e de uma rede com mais de 700 prestadores de referência em Moçambique, Angola, Cabo Verde, entre outros países. Marca sob a qual são comercializados os Seguros de Saúde com apoio de um conjunto de Prestadores de Cuidados de Saúde, e uma gama de soluções adequadas às necessidades dos clientes, através de Planos Individuais e de Grupo
FIDELIDADE ASSISTANCE	A Fidelidade Assistência – Companhia de Seguros, S.A., é uma seguradora especializada em seguros de Assistência e de Proteção Jurídica. Atuando essencialmente como resseguradora, é líder de mercado em

Marca	Descrição
	Portugal. Dá suporte aos seus Clientes, à escala global, através da sua rede de representantes, e da rede APRIL internacional de que faz parte.
via directa COMPANHIA DE SEGUROS S.A.	A Via Directa – Companhia de Seguros S.A., é a seguradora do Grupo vocacionada para a comercialização de seguros através de canais remotos (telefone e internet), operando através de várias marcas, entre elas a OK!Teleseguros. É pioneira na venda de seguros online em Portugal e líder no segmento das seguradoras diretas.
	A Companhia Portuguesa de Resseguros, S.A., atua no resseguro dos ramos Não-Vida em Portugal, subscrevendo essencialmente riscos ao abrigo dos Tratados não Proporcionais com a Fidelidade.

ANEXO C

RISCOS MATERIAIS COM AVALIAÇÃO

Área	Risco	Processo	VaR	Controlos	Ambiente de Controlo
A14	3.6.4 Atrasos na execução de operações	04.04.04 Gestão de processos relacionados Tribunal de Trabalho	949 906,00 €	0	Médio
A10	3.6.4 Atrasos na execução de operações	02.02.01 Contratos de resseguro facultativo cedido	225 520,00 €	1	Alto
A4	3.6.9 Erros de cálculo	10.02.01 Planeamento orçamental	170 968,00 €	2	Alto
A14	3.6.3 Falhas na execução das operações	04.02.02 Gestão de reembolsos de sinistros	167 410,00 €	2	Médio
A14	3.6.2 Falhas nos pagamentos ou liquidações	04.01.04 Encerramento de processos de sinistros	167 410,00 €	0	Médio Alto
A14	3.6.2 Falhas nos pagamentos ou liquidações	04.02.01 Pagamentos aos sinistrados/ tomadores/ lesados	167 168,00 €	0	Médio
A10	3.5.1 Falhas no desempenho de contrapartes	02.01.01 Tratados de resseguro cedido	155 797,00 €	1	Alto

Área	Risco	Processo	VaR	Controlos	Ambiente de Controlo
A10	3.5.1 Falhas no desempenho de contrapartes	02.01.01 Tratados de resseguro cedido	155 797,00 €	1	Médio
A14	4.1.1 Fraude externa	04.02.01 Pagamentos aos sinistrados/ tomadores/ lesados	148 444,00 €	2	Médio
A14	3.6.3 Falhas na execução das operações	04.01.03 Gestão de processos de sinistros	86 554,00 €	1	Médio Baixo
A13	4.1.1 Fraude externa	03.01.02 Pagamento de estornos	66 930,00 €	1	Médio Alto
A14	3.4.2 Falhas no fornecimento de bens e serviços	04.01.03 Gestão de processos de sinistros	55 555,00 €	2	Médio
A10	1.3.1 Falhas na conceção, implementação ou distribuição de produtos	01.01.02 Implementação/lançamento de produtos	54 612,00 €	3	Médio Alto
A4	3.6.3 Falhas na execução das operações	07.02.02 Despesas em serviço	48 497,00 €	1	Alto
A5	3.6.4 Atrasos na execução de operações	08.05.03 Faturação de prestadores/ fornecedores	44 119,00 €	2	Alto
A3	3.7.1 Deficiências na contratualização de subcontratação	08.05.01 Contratação de prestadores/ fornecedores	41 430,00 €	5	Alto
A14	3.6.3 Falhas na execução das operações	08.02.01 Gestão de reclamações	40 325,00 €	0	Médio Baixo
A10	3.6.9 Erros de cálculo	03.02.03 Gestão de contas de resseguro	40 325,00 €	2	Alto
Total			**2 786 767,00 €**		

ANEXO D

CONTROLOS COM DEFICIÊNCIAS

#	Controlo	Tipo	Execução	Eficácia	Evidência	Áreas Mitigadas
1	Requisitos legais e regulamentares	Manual	Baixo	Alto	Baixo	A3
2	Validação por colaboradores	Manual	Alto	Baixo	Alto	A11
3	Restrições de sistema	Manual	Alto	Baixo	Alto	A11
4	Alerta de sistema	Automático	Alto	Baixo	Alto	A11
5	Segregação de funções	Manual	Alto	Baixo	Alto	A11
6	Restrições de sistema	Automático	Alto	Baixo	Alto	A11
7	Análise periódica	Manual	Alto	Baixo	Alto	A11
8	Análise periódica	Manual	Alto	Baixo	Alto	A11
9	Reconciliação	Manual	Alto	Baixo	Alto	A11
10	Validação por colaboradores	Manual	Alto	Baixo	Alto	A11
11	Validação por colaboradores	Manual	Alto	Baixo	Alto	A11
12	Alerta de sistema	Automático	Alto	Baixo	Alto	A12
13	Validação por colaboradores	Manual	Alto	Baixo	Alto	A14
14	Análise periódica	Manual	Alto	Baixo	Alto	A14
15	[INV] Autorização de operações	Manual	Alto	Baixo	Alto	A14
16	Validação por colaboradores	Manual	Alto	Baixo	Médio	A14
17	Validação por colaboradores	Manual	Alto	Baixo	Alto	A14
18	Validação por colaboradores	Manual	Médio	Baixo	Médio	A14
19	Validação por colaboradores	Manual	Alto	Baixo	Alto	A14
20	Validação por colaboradores	Manual	Alto	Baixo	Alto	A10
21	Validação por colaboradores	Manual	Alto	Baixo	Alto	A8
22	Validação por colaboradores	Manual	Alto	Baixo	Alto	A8
23	Reconciliação	Manual	Alto	Baixo	Alto	A5
24	Autorização de operações	Manual	Alto	Baixo	Alto	A4
25	Análise periódica	Manual	Alto	Baixo	Alto	A4
26	Validação por colaboradores	Manual	Alto	Baixo	Alto	A4
27	Validação por colaboradores	Manual	Alto	Baixo	Alto	A4
28	Validação por colaboradores	Manual	Médio	Baixo	Médio	A7

#	Controlo	Tipo	Execução	Eficácia	Evidência	Áreas Mitigadas
29	Validação por colaboradores	Manual	Alto	Baixo	Alto	A7
30	Validação por colaboradores	Manual	Alto	Baixo	Médio	A2
31	Segregação de funções	Manual	Alto	Baixo	Alto	A11
32	Reconciliação	Manual	Alto	Alto	Baixo	A10
33	Alertas de sistema sobre prazos	Manual	Alto	Alto	Baixo	A4
34	Validação por colaboradores	Manual	Alto	Alto	Baixo	A7
35	Reconciliação	Manual	Médio	Alto	Alto	A14
36	Análise periódica	Manual	Médio	Alto	Médio	
37	Reconciliação	Manual	Médio	Alto	Alto	A8
38	Validação por colaboradores	Manual	Médio	Alto	Médio	A8
39	Repositório de entidades	Manual	Alto	Alto	Médio	A12
40	Análise periódica	Manual	Alto	Alto	Médio	A3
41	Alertas do sistema no Outlook	Manual	Alto	Alto	Médio	A6
42	Validação por colaboradores	Manual	Alto	Alto	Médio	A15
43	Validação por colaboradores	Manual	Alto	Alto	Médio	A15
44	Reconciliação	Manual	Alto	Alto	Médio	A6
45	Reconciliação	Manual	Alto	Alto	Médio	A6
46	Alertas do sistema Outlook	Manual	Alto	Alto	Médio	A13
47	Validação por colaboradores	Manual	Alto	Alto	Médio	A13
48	Validação por colaboradores	Manual	Alto	Alto	Médio	
49	Reuniões semanais com o prestador de serviços multirrisco	Manual	Alto	Alto	Médio	A12

ANEXO E

OPORTUNIDADES DE MELHORIA

#	Área	Aplicativo	Risco com Var>1M€	Risco Material com avaliação	Risco Material sem avaliação	Risco Imaterial	Controlos com deficiências	Risco material sem controlo	Risco com Ambiente de controlo deficiente	Risco com Eventos de Perda
A	A14	Novo	3				1			
B	A14	Novo	1				2			
C	A14	Novo	1				2			
D	A14	Novo	1				2			
E	A14	Novo	1				1			
F	A14	Novo	2	1			1			
G	A14	Novo	1							
H	A10			1			1			
I	A10			1						
J	A3			1						
K	A3			1						
L	A4			2			1			
M	A4			1			1			

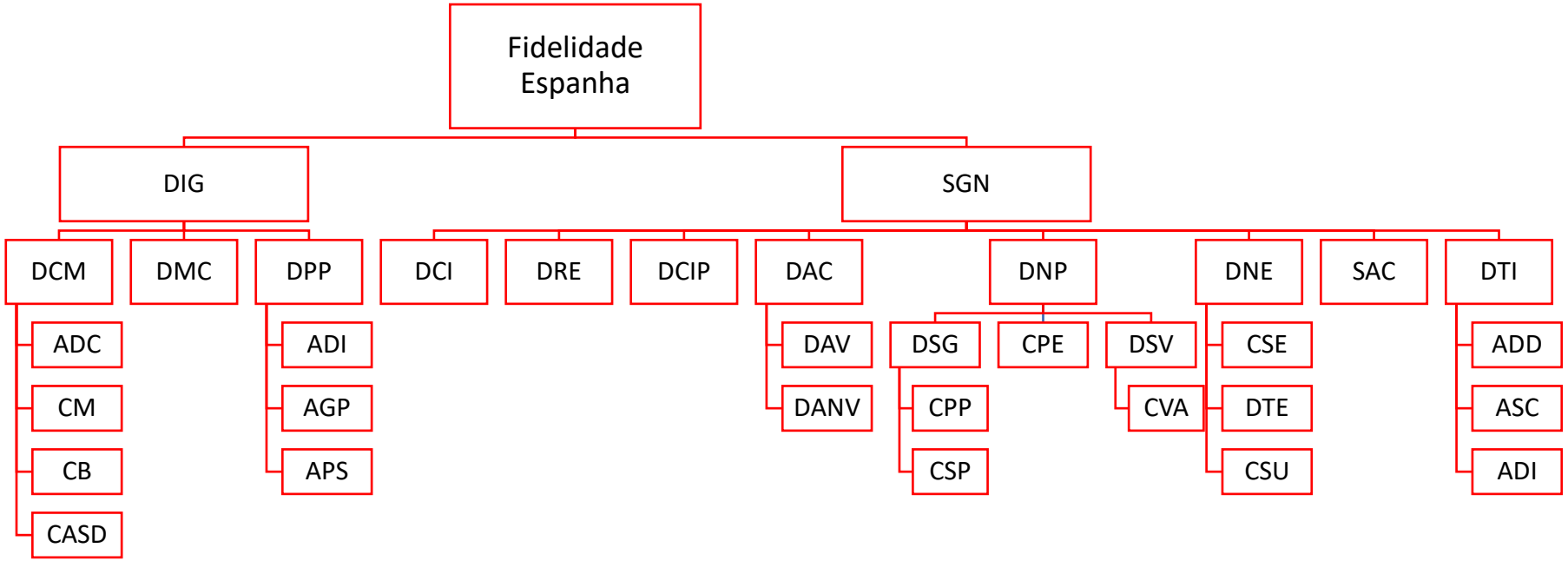
#	Área	Aplicativo	Risco com Var>1M€	Risco Material com avaliação	Risco Material sem avaliação	Risco Imaterial	Controlos com deficiências	Risco material sem controlo	Risco com Ambiente de controlo deficiente	Risco com Eventos de Perda
N	A14	Novo		1			4	2	2	
O	A14	Novo		3			3	2		1
P	A14	Novo		1			2			
Q	A14	Novo		2			3	2	6	
R	A14	Novo		1			4	1	1	
S	A14	Novo		1						
T	A14	Novo		1			1			
U	A9	Outlook			4			4		
V	A9	SAS			1			1		
W	A15				1			1	1	
X	A13				1				1	
Y	A11				1				1	
Z	A16				1			1	1	
AA	A7				1				1	
AB	A4					1				
AC	A11					1				
AD	A11					1				
AE	A16					1			1	
AF	A7					1				
AG	A7					1	3			
AH	A7					1	4			
AI	A7					1				
AJ	A7					1				
AK	A11						1	1		1
AL	A11						1			

#	Área	Aplicativo	Risco com Var>1M€	Risco Material com avaliação	Risco Material sem avaliação	Risco Imaterial	Controlos com deficiências	Risco material sem controlo	Risco com Ambiente de controlo deficiente	Risco com Eventos de Perda
AM	A11	Fidemed					1			
AN		GIS					2			
AO		GIS					1			
AP							1			
AQ	A11						1			
AR	A14						1			
AS	A8						1			
AT	A5						1			
AU	A4						1			
AV	A4						1			
AW	A4						2			
AX	A4						1			
AY	A4						1			
AZ	A7						3			
BA	A7						1			
BB	A11						1			
BC	A4	Outlook					1			
BD	A4						1			
BE	A7						1			
BF	A8						2			
BG	A12						1			
BH	A3						1			
BI	A3						1			
BJ	A15						1			
BK	A13	Outlook					1			
BL	A7						1			
BM	A12						1			

#	Área	Aplicativo	Risco com Var>1M€	Risco Material com avaliação	Risco Material sem avaliação	Risco Imaterial	Controlos com deficiências	Risco material sem controlo	Risco com Ambiente de controlo deficiente	Risco com Eventos de Perda
BN	A14	Novo						1		
BO	A11							1		
Total		**22**	**7**	**14**	**7**	**9**	**46**	**11**	**9**	**2**

ANEXO F

ESTRUTURA ORGANIZACIONAL


Fidelidade Espanha
DIG
SGN
DCM
DMC
DPP
DCI
DRE
DCIP
DAC
DNP
DNE
SAC
DTI
ADC
CM
CB
CASD
ADI
AGP
APS
DAV
DANV
DSG
CPE
DSV
CPP
CSP
CVA
CSE
DTE
CSU
ADD
ASC
ADI