A responsabilidade pela Gestão dos Riscos de Negócio

Ricardo Mário Ferrás Pestana

Dissertação de Mestrado

Mestrado em Auditoria

Porto – 2015

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

A responsabilidade pela Gestão dos Riscos de Negócio

Ricardo Mário Ferrás Pestana

Dissertação de Mestrado

Apresentada ao Instituto de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação do

Dr. Carlos Mendes

Porto – 2015

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

Resumo

A temática da Gestão dos Riscos de Negócio tem tido uma grande importância ao longo dos últimos anos, protegendo e acrescentando valor às organizações e aos "*stakeholders"*, motivado pelas grandes crises económicas.

A Gestão dos Riscos de Negócio permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos com maior impacto e probabilidade.

Este trabalho tem como principal objetivo apurar como as organizações atribuem a responsabilidade na Gestão dos Riscos de Negócio.

Em Portugal, as sociedades emitentes de ações admitidas à negociação em mercado regulamentado, são obrigadas a disponibilizar anualmente informação sobre o grau de acolhimento do Código de Governo das Sociedades, o qual consiste num conjunto de recomendações elaboradas, onde parte dessas recomendações são referentes a Gestão dos Riscos de Negócio.

Para o efeito analisámos os últimos relatórios de gestão, na sua componente de governo das sociedades das empresas que integram o índice do PSI-20 da Euronext de Lisboa, de modo a apurar e a concluir quais são as áreas das empresas responsáveis pela Gestão dos Riscos de Negócio.

Palavras chave: Gestão; A responsabilidade pela Gestão dos Riscos de Negócio; Risco.

Abstract

Enterprise Risk Management subject has a greater importance over the last years, protecting and adding value to the organizations and to the stakeholders, motivated by the great economic crisis.

Enterprise Risk Management allows managers to identify, assess and manage the risks according to the uncertainty level, focusing on the risks with bigger impact and probability.

The main goal of this work is to ascertain how the organizations assign the responsibility on Enterprise Risk Management.

In Portugal, the societies that issue shares admitted to the negotiation in a regulated market, are yearly obliged to make available information about the Corporate Governance Code compliance degree, which consists in a joint of produced recommendations, where part of these recommendations are regarded to Enterprise Risk Management.

For this purpose, we analyzed the last management reports, in its governance component of the companies that integrate the index of the PSI-20 of Lisbon Euronext, to investigate which are the companies areas accountable for Enterprise Risk Management.

Key words: Management**;** Responsibility for the Enterprise Risk Management; Risk**.**

Agradecimentos

Agradeço aos meus pais e em especial à Carina pelo incentivo, apoio e compreensão que sempre me dispensaram ao longo do meu percurso académico.

O meu sincero agradecimento a todos aqueles que, de formas diferentes contribuíram para que a realização deste trabalho fosse possível.

Agradeço também ao Professor Carlos Mendes, pela disponibilidade e o apoio demonstrado durante a concretização desta dissertação.

Lista de Abreviaturas

ABNT - Associação Brasileira de Normas Técnicas

AIRMIC - *The Association of Insurance and Risk Managers*

AS – *Australian Standard*

CEO – *Chief Executive Officer*

CFO – *Chief Financial Officer*

COSO - *The Committee of Sponsoring Organizations of the Treadway Commission*

ERM – *Enterprise Risk Management*

FERMA - *Federation of European Risk Management Associations*

IEC - *International Electrotechnical Commission*

IFAC - *The International Federation of Accountants*

IIA – *The Institute of Internal Auditors*

IPAI - Instituto Português de Auditoria Interna

IRM - *The Institute of Risk Management*

ISA - *International Standard on Auditing*

ISO - *International Organization for Standardization*

NBR – Norma Brasileira

NZS - *New Zealand Standard*

PWC – *PricewaterhouseCoopers*

SOX – *Sarbanes-Oxley Act*

Índice

Lista de Figuras

Lista de Tabelas

Introdução

As consequências que podem resultar de uma falha nos controlos, a rápida evolução tecnológica, a velocidade de mudança, a crescente complexidade da economia, as crescentes expectativas dos consumidores, a agressividade da concorrência, entre outros factores, afectam as organizações tornado-as mais vulneráveis. Estas causas expõem as organizações a inúmeros riscos, levando-as a alterarem-se e adaptarem-se, de modo a assegurar um crescimento sustentado.

As alterações de natureza estrutural da envolvente conduziram a uma mudança na definição de Auditoria Interna do IIA em Junho de 1999 (Alves 2009: p.29). Anteriormente o objectivo era assegurar a qualidade da informação e a proteção dos ativos. Como consequência dessas alterações, a Auditoria Interna passou a reconhecer os riscos e as eventuais perdas de oportunidades, de forma a ajudar as organizações a atingir os seus objetivos.

O presente trabalho pretende apurar qual é a área/função da empresa responsável pela Gestão dos Riscos de Negócio.

O trabalho encontra-se dividido em dois capítulos. No primeiro capítulo são expostos os estudos e as abordagens já realizadas por vários autores sobre este tema. Numa primeira fase é apresentada a Lei *Sarbanes-Oxley*, conceitos sobre a Gestão de Risco de Negócio, a importância de uma adequada Gestão de Riscos de Negócio numa organização e o papel da CMVM relativamente ao Bom Governo das Sociedades Cotadas em matéria de Gestão de Riscos de Negócio. Numa segunda fase é abordado o conceito de Auditoria Interna, a sua evolução, a mudança do seu paradigma, os objetivos e funções, o seu papel na organização, a independência e o papel do auditor interno.

No segundo capítulo é efetuada uma exposição do modo e forma como a investigação se concretiza, descrevendo a população objeto de estudo, assim como os procedimentos adotados na recolha de dados.

O presente estudo termina com o 3.º Capítulo onde são apresentadas as conclusões teóricas e práticas relativas ao estudo de caso apresentado.

A principal limitação deste estudo prende-se com a impossibilidade de obtenção de dados diretos através de entrevistas, os quais permitiriam complementar e validar a análise de conteúdo, nomeadamente dos relatórios.

Atendendo ao facto de neste estudo só terem sido recolhidos os relatórios referente as empresas do PSI-20 da "*Euronext"* de Lisboa, sugere-se que numa investigação futura o universo em análise seja alargado a todas as sociedades emitentes de ações admitidas à negociação em mercado regulamentado.

1. Capítulo I [Revisão da Literatura]

1.1. A Gestão das Organizações

Vivemos numa sociedade dominada por organizações, de grandes ou pequenas dimensões, com ou sem fins lucrativos, nas quais as pessoas trabalham em conjunto com vista à prossecução de objetivos que não seriam possíveis atingir se as mesmas trabalhassem isoladamente (Teixeira, 2005: p.3).

De Acordo com Almeida (2005: p.82), a palavra "Gestão" constitui a tradução da sigla inglesa "*management*", que alguns autores preferem designar por "administração". A Gestão é considerada a coordenação e supervisão do trabalho dos outros, de modo a que suas atividades sejam desempenhadas eficiente e eficazmente (Marques, 2012: p.3). De uma forma muito simples e abrangente é possível definir o conceito de Gestão como o processo de conseguir resultados com o esforço dos outros (Teixeira, 2005: p.3).

1.1.1. Funções da Gestão

Segundo Teixeira (2005: p.3), a tarefa da Gestão é interpretar os objetivos propostos e transformá-los em ação empresarial, através do planeamento, da organização, da direção e do controlo de todos os esforços realizados em todas as áreas e em todos os níveis da empresa, a fim de atingir esses mesmos objetivos.

A gestão abarca portanto quatro funções fundamentais:

- Planear;
- Organizar;
- Dirigir;
- Controlar.

1.1.1.1. Função Planear

Planear, significa determinar antecipadamente o que deve ser feito e como ser feito (Almeida, 2005: p.84). Consiste em definir como a organização irá atingir

determinado objetivo. Contudo, é preciso ter um conjunto de informações para determinar os caminhos mais adequados a serem seguidos (Oda *et al*., 2008: p.74).

De acordo com Santos (2008: p.30), o planeamento é a definição da estratégia, dos objetivos, da missão e da tática. Uma vez que os planos estabelecem a forma como a empresa se irá desenvolver no futuro, é necessário definir quem vai atuar para que determinado objetivo aconteça, quem são os intervenientes, como se relacionam, com que meios e que atividade ou função cabe a cada um isoladamente ou em grupo (Teixeira, 2005: p.4).

De uma forma mais ampla Nelson *et al*. (2006: p.12), assumem que o trabalho dos gestores consiste em desenvolver planos, que determinem os objetivos que uma empresa irá procurar atingir, os produtos e serviços que irá fornecer, de que forma e a quem os irá entregar, e a que preço.

1.1.1.2. Função Organizar

Organizar, consiste em estabelecer relações formais entre as pessoas e também entre as pessoas e os recursos, de modo a atingir os objectivos propostos (Teixeira, 2005: p.4).

De acordo com Stoner *et al.* (1985: p.6) organizar consiste "*no processo de arrumar e alocar o trabalho, a autoridade e os recursos entre os membros de uma organização, de modo a que eles possam alcançar eficientemente os objetivos da mesma*". Baseia-se em estabelecer uma estrutura, por mínima que seja, para desempenhar as suas atividades (Oda *et al.,* 2008: p.81).

A função organizar é composta pelas seguintes atividades (Livian, 1987: p.14):

- Estabelecer relações formais entre as pessoas e os recursos, para atingir os objetivos do plano;
- Definir quem faz o quê e quando;
- Definir as relações e as interações entre as pessoas e os grupos;
- Afetar os recursos e meios às pessoas e aos grupos.

Segundo Teixeira (2005: p.4), no planeamento é fundamental a definição das funções que competem a cada elemento da organização, quais os recursos disponíveis e como se distribuem. Mas se nada se seguir, fica tudo na mesma, é necessário fazer com que as pessoas o façam, ou seja dirigir.

1.1.1.3. Função Dirigir

De acordo com Almeida (2005: p.85), a função dirigir é compreendida como o processo de determinar, afetar ou controlar o comportamento dos outros.

O processo de dirigir o comportamento dos outros envolve 3 aspetos fundamentais: liderar, motivar e comunicar.

- Liderar: é a capacidade de conseguir com que os outros façam o que o líder quer (Teixeira, 2005: p.4). Liderar é uma forma de comunicação, baseada no prestígio aceite pelos dirigidos, constituindo um processo de influenciar as atividades de um individuo ou grupo, para a prossecução dos objetivos (Almeida, 2005: p.85).
- Motivar: consiste em reforçar a vontade das pessoas, no sentido de as mesma se esforçarem para alcançar os objetivos das organizações (Teixeira, 2005: p.4). Para conseguir motivar, há que procurar a conciliação entre os objetivos individuais e organizacionais (Almeida, 2005: p.85).
- Comunicar: é um processo de transferência de informações, ideias ou sentimentos (Almeida, 2005: p.85).

De acordo com Nelson *et al*. (2006: p.13), grandes líderes podem proporcionar enormes acontecimentos, inspirando os seus funcionários para ações e objetivos extraordinários.

1.1.1.4. Função Controlar

O controlo é um processo de comparação entre o atual desempenho da organização e as normas previamente estabelecidas, indicando as eventuais ações corretivas (Teixeira, 2005: p.5). É necessário comparar os resultados com os objetivos e introduzir ações de correção (Almeida, 2005: p.85).

Essas ações têm caráter pedagógico, isto é, as pessoas necessitam de formação para conseguirem fazer melhor, outras vezes é necessário reformular os planos inicialmente estabelecidos (Teixeira, 2005: p.5).

Para atingirem os seus objetivos e os objetivos da empresa, os gestores necessitam de estabelecer padrões de desempenho com base nas metas e objetivos da empresa, medir e comunicar o desempenho real, comparar ambos e pôr em prática ações corretivas ou preventivas sempre que seja necessário (Nelson *et al*., 2006: p.13).

1.2. Gestão de Risco de Negócio

1.2.1. Sarbanes-Oxley Act

No final do século XX, os Estados Unidos da América depararam-se com uma crise, protagonizada por consecutivos escândalos financeiros que acabaram por afetar conceituadas empresas americanas. As principais ilegalidades ocorridas foram protagonizadas pelos gestores das empresas, o que acabou por desencadear uma crise de confiança no mercado global. Foi neste cenário de insegurança que surge nos EUA, a lei SOX (*Sarbanes-Oxley*), assinada pelo Presidente Norte-americano em 30 de Julho de 2002 com o objetivo de melhorar o reporte financeiro das Empresas e a Proteção dos Investidores (Alves, 2009: p.15).

Segundo Gonçalves (2009: p.12), a lei SOX é um dispositivo legislativo que impôs reformas substanciais para as organizações. O objetivo principal é nortear a visibilidade dos investidores, com a procura da exatidão e fiabilidade das informações financeiras divulgadas pelas empresas, com base no aperfeiçoamento do controlo interno sobre as informações.

De acordo com Pires (2008: p.20):

"A SOX centra-se na revisão dos procedimentos de Corporate Governance para empresas cotadas, nacionais ou estrangeiras, especialmente os relacionados com a verificação da adequação da informação relativa a resultados e com a divulgação do relato financeiro. Também estabelece a responsabilidade pessoal do CEO (Chief Executive Officer) e do CFO (Chief Financial Officer) pela adequação desta informação, disposições sobre proteção da fraude, incluindo requisitos para a independência do auditor, a rotação das empresas que prestam os serviços de auditoria, uso apropriado de medidas financeiras, proteção dos dispositivos de comunicação de práticas indevidas (whistleblowers)".

Conforme citado por Barros (2012: p.7), as principais vantagens da *SOX* para as organizações são:

- A viabilização dos controlos internos;
- Avaliação de fluxo de informação;
- O mapeamento de processos críticos das empresas;
- A alocação de responsabilidades aos responsáveis internos;
- A identificação de não conformidades;
- A Gestão de Risco de Negócio associada a estes processos.

O objetivo desta lei visou fundamentalmente criar um novo ambiente de controlo, apoiado por um conjunto de novas responsabilidades e sanções aos administradores para coibir as práticas lesivas que expõem as sociedades de capital aberto a elevados níveis de risco e que fazem com que os "*stakeholders"* se retraiam em participar no capital dessas empresas (Pereira, 2012: p.37).

1.2.2. Conceitos de Gestão de Risco de Negócio

De Acordo com Vale (2011: p.14):

"O conceito de "risk management" sintetiza um conjunto de asserções e meios afetos ao escrutínio, avaliação e relato do risco do negócio, nasceu nos Estados Unidos da América, e foi pela primeira vez mencionado em 1956, num artigo publicado na "Harvard Business Review", num contexto então muito circunscrito ao alargamento de responsabilidades da função de gestor de seguros e muito marcado por discussões académicas."

A Gestão dos Riscos de Negócio (IIA, 2004: p.3), é um processo estruturado, consistente e contínuo, implementado em toda a organização para identificar, avaliar, medir e relatar ameaças e oportunidades que afetam a realização dos seus objetivos.

Segundo o FERMA (2003: p.3):

"A Gestão dos Riscos de Negócio é um elemento central na gestão da estratégia de qualquer organização. É o processo através do qual as organizações analisam metodicamente os riscos inerentes às respetivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades."

O COSO (2004: p.4) define o risco como sendo a possibilidade de um evento ocorrer e afetar negativamente a realização dos objetivos definidos. Os eventos podem resultar de fontes internas ou externas à organização e podem causar impactos positivos e/ou negativos. Nesse sentido, o COSO refere que os eventos que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os riscos de impacto positivo podem contrabalançar com os de impacto negativo ou podem representar oportunidades que, por sua vez, representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos.

Conforme citado por Pereira (2012: p.4):

"A Gestão dos Riscos de Negócio admite que qualquer organização, independentemente do seu tamanho, fim lucrativo, origem de capitais, ou atividade

económica, existe para gerar valor para os "stakeholders". Todas as entidades enfrentam incertezas, o desafio da administração é determinar o nível de incerteza que a sua organização consegue enfrentar, aumentando, desta forma, o seu valor para os "stakeholders" e para ela própria."

Segundo Ferreira (2010: p.15), a Gestão dos Riscos de Negócio é um meio para atingir um fim e não um fim em si mesmo É um processo educativo que nos consciencializa para a existência de riscos e que aos gestores cabe a responsabilidade de os gerir.

O processo de Gestão dos Riscos de Negócio consiste em (Almeida, 2008: p.20):

- Definir e estabelecer o enquadramento e a infraestrutura da gestão de Risco;
- Identificar e Avaliar os riscos de negócio;
- Avaliar as estratégias de Gestão de Risco;
- Desenhar e implementar ações de Gestão do Risco;
- Monitorar e reportar as ações de risco;
- Informação para a tomada de Decisão.

De acordo com Santos (2013: p.23):

"Dada a importância e a necessidade de controlar os riscos que afetam as organizações, cada vez mais complexos, abrangentes e universais, há iniciativas mundiais no sentido de tentar padronizar orientações/diretrizes, sobre a Gestão de Risco de Negócio de forma a garantir a uniformização de conceitos, processos para implementação da Gestão de Riscos de Negócio, estrutura organizacional e objetivos da Gestão de Risco de Negócio.

Atualmente existem várias metodologias de Gestão de Riscos de Negócio, entre as quais se destaca:

- Norma de Gestão de Riscos de Negócio da FERMA: *Risk Management Standard* emitida em 2002 pela *Federation of European Risk Management Associations*;
- Norma de Gestão de Riscos Australiana AS/NZS 4360 (2004) - *Risk Management Guidelines*;
- Gestão de Risco Empresarial: ERM – *Enterprise Risk Management Framework*, emitido pelo COSO em 2004;e
- ISO 31000 da *International Organization for Standardization* emitida em 2009."

1.2.3. Gestão de Risco Empresarial: ERM – *Enterprise Risk Management Framework*

Os escândalos financeiros das empresas que manipularam as informações financeiras como a "*Enron"*, "*Tyco"*, "*WorldCom"* e outras, afetaram de forma significativa a confiança dos investidores, funcionários e outros "*stakeholders*", vindo reforçar a necessidade do desenvolvimento de um modelo de Gestão de Risco Empresarial que fornecesse princípios e conceitos chave, uma linguagem comum e que constituísse um guia para a Gestão de Riscos de Negócio nas organizações (Ferreira, 2010: p.19).

De acordo com Santos (2013: p.39), *"em 2004, para satisfazer as necessidades decorrentes de uma preocupação e focalização crescentes na Gestão de Riscos de Negócio, o COSO emitiu um modelo integrado de Gestão do Risco Empresarial (ERM – "Enterprise Risk Management"), desenvolvido pela PWC, sob a sua supervisão, e que incorpora dentro de si o modelo de controlo interno COSO de 1992, permitindo que as organizações adotassem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno progredindo para um processo de Gestão de Riscos de Negócio".*

O COSO ERM é um enquadramento conceptual que ajuda as organizações a perceber o que é o risco, de que modo está presente na empresa e de que forma pode afetar adversamente os objetivos estratégicos da organização e a criação de valor. É um guia prático de fácil aplicação e é desenhado de modo a identificar determinados acontecimentos que possam afetar a organização. Destina-se a identificar, avaliar e gerir

o risco de modo a fornecer uma segurança razoável quanto à realização dos objetivos da organização (COSO, 2004: p.125:127).

De acordo com Ferreira (2010: p.20), as organizações enfrentam incertezas, desafios e uma diversidade de riscos, sendo o grande desafio da gestão determinar qual é o nível de incerteza que a empresa está preparada para aceitar. A Gestão de Riscos de Negócio permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos cujo impacto seja maior, com o objetivo de criar valor para os acionistas.

O modelo de Gestão do Riscos de Negócio proposto pelo COSO ERM está assente em 8 componentes que são afetados de acordo com os objetivos da organização. Este modelo estabelece quatro categorias de objetivos para a organização:

- Estratégicos: referem-se às metas de nível mais elevado;
- Operações: o objetivo é a utilização eficaz e eficiente dos recursos;
- Comunicação: relacionados à confiabilidade dos relatórios;
- Conformidade: fundamentam-se no cumprimento das leis e dos regulamentos pertinentes.

De acordo com Sousa (2012: p.40), os quatro objetivos de este modelo de Gestão de Riscos de Negócio, deverão ser caracterizadas da seguinte forma: A um nível mais elevado e diretamente relacionados com a missão e visão estão os objetivos estratégicos. Os operacionais estão com o uso eficiente e efetivo dos recursos da organização no desenvolvimento das suas atividades. A realização dos objetivos estratégicos e operacionais está sujeita a eventos externos à organização que nem sempre estão sob o seu controlo. Por outro lado temos o objetivo da confiabilidade na informação reportada e o objetivo de cumprimento das leis e regulamentos, que já estão numa zona de total controlo da organização, sendo esperado com um grau razoável de segurança que sejam cumpridos.

Essa classificação possibilita um foco nos aspetos específicos da Gestão de Riscos de Negócio. Apesar de estas categorias serem distintas, elas relacionam-se, uma vez que um dado objetivo poderá estar presente em mais do que uma categoria, elas

tratam de necessidades empresariais diferentes, cuja responsabilidade direta poderá ser atribuída a diversos gestores (COSO, 2004: p.21)

Existe uma relação direta entre objetivos e componentes, uma vez que os objetivos são metas que a entidade pretende alcançar e os componentes são os meios necessários para atingir esses objetivos (Ferreira, 2010: p.9).

Esta relação é estruturada através de uma matriz tridimensional, conforme mostra a figura a seguir:

Figura 1 - Cubo COSO ERM
Adaptado de: COSO (2004). "Gestão de Riscos Corporativos – Estrutura Integrada".

De acordo com Ferreira (2010: p.21), *"o modelo deverá ser avaliado e implementado de uma forma abrangente a toda a organização, partindo de um nível mais elevado (Entidade) até chegar ao nível mais básico (Atividades) ".*

Neste modelo, os componentes da Gestão de Riscos de Negócio estão identificados como sendo os seguintes (COSO, 2004: p.6):

- "*Ambiente Interno: Estabelece uma filosofia de abordagem à Gestão de Riscos de Negócio. Assume que eventos que sejam esperados ou inesperados poderão ocorrer. Estabelece a cultura de risco da entidade. Considera todos os outros aspetos relativos à forma como as ações da organização poderão afetar a sua cultura de risco;*

- *Definição de Objetivos: Aplica-se quando a gestão tem em conta a estratégia de risco na definição de objetivos. Suporta o apetite pelo risco da entidade, Determina a tolerância do risco, i.e. o nível aceitável de variação em volta dos objetivos, alinhada com o apetite pelo risco;*

- *Identificação de Eventos: Diferencia riscos e oportunidades. Os eventos que possam ter impacto negativo representam risco, e os eventos que possam ter um impacto positivo representam oportunidades, que a gestão deve ter em conta na definição da estratégia;*

- *Avaliação de Risco: Permite a uma entidade compreender a dimensão do impacto que os potenciais eventos poderão ter nos objetivos. Avalia os riscos a partir de duas perspetivas: Probabilidade e Impacto. É utilizada para avaliar os riscos e também é utilizada para quantificar os objetivos com eles relacionados. Utiliza uma combinação de metodologias quer qualitativas quer quantitativas. Relaciona horizontes temporais a horizontes de objetivos e avalia o risco quer numa base inerente quer residual;*

- *Resposta ao Risco: Identifica e avalia possíveis respostas ao risco; Avalia as opções relativas ao apetite pelo risco da entidade, custos vs. benefícios das respostas ao risco potencial, e o nível a que a resposta deverá ter em relação à redução do impacto e/ou da probabilidade. Seleciona e executa a resposta baseada na avaliação do portfolio de riscos e respostas;*

- *Atividades de Controlo: Políticas e procedimentos que ajudam a assegurar que as respostas aos riscos, assim como outras orientações da entidade, são realizadas. Realizam-se em toda a organização, a todos os níveis e em todas as*

Funções. Incluem os controlos gerais e das aplicações das tecnologias de informação;

- *Informação & Comunicação: A gestão identifica, recolhe, e comunica a informação pertinente de uma forma e em prazo que permite às pessoas exercer as suas responsabilidades. A comunicação é feita de forma alargada, fluindo nos sentidos descendente, horizontal, e ascendente dentro da organização;*

- *Supervisão: A eficácia das outras componentes da ERM é supervisionada através de: Atividades contínuas de supervisão; Avaliações específicas; E a combinação das duas".*

1.2.4. Norma de Gestão dos Riscos de Negócio da FERMA: *Risk Management Standard* (*Federation of European Risk Management Associations*, 2003)

A Norma de Gestão dos Riscos de Negócio é o resultado do trabalho de uma equipa composta por elementos das principais organizações de Gestão de Riscos de Negócio do Reino Unido – *"The Institute of Risk Management" (IRM), "The Association ofInsurance and Risk Managers" (AIRMIC) e ALARM "The National Forum for Risk Management in the Public Sector".*

Cumprindo as várias componentes desta norma e podendo fazê-lo de formas diversas, as organizações ficarão em posição de informar sobre a sua conformidade com a mesma. A norma representa as melhores práticas em relação às quais as organizações se podem autoavaliar (FERMA, 2003: p.2).

De acordo com a FERMA (2003: p.3), a norma de Gestão de Riscos de Negócio tem as seguintes componentes:

1) Definição de Risco: O risco pode ser entendido como a combinação da probabilidade de um acontecimento e das suas consequências. O facto de existir atividade, proporciona eventos ou situações cujas consequências constituem oportunidades ou ameaças.

2) Gestão dos Riscos de Negócio: É um processo através do qual as organizações analisam os riscos inerentes às respetivas atividades, com o objetivo de atingirem vantagens em cada atividade e no conjunto de todas as atividades:

   a) Fatores externos e internos: Os riscos que uma organização e respetivas atividades apresentam, podem ter origem em fatores que podem ser internos ou externos à organização;

   b) Processo de Gestão de Riscos de Negócio: A Gestão dos Riscos de Negócio protege e acrescenta valor à organização e aos diversos intervenientes, apoiando da seguinte forma os objetivos da organização:

      i) "Criação de uma estrutura na organização que permita que a atividade futura se desenvolva de forma consistente e controlada;

      ii) Melhoria da tomada de decisões, do planeamento e da definição de prioridades, através da interpretação abrangente e estruturada da atividade do negócio, da volatilidade dos resultados e das oportunidades/ameaças do projeto:

      iii) Contribuição para uma utilização/atribuição mais eficiente do capital e dos recursos dentro da organização e redução da volatilidade em áreas de negócio não essenciais;

      iv) Proteção e melhoria dos ativos e da imagem da empresa;

      v) Desenvolvimento e apoio à base de conhecimentos das pessoas e da organização;

      vi) Otimização da eficiência operacional" (FERMA 2003: p.3:5).

3) Avaliação de riscos: A avaliação de riscos é definida pelo documento ISO/IEC "*Guide"* 73 como o processo geral de análise de riscos e estimativa de riscos.

   - O ISO/IEC "*Guide"* 73 é um guia que fornece vocabulário básico, para um entendimento comum, sobre os conceitos de Gestão dos Riscos de Negócio entre organizações e funções, e em diferentes aplicações. Este Guia é

genérico, e é compilado para abranger de uma forma geral a Gestão dos Riscos de Negócio (ISO, 2009)

4) Análise de Riscos:

a) Identificação de Riscos: A análise de riscos deve ser abordada de modo a garantir que todas as atividades dentro da organização foram identificadas e todos os riscos delas decorrentes foram definidos. Toda a volatilidade associada relativa a estas atividades deve ser identificada e classificada por categorias:

i) "Estratégicas: Relacionadas com os objetivos estratégicos da organização a longo prazo;

ii) Operacionais: Relacionadas com os assuntos quotidianos com os quais a organização é confrontada quando se esforça para atingir os seus objetivos estratégicos;

iii) Financeiras: Relacionadas com a gestão e controlo eficazes dos meios financeiros da organização e com os efeitos de fatores externo;

iv) Gestão do conhecimento: Relacionadas com a gestão e controlo eficazes dos recursos do conhecimento e com a produção, proteção e comunicação destes;

v) Conformidade: Relacionadas com temas como saúde e segurança, meio ambiente, práticas comerciais, proteção do consumidor, proteção de dados, assuntos regulamentares e legislação laboral" (FERMA, 2003: p.6).

b) Descrição dos riscos: O objetivo da descrição dos riscos é a apresentação dos riscos identificados, de forma estruturada. A seguinte tabela de descrição dos riscos pode facilitar a descrição e avaliação de riscos.

1. Designação do risco	

2. Âmbito do risco	Descrição qualitativa de acontecimentos, como dimensão, tipo, número e dependências.
3. Natureza do risco	Exºs: estratégicos, financeiros, operacionais, de conhecimento ou conformidade.
4. Intervenientes	Intervenientes e respetivas expectativas.
5. Quantificação do risco	Importância/relevância e probabilidade.
6. Tolerância/Apetência para o risco	Potencial de perda e impacto financeiro do risco; Valor em risco (*value at risk*); Probabilidade e dimensão de perdas/ganhos potenciais; Objetivo (s) do controlo do risco e nível de desempenho pretendido.
7. Tratamento e mecanismos de controlo do risco	Principais meios através dos quais o risco é atualmente gerido; Níveis de confiança do controlo existente; Identificação dos protocolos de monitorização e revisão.
8. Possíveis ações de melhoria	Recomendações para redução do risco.
9. Desenvolvimento de estratégias e políticas.	Identificação da função responsável pelo desenvolvimento de estratégias e políticas.

Tabela 1 - Tabela de descrição dos riscos
Fonte: FERMA - Federation of European Risk Management Associations (2003). *"Norma de Gestão de Riscos de Negócio".*

c) Estimativa dos riscos: A estimativa dos riscos pode ser quantitativa, semi-quantitativa ou qualitativa em termos de probabilidade de ocorrência e possível consequência.

d) Métodos e técnicas de análise de riscos: Podem ser utilizadas diversas técnicas para analisar riscos. Estas técnicas podem ser específicas, de riscos com aspetos positivos ou negativos ou podem ter a capacidade de analisar ambos os tipos.

e) Perfil dos riscos: O resultado do processo de análise de riscos pode ser utilizado para gerar um perfil dos riscos que classifica cada risco segundo a sua importância e fornece uma ferramenta para determinar a prioridade dos esforços de tratamento.

5) Comparação de riscos: No momento em que o processo de análise de riscos estiver finalizado, é necessário comparar os riscos estimados com os critérios de riscos definidos pela organização. *"Os critérios de riscos podem englobar os custos e receitas associados, exigências legais, fatores socioeconómicos e ambientais, preocupações dos intervenientes, etc. Desta forma, a estimativa de riscos e subsequente comparação apoia na tomada de decisões sobre a importância dos riscos para a organização e sobre a possibilidade de cada risco específico ser aceite ou corrigido" (*FERMA, 2003: p.10).

6) Tratamento de riscos: O tratamento de riscos é o processo de selecionar e implementar medidas para alterar um risco. "*O elemento principal do tratamento de riscos é o controlo/diminuição dos riscos, mas engloba, num contexto mais vasto, por exemplo, o evitar de riscos, a transferência, o financiamento, etc."* (FERMA, 2003: p.10).

7) Comunicação de riscos

   a) Comunicação interna: Dentro de uma organização os vários níveis necessitam de diferentes tipos de informações que serão obtidos através do processo de Gestão dos Riscos de Negócio.

   " O Conselho de Administração deve:

   - *Conhecer os riscos mais importantes que a organização enfrenta;*
   - *Conhecer os possíveis efeitos no valor acionista provocados pelos desvios relativamente aos níveis de desempenho esperados;*
   - *Garantir níveis adequados de sensibilização aos riscos em toda a organização;*
   - *Saber de que forma a organização vai gerir uma crise;*

- *Conhecer o nível de confiança dos intervenientes na organização;*
- *Saber como gerir as comunicações com os investidores, quando aplicável;*
- *Ter a certeza de que o processo de Gestão dos Riscos de Negócio é eficaz;*
- *Publicar uma política clara que abranja a abordagem geral e as responsabilidades da Gestão dos Riscos de Negócio.*

As Unidades de Negócio devem:

- *Estar conscientes dos riscos inerentes às respetivas áreas de responsabilidade, dos possíveis impactos que estes podem ter noutras unidades e das consequências que outras unidades lhes podem provocar;*
- *Dispor de indicadores de desempenho que lhes permitam monitorizar nas atividades chave, quer financeiras quer operacionais, os progressos para o cumprimento dos objetivos;*
- *Identificar intervenções necessárias à correção de desvios (por exemplo, previsões e orçamentos);*
- *Dispor de sistemas que informem sobre variações orçamentais e de previsões, com uma frequência adequada, que permitam reações apropriadas;*
- *Comunicar, sistemática e imediatamente, à direção de topo todos os riscos novos ou falhas constatadas nas medidas de controlo existentes.*

Cada indivíduo deve:

- *Compreender o seu nível de responsabilização relativamente a riscos individuais;*
- *Compreender de que forma podem contribuir para a melhoria contínua da Gestão dos Riscos de Negócio;*
- *Compreender que a Gestão dos Riscos de Negócio e a sensibilização para a existência de riscos são elementos chave da cultura da organização;*

- *Comunicar, sistemática e imediatamente, à direção de topo todos os riscos novos ou falhas constatadas nas medidas de controlo existentes"* (FERMA, 2003: p.11).

b) Comunicação externa: Regularmente, uma empresa precisa de prestar contas aos intervenientes, definindo as respetivas políticas de Gestão dos Riscos de Negócio e a eficácia na obtenção de objetivos.

8) Estrutura e administração da Gestão dos Riscos de Negócio:

a) Política de Gestão dos Riscos de Negócio: Uma política de Gestão dos Riscos de Negócio deve definir a atitude e apetência para o risco e a abordagem para a Gestão dos Riscos de Negócio. A política deve também definir as responsabilidades relativas à Gestão dos Riscos de Negócio em toda a organização. Além disso, esta declaração de intenções deve também referir todos os requisitos legais aplicáveis, como por exemplo a nível de saúde e segurança.

b) Papel do Conselho de Administração: O Conselho de Administração tem a responsabilidade de definir a direção estratégica da organização e criar o ambiente e as estruturas necessárias para que a Gestão dos Riscos de Negócio funcione de forma eficaz

c) Papel das unidades de negócio: Dentro das suas competências, estabelece o seguinte:

- *"As unidades de negócio têm a responsabilidade de gerir diariamente os riscos;*

- *As direções das unidades de negócio são responsáveis pela promoção da sensibilização sobre a existência de riscos nas respetivas atividades; devem introduzir objetivos de Gestão dos Riscos de Negócio nas suas unidades;*

- *A Gestão dos Riscos de Negócio deve ser um tema regular das agendas das reuniões de direção, de modo a permitir a consideração de exposições a riscos e a redefinição de prioridades das tarefas à luz de uma análise eficaz dos riscos;*

- *As direções das unidades de negócio devem garantir que a Gestão dos Riscos de Negócio é incorporada tanto na fase de conceção dos projetos, como ao longo da execução de cada um deles"* (FERMA, 2003: p.12:13).

9) Papel da Função de Gestão dos Riscos de Negócio: Dependendo da dimensão da organização, o número de elementos envolvidos na Gestão de Riscos de Negócio pode ir desde um único responsável até um departamento de grande escala.

"A Função Gestão dos Riscos de Negócio deve incluir:

- *A definição de políticas e estratégias de Gestão de Riscos de Negócio;*
- *O principal responsável pela Gestão dos Riscos de Negócio a nível estratégico e operacional;*
- *O desenvolvimento da sensibilização para a existência de riscos dentro da organização, incluindo formação e informação adequadas;*
- *O estabelecimento de políticas e estruturas de risco internas nas unidades de negócio;*
- *A conceção e revisão de processos de Gestão dos Riscos de Negócio;*
- *A coordenação de diversas atividades funcionais que forneçam aconselhamento sobre questões de Gestão dos Riscos de Negócio;*
- *O desenvolvimento de processos de resposta a riscos, incluindo programas e/ou planos de contingência e de continuidade das atividades;*
- *A preparação de relatórios sobre riscos para o Conselho de Administração"* (FERMA, 2003: p.13:14).

1.2.5. Norma de Gestão dos Riscos de Negócio - ISO 31000 da *International Organization for Standardization* emitida em 2009

A crise financeira atual resulta da falha na gestão efetiva do risco, no caso de Portugal ainda são poucas as empresas que têm uma Gestão dos Riscos de Negócio a funcionar de acordo com as melhores práticas (Sousa, 2012: p.11). Desta forma e nesse

sentido "foi emitida a norma ISO 31000: 2009, *Risk Management – Principles and Guidelines*", cujo principal objetivo consiste na divulgação de uma abordagem que ajude as organizações de todos os tipos e dimensões a fazerem a gestão efetiva do risco (Sousa, 2012: p11).

A ISO 31000, publicada em 2009, é a mais recente norma internacional sobre Gestão dos Riscos de Negócio e foi produzida pela "*International Organization for Standardization"*. Esta norma teve como base a norma AS/NZS 4360 (2004) e foi desenvolvida por uma comissão de representantes de 35 países, que se associaram para criar um grupo de trabalho, designado por *ISO "Technical Management Board on Risk Management"* e que abrangeu especialistas em gestão de risco de diversas áreas (como a financeira, segurança, qualidade, meio ambiente, tecnologia, saúde, defesa, seguros, entre outros). O trabalho obtido não divulga apenas as conclusões desta comissão mas as opiniões e experiências de centenas de profissionais envolvidos na Gestão dos Riscos de Negócio (Santos, 2013: p13).

Esta Norma atende às necessidades, de várias partes (ABNT NBR ISO 31000, 2009: p.30):

- *"Os responsáveis pelo desenvolvimento da política de gestão de riscos no âmbito das suas organizações;*
- *Os responsáveis por assegurar que os riscos são geridos de forma eficaz, na organização, área, atividade ou projeto específicos;*
- *Os que precisam de avaliar a eficácia de uma organização ao nível da gestão de riscos; e*
- *Os criadores das normas, guias, procedimentos e códigos de práticas que, no todo ou em parte, estabelecem como o risco deve ser gerido".*

De acordo com Santos (2013: p.31), a norma ISO 31000 aconselha as organizações a desenvolver, implementar e melhorar continuamente um sistema de Gestão dos Riscos de Negócio, como um componente integral do seu sistema de gestão. Dessa forma, a norma pode ser acolhida por qualquer tipo organização, qualquer que

seja o sector de atividade em que está inserida, e pode ser aplicada a toda a organização e para uma ampla gama de atividades, processos, funções, projetos, produtos, serviços, ativos, operações e decisões.

A Gestão dos Riscos de Negócio quando é implementada e mantida de acordo com esta Norma possibilita a uma organização (ABNT NBR ISO 31000, 2009: p.V:VI):

- *"Aumentar a probabilidade de atingir os objetivos;*
- *Encorajar uma gestão pró-ativa;*
- *Estar atenta para a necessidade de identificar e tratar os riscos através de toda a organização;*
- *Melhorar a identificação de oportunidades e ameaças;*
- *Atender às normas internacionais e requisitos legais e regulatórios pertinentes;*
- *Melhorar o reporte das informações financeiras;*
- *Melhorar a governança;*
- *Melhorar a confiança das partes interessadas;*
- *Estabelecer uma base confiável para a tomada de decisão e o planeamento;*
- *Melhorar os controlos;*
- *Alocar e utilizar eficazmente os recursos para o tratamento de riscos;*
- *Melhorar a eficácia e a eficiência operacional;*
- *Melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente;*
- *Melhorar a prevenção de perdas e a gestão de incidentes;*
- *Minimizar perdas;*
- *Melhorar a aprendizagem organizacional; e*

- *Aumentar a resiliência da organização."*

O processo de Gestão dos Riscos de Negócio deve ser implementado pela organização, como um processo transversal e integrado que englobe a governação, estratégia e planeamento, gestão, processos de relato, politicas, valores e cultura (Sousa, 2012: p.45).

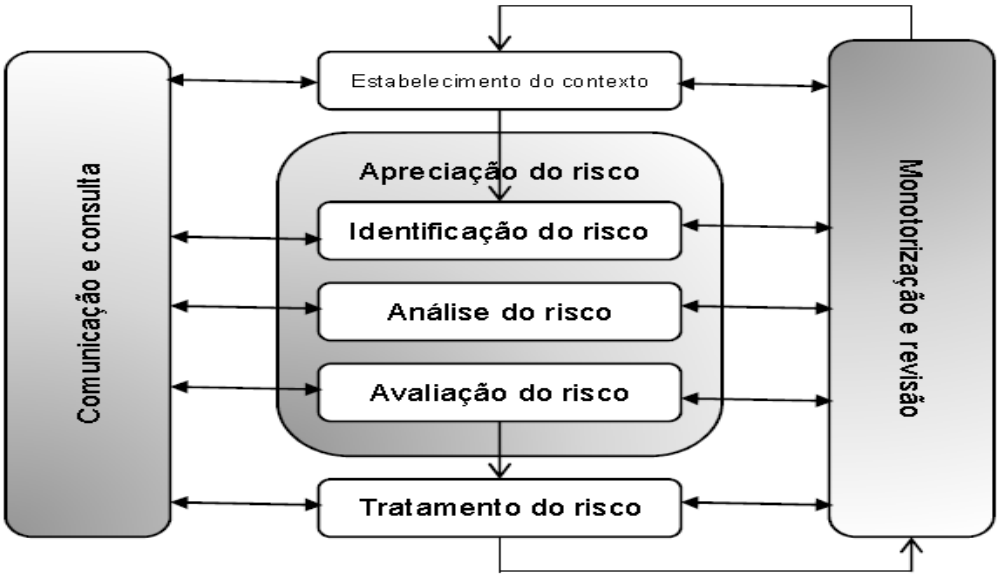


Figura 2 - Processo Gestão dos Riscos de Negócio
Fonte: ABNT NBR ISO 31000:2009

De acordo com Santos (2013: p.32):

"A implementação de um processo de gestão de risco bem-sucedida, baseado na ISO 31000, permitirá ajudar as organizações a cumprir normativos e requisitos legais, a estabelecer uma maior confiança no planeamento e na tomada de decisões assim como no uso adequado dos recursos, no aumento da consciencialização sobre a necessidade de identificar e tratar os riscos a que a organização está sujeita e melhorar a identificação de oportunidades e ameaças, os controlos, a eficácia operacional e a eficiência".

Para a Gestão dos Riscos de Negócio ser eficaz, convém que uma organização, em todos os níveis, atende aos princípios de que a Gestão dos Riscos de Negócio:

- Cria e protege valor;

- É parte integrante de todos os processos organizacionais;
- É parte da tomada de decisões;
- Aborda explicitamente a incerteza;
- É sistemática, estruturada e oportuna;
- Baseia-se nas melhores informações disponíveis;
- É feita sob medida;
- Considera fatores humanos e culturais;
- É transparente e inclusiva;
- É dinâmica, iterativa e capaz de reagir a mudanças;
- Facilita a melhoria contínua da organização (ABNT NBR ISO 31000, 2009: p.7:8).

De forma a uniformizar este processo e possibilitar uma melhor perceção por parte dos utilizadores a norma apresenta e descreve vários termos e definições entre os quais:

- Risco: o "efeito da incerteza nos objetivos". Coloca a ênfase no efeito, em vez do evento. A questão é, quais as consequências que o risco pode ter para a concretização dos objetivos?;
- Apetite de risco: quantidade e o tipo de risco que a organização está preparada para manter ou tirar;
- Critérios de risco: termos de referência contra a qual o significado de um risco é avaliado;
- Risco residual: risco remanescente após o tratamento do risco;
- Proprietário do risco: pessoa ou entidade com a responsabilidade e autoridade para gerenciar o risco;

- Probabilidade: "possibilidade de algo acontecer ", pode ser medido em termos qualitativos ou quantitativos;

- Consequência: resultado de um evento que afeta os objetivos, pode ser positivo ou negativo (ABNT NBR ISO 31000, 2009: p.1:2).

Face às recomendações e ao possível sucesso da implementação deste processo, é possível "*concluir que a gestão do risco, de acordo com os princípios gerais da ISO, faz parte integrante da organização estando presente em todos os processos desde a definição da estratégia e do orçamento aos processos operacionais de rotina. Em suma, faz parte da cultura da organização*" (Sousa, 2012: p.44).

"O que se pretende no fundo com este tipo de norma é melhorar a identificação de oportunidades e ameaças, a conformidade com requisitos legais/regulamentares, e normas internacionais, com as demonstrações financeiras e com a governação" (ABNT NBR ISO 31000, 2009: p.VI).

1.2.6. Importância da Gestão dos Riscos de Negócio para a Empresa

De acordo com a Norma de Gestão dos Riscos de Negócio (FERMA 2003: p.5), "*Gestão de Riscos de Negócio protege e acrescenta valor à organização e aos diversos intervenientes, apoiando da seguinte forma os objetivos da organização:*

- *Criação de uma estrutura na organização que permita que a atividade futura se desenvolva de forma consistente e controlada;*
- *Melhoria da tomada de decisões, do planeamento e da definição de prioridades, através da interpretação abrangente e estruturada da atividade do negócio, da volatilidade dos resultados e das oportunidades/ameaças do projeto;*
- *Contribuição para uma utilização/atribuição mais eficiente do capital e dos recursos dentro da organização;*
- *Redução da volatilidade em áreas de negócio não essenciais;*
- *Proteção e melhoria dos ativos e da imagem da empresa;*
- *Desenvolvimento e apoio à base de conhecimentos das pessoas e da organização;*
- *Otimização da eficiência operacional."*

De Acordo com o COSO (2004: p.3), a Gestão dos Riscos de Negócio tem por finalidade:

- Alinhar o apetite pelo risco com a estratégia adotada: desenvolvendo mecanismos para gerir os riscos;
- Fortalecer as decisões em resposta aos riscos: possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos (como evitar, reduzir, compartilhar e aceitar os riscos);
- Reduzir as surpresas e prejuízos operacionais: melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas, custos ou prejuízos associados;
- Identificar e administrar riscos múltiplos: possibilita uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos;
- Aproveitar oportunidades: a organização posiciona-se para identificar e aproveitar as oportunidades de forma proactiva;
- Otimizar o capital: a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital.

1.2.7. O papel da Gestão no âmbito da Gestão dos Riscos de Negócio

O IIA (2009: p.5:6) refere que a Gestão tem a responsabilidade global de assegurar que os riscos são geridos. Na prática, a Gestão irá delegar a operacionalização da estrutura de Gestão de Riscos de Negócio aos diversos Gestores/Responsáveis. Acrescenta ainda que todos os membros de uma organização tem o seu papel no sucesso da Gestão de Risco empresariais, sendo que a principal responsabilidade na identificação e gestão dos riscos pertence aos administradores.

Todos os colaboradores de uma organização tem uma parcela de responsabilidade na Gestão de Riscos de Negócio. A Gestão é a principal responsável e deve assumir a responsabilidade da iniciativa. Cabe aos Gestores/Responsáveis apoiar a filosofia de Gestão de Riscos de Negócio, incentivar a observação do apetite pelo risco e gerir os riscos dentro das suas esferas de responsabilidade, conforme as tolerâncias definidas pelo risco. Regra geral, cabe ao diretor de riscos, diretor-financeiro, auditor interno e outros, responsabilidades fundamentais de suporte. Os outros membros da

organização são responsáveis pela execução da Gestão de Riscos de Negócio em cumprimento das diretrizes e dos protocolos estabelecidos. Diversas partes externas, como clientes, fornecedores, revendedores, parceiros comerciais, auditores externos e analistas frequentemente fornecem informações úteis para a condução da Gestão de Riscos de Negócio, porém não são responsáveis pela sua eficácia e nem fazem parte do gerenciamento de riscos da organização (COSO, 2004: p.92:99).

1.2.8. A CMVM e o Governo das Sociedades Cotadas

Em Portugal também existem mecanismos para proteger os investidores que operam na bolsa. A Comissão do Mercado de Valores Mobiliários (CMVM) é a entidade encarregada de emitir regulamentos e recomendações para as empresas cotadas. A sua missão é supervisionar e regular os mercados de valores mobiliários e instrumentos financeiros derivados. A CMVM tem poderes de supervisão, que consistem no acompanhamento permanente da atuação das pessoas ou entidades que intervêm no mercado de capitais, fiscalização do cumprimento de regras, deteção de infrações, punição dos infratores e difusão de informações (nomeadamente sobre empresas cotadas).

De acordo com a CMVM (2007: p.1) "*Governo das sociedades é o sistema de regras e condutas relativo ao exercício da direção e do controlo das sociedades emitentes de ações admitidas à negociação em mercado regulamentado. O seu objetivo é antes o de procurar contribuir para a otimização do desempenho das sociedades e favorecer todas as pessoas cujos interesses estão envolvidos na atividade societária".*

De acordo com as "Recomendações da CMVM sobre o Governo das Sociedades Cotadas" (CMVM, 2013: p.2) é referido que:

> *"O Conselho de Administração ou o Conselho Geral e de Supervisão, consoante o modelo aplicável, devem fixar objetivos em matéria de assunção de riscos e criar sistemas para o seu controlo, com vista a garantir que os riscos efetivamente incorridos são consistentes com aqueles objetivos."*

O Regulamento da CMVM n.º 4/2013 descreve os requisitos gerais das sociedades cotadas. O artigo 1ª do referido regulamento, aborda a Estrutura e Práticas

de Governo das Sociedades e solicita às empresas um relatório detalhado sobre a estrutura e as práticas de governo societário.

A CMVM refere ainda que o órgão de fiscalização deve avaliar o funcionamento dos sistemas de controlo interno e de gestão de riscos e propor os ajustamentos que se mostrem necessários. (CMVM, 2013: p.4)

1.3. Auditoria Interna

1.3.1. Evolução

De acordo com Martins et al. (1999: p.10), os primeiros auditores internos apareceram há mais de setenta anos nos Estados Unidos da América. No entanto, o reconhecimento da função de Auditoria Interna, tem apenas cerca de trinta anos. Na Europa, depois do Reino Unido, é a Alemanha quem pratica Auditoria Interna há mais tempo. Em Portugal, a Auditoria Interna é recente. O tecido empresarial português só nos últimos anos têm vindo a acompanhar as inovações operadas neste âmbito, adotando-as e ajustando-as consoante as suas possibilidades e o entendimento da função pelas suas Administrações. Em 1941 surge nos Estados Unidos da América, a organização mundial de auditores internos, denominada por "*Institute of Internal Auditors"* (IIA), Em Portugal apenas em 1992 foi criado o IPAI (Instituto Português de Auditores Internos).

Inicialmente a Auditoria Interna era compreendida como uma atividade que visava essencialmente a avaliação da fiabilidade dos controlos internos, por vezes, designada de "o controlo dos controlos" (Pinheiro, 2013: p.17). "*A partir de 1980 a Auditoria Interna ganha uma maior projeção, assistindo-se assim a um alargamento progressivo do seu âmbito, passando este trabalho a incluir um conjunto muito mais amplo de análise às operações, recursos e controlos. Passados dez anos a Auditoria assume, de facto, a importância que se conhece atualmente, apesar de ainda hoje em Portugal se considerar que tem muito para progredir. Trata-se de uma função muito mais abrangente e sistemática do que já foi e a sua atividade baseia-se cada vez mais no auxílio na identificação e Gestão de Riscos de Negócio"* (Pires, 2010: p.52).

1.3.2. Mudança de Paradigma

Até 1999 o IIA define Auditoria Interna como (Humprey et al., 2004: p.7:8):

> *"Uma função de avaliação independente, estabelecida na organização para examinar e avaliar as suas atividades, como um serviço para a organização. O objetivo da Auditoria Interna é apoiar os membros da organização no desempenho eficaz das suas responsabilidades. Com este fim, a Auditoria Interna fornece-lhes análises, avaliações, recomendações, conselhos, e informação concernente às atividades revistas. O objetivo da auditoria inclui a promoção de um controlo eficaz a um custo razoável (IIA, até 1999) ".*

Nesta definição o objetivo é assegurar a qualidade da informação, a proteção dos ativos, a eficácia dos sistemas, o cumprimento das normas e a qualidade no desempenho das atividades de modo a ajudar os membros da organização no desempenho das suas funções para poderem atingir os objetivos propostos.

Face às demais alterações económicas, e com a evolução da globalização, a Auditoria Interna passa a ser definida como *"uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações de uma organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação dos processos da eficácia da Gestão de Riscos de Negócio, do controlo e de governação"* (IIA, 2009: p.5). Esta definição defende que, a Auditoria Interna ajuda a gestão no desempenho eficaz das suas funções de modo a acrescentar valor à organização. Por sua vez apoia a avaliação, e caso necessário, melhora a eficiência do processo de Gestão de Riscos de Negócio, controlo ou governo das sociedades (Alves 2009: p.29).

De acordo com Pinheiro (2005: p.20)*:*

> *"A Auditoria Interna visa, essencialmente, apoiar a gestão de topo e os gestores operacionais, a identificar os riscos negativos das*

atividades/subprocessos e contribuir, necessariamente, com propostas de ações corretivas, numa lógica de criação de valor cliente e valor acionista.

1.3.3. Objetivos e Funções

O objetivo da Auditoria Interna é ser uma ferramenta de apoio à gestão, que auxilie a organização a alcançar os seus objetivos, servindo de assessor e consultor da mesma na identificação dos riscos e propondo possíveis estratégias de Acão que permitam às empresas melhor desempenho dentro do sector económico (Martins, 2013: p.9). De acordo com o Instituto Português de Auditoria Interna, a Auditoria Interna tem que avaliar e efetuar recomendações apropriadas para a melhoria do processo de governação, no cumprimento dos seguintes objetivos (IPAI, 2009a):

- *"Promover a ética e valores apropriados no seio da organização;*
- *Assegurar a gestão do desempenho organizacional e sua responsabilização de forma eficaz;*
- *Transmitir de forma eficaz a informação sobre risco e controlo, às áreas apropriadas da organização;*
- *Coordenar eficazmente as atividades de comunicação e informação ao Conselho, aos auditores externos e internos e aos gestores."*

O objetivo primordial da Auditoria Interna é o de auxiliar a empresa e todos os níveis de gestão no cumprimento das suas responsabilidades, em promover sistemas de controlo adequados, visando a melhoria da performance e do desenvolvimento sustentável da empresa (Pinheiro, 2010: p.32).

De acordo com a ISA 610 do IFAC (2009: p.629), de um modo geral, as atividades de Auditoria Interna têm os seguintes objetivos:

- Monitorização do controlo interno: O estabelecimento de um adequado controlo interno é responsabilidade da Administração, contudo a

responsabilidade pela gestão, revisão e monitorização dos controlos assim como possíveis recomendações, é atribuído à Auditoria Interna;

- Exame da informação financeira e operacional: Pode incluir, a revisão dos meios utilizados para identificar, mensurar, classificar e relatar tal informação;
- Revisão da economia, eficiência e eficácia das operações incluindo controlos não financeiros de uma entidade;
- Revisão da conformidade com leis, regulamentos e outros requisitos externos e com as políticas e diretivas da gerência e outros requisitos internos;

As principais funções da Auditoria Interna podem ser subdivididas em (Tribunal de Contas, 2011: p.29):

- Apoio à Direção: Quando esta lhe reconhece utilidade e a posiciona a um nível hierárquico elevado, e reconhece que a Auditoria Interna acrescenta valor á organização;
- Vigilância do Sistema de Controlo Interno: Proporciona à Direção informação sobre a eficácia do controlo interno, e tem como principal responsabilidade dotar a organização de uma ferramenta de controlo, mediante os pontos fracos da organização;
- Apoio à Gestão de Riscos de Negócio e Processos de Governação: verificar se a metodologia para implementar o processo de Gestão de Riscos de Negócio é entendida pelos diferentes grupos envolvidos na governação da organização;
- Assessoria: Executada por solicitação dos serviços, tem carácter consultivo e destina-se a apoiar a gestão na concretização dos objetivos, a atividade de Auditoria Interna poderá prestar serviços de consultadoria, desde que seja assegurada a sua independência e objetividade;
- Investigação: Executada só por solicitação da Direção, destina-se a situações específicas.

1.3.4. A Auditoria Interna e o seu papel na organização

A Auditoria Interna é a peça mais importante, para a gestão das organizações, pois confronta os resultados obtidos, com a estratégia e o plano de ação elaborado pela empresa, com a finalidade de identificar ameaças e oportunidades, para a realização dos seus objetivos (Pinto, 2012: p.53). A Auditoria Interna pode identificar áreas, que requerem atenção especial, identificar problemas e insuficiências que careçam de solução, e desse modo propor medidas, com vista a reduzir e a eliminar os principais problemas, nomeadamente no que respeita (Marques 1997: p.77):

- *"À avaliação e à execução dos objetivos e das políticas estabelecidas e ao cumprimento das disposições legais e demais normativos existentes;*
- *À necessidade de alterar normativos, critérios, processos e procedimentos;*
- *À adequação e eficácia dos meios e dos processos;*
- *À adequação e eficácia dos sistemas de controlo interno e de gestão"* (Marques, 1997: p.77).

Segundo o Tribunal de Contas (2011: p.28):

"Auditoria Interna desempenha um papel fundamental numa organização, constituindo um instrumento privilegiado ao serviço da gestão. Desenvolve uma atividade independente, de apreciação objetiva e de consultadoria destinada a acrescentar valor e a melhorar o funcionamento da organização, adotando uma visão integrada e abrangente. A Auditoria Interna deve contribuir para o reforço da responsabilidade da gestão a todos os níveis da organização, assegurando, nomeadamente, a observância das políticas, dos objetivos, dos planos, das normas e dos regulamentos, fazer uma adequada supervisão da gestão e controlo de risco e, também, melhorias no processo de governação."

De acordo com Marques (1997: p.77), o bom funcionamento do serviço de Auditoria Interna, contribui para uma melhoria da cultura organizacional e para o aperfeiçoamento dos métodos e processos da organização, com reflexos na:

- *"Melhoria da gestão dos aprovisionamentos;*
- *Melhoria da gestão administrativa e financeira;*
- *Melhoria da gestão comercial e do marketing;*
- *Melhoria da comunicação interna;*
- *Melhoria dos fluxos de informação descendente e ascendente;*
- *Melhoria da qualidade dos serviços prestados aos clientes, internos e externos;*
- *Melhoria da rendibilidade e das margens;*
- *Melhoria da qualidade dos produtos/serviços fornecidos e da imagem da unidade económica"* (Marques, 1997: p.77:78).

A atividade de Auditoria Interna pode ser utilizada para formação e preparação de quadros promissores e recrutamento interno de quadros superiores para o exercício de funções. O que já vem a acontecer em países técnica e culturalmente mais evoluídos ao nível da gestão, onde muitas empresas utilizam as equipas de Auditoria Interna para formação e recrutamento de elementos para quadros de direção e administração, depois de terem adquirido e interiorizado uma visão global da empresa e do seu enquadramento (Marques, 1997: p.78).

1.3.5. A Independência e o Papel do Auditor Interno

A independência do auditor é fundamental para a credibilidade e qualidade da informação financeira. Trata-se de uma exigência material face às condições de atuação junto das empresas e de outras entidades, é uma dificuldade perante as dependências e pressões a que está sujeito, no desempenho das funções de auditoria (Carneiro, 2013: p.24). Desta forma, a independência aumenta a capacidade do auditor agir com integridade, ser objetivo e manter o ceticismo profissional, de modo a assegurar a fiabilidade dos seus relatórios.

Segundo Martins et al. (1999: p.60), a independência permite que os auditores internos emitam opiniões imparciais e sem preconceitos, o que é fundamental para uma apropriada realização dos trabalhos de Auditoria. À independência, aliamos a neutralidade e objetividade que deve caracterizar continuadamente a ação do

departamento de Auditoria Interna. Está relacionada fundamentalmente com os seguintes elementos básicos:

- *"Objetividade: é importante que o auditor interno não desenvolva nem implante procedimentos, nem tão pouco prepare registos ou se vincule, de forma discreta, com a atividade que usualmente ele deverá auditar e avaliar, pois fazendo-o, a sua objetividade poder-se-ia ver seriamente afetada.*
- *Nível hierárquico dentro da organização: caso o diretor do departamento de Auditoria Interna tenha responsabilidade direta, que lhe venha outorgada pela direção e atue como "staff" desta, sem responsabilidades de gestão, existe independência"* (Martins e Morais, 1999: p.60).

O auditor deve ter conhecimento das estratégias de negócio e conferir, constantemente, os planos de auditoria para que estes reflitam as condições atuais. Isto é o auditor interno deverá manter-se atualizado relativamente a todas as normas e regulamentos que possam afetar a organização (Pinheiro, 2013: p.17). "*Deve desempenhar a sua atividade com visão holística e proactiva, antecipando-se aos factos, de modo que a sua opinião seja de fundamental importância nos rumos da organização. Ao mesmo tempo, deverá estar atento a novas tendências no mercado em que a sua organização atua. A sua participação na gestão operacional das organizações deve ir muito além de uma "fiscalização" sobre os processos, atuando em sintonia com as solicitações do mercado, com metas e estratégias bem definidas, que é fundamental para a sobrevivência empresarial"* (Teixeira, 2006: p.60).

De acordo com Martins e Morais (1999: p.51):

"O auditor interno, atua como "olhos" e "ouvidos" da direção, verificando o controlo das operações, profunda e pormenorizadamente. As suas análises e recomendações são uma preciosa ajuda para a direção e para os corpos diretivos de cada área específica, com o objetivo de alcançar um controlo mais eficaz, melhorar a operacionalidade e aumentar os benefícios."

Conforme citado por Carneiro (2013: p.25), não é mais possível conceber uma abrangente Gestão dos Riscos de Negócio sem considerar, de alguma forma, o papel do auditor interno como instrumento de identificação de vulnerabilidades e, até mesmo, de auxílio à implementação de processos de correção.

1.4. Gestão dos Riscos de Negócio Vs. Auditoria Interna

1.4.1. Papel da Auditoria Interna na Gestão dos Riscos de Negócio

Um dos principais cuidados da gestão está relacionada com os potenciais benefícios para a organização. Ligado a esta preocupação surge o risco, que inclui todos os riscos, desde o financeiro ao de negócio. O risco é extremamente importante para a Auditoria Interna, devido a sua relação com o sistema de controlo, pois quanto maior é o risco, maior é a necessidade de controlo (Martins *et al*., 1999: p.71).

Segundo a Norma de Gestão dos Riscos de Negócio (FERMA, 2002: p.13), o papel da Auditoria Interna pode diferir de uma organização para outra organização Na prática, a função da Auditoria Interna poderá incluir alguns ou todos os seguintes pontos:

- *Focar o trabalho da Auditoria Interna nos riscos significativos que foram identificados pela gestão da organização e fazer auditorias aos processos de Gestão dos Riscos de Negócio;*
- *Fornecer garantias sobre a Gestão dos Riscos de Negócio;*
- *Proporcionar um apoio e um envolvimento ativos ao processo de Gestão de Riscos de Negócio;*
- *Possibilitar a identificação/avaliação de riscos e dar formação aos funcionários sobre Gestão dos Riscos de Negócio e controlo interno coordenar a comunicação de riscos ao Conselho de Administração, ao comité de auditoria, etc.*

O "*The Institute of Internal Auditors"* (IIA, 2009: p.5:6), divide o papel da Auditoria Interna na Gestão dos Riscos de Negócios em 3 grupos:

1. Consultadoria:
    - Disponibilização das ferramentas de gestão e das técnicas utilizadas pela Auditoria Interna para analisar os riscos e controlos;
    - Aproveitar a experiencia na Gestão dos Riscos de Negócio e do conhecimento global da organização;
    - Deve Organizar "*Workshops"*, formação da organização matéria de riscos e controlos, e promover o desenvolvimento de um canal de comunicação e da estrutura da organização;
    - Agir como um ponto central para a coordenação, acompanhamento e elaboração de relatórios sobre os riscos da organização;
    - Apoiar os gestores a trabalharem para identificar a melhor forma de mitigar o risco.
2. Garantias:
    - Deve ficar claro que a gestão é responsável pela Gestão dos Riscos de Negócio;
    - As responsabilidades do auditor interno devem ser documentadas na carta de Auditoria Interna e aprovadas pelo comité de auditoria;
    - A Auditoria Interna não deve gerir qualquer um dos riscos em nome da administração;
    - A Auditoria Interna deve aconselhar e apoiar à tomada de decisão da administração, em vez de tomar decisões referentes á Gestão dos Riscos de Negócio;
    - A Auditoria Interna também não pode dar garantias objetivas em qualquer parte do quadro da Gestão dos Riscos de Negócio. Tais garantias devem ser fornecidas por terceiros devidamente qualificados;
    - Qualquer trabalho além das atividades de *"Assurance"* deve ser reconhecido como um compromisso de consultoria e as normas de execução relacionadas com tais compromissos, devem ser seguidas.
3. Experiencia e Conhecimento da Organização:
    - Os auditores internos e gestores do risco de negócio compartilham alguns conhecimentos, experiencia e valores. No entanto, os gestores de risco de negócio, como tal, servem apenas a gestão da organização e não tem que fornecer uma garantia independente e objetiva para o comité de auditoria;

- O responsável da Auditoria Interna não deve prestar serviços de consultoria nesta área se os conhecimentos adequados não estiverem disponíveis.

No Código de Ética e Normas Profissionais (IPAI, 2009b):

"*A atividade de Auditoria Interna tem que avaliar a eficácia e contribuir para a melhoria da Gestão de Riscos de Negócio, isto é, tem de determinar se os processos de Gestão dos Riscos de Negócio são eficazes é um julgamento que resulta da avaliação feita pelo auditor interno, de que:*

- *Os objetivos da organização sustentam e estão alinhados com a missão da organização;*
- *Os riscos significativos são identificados e avaliados;*
- *São selecionadas as respostas adequadas que alinham os riscos com o apetite de risco da organização;*
- *A informação relevante sobre o risco é identificada e comunicada em tempo oportuno transversalmente pela organização."*

De acordo com Ferreira (2010: p.88):

> *"A Auditoria Interna apresenta uma mudança de atitude e uma nova visão, uma vez que deixou de "olhar" só para os factos passados para passar a "olhar" para o presente e futuro, tornando-se um apoio importante da gestão e, como tal, acresce valor à organização. Com vista a este fim, acrescentar valor, o Auditor Interno passa a ter um papel importante no processo de Gestão dos Risco de Negócio."*

1.4.2. Funções do Auditor na Gestão dos Riscos de Negócio

De acordo com o "*The Instituite of Internal Auditors"* (IIA, 2004: p.5), o profissional de Auditoria Interna em matéria de Gestão dos Riscos de Negócio, deve seguir as seguintes funções:

- Funções fundamentais da Auditoria Interna, sobre a Gestão dos Riscos de Negócio:
    - Fornecer garantia em processos de Gestão dos Riscos de Negócio;
    - Dar garantia de que os riscos são avaliados corretamente;
    - Avaliar o processo de Gestão dos Riscos de Negócio;
    - Emitir relatórios de avaliação dos principais riscos;
    - Rever a Gestão dos Riscos de Negócio chave.
- Funções legítimas de Auditoria Interna que devem ser realizadas com Garantias:
    - Facilitar a identificação e avaliação de riscos;
    - Formar e gestão da resposta a riscos;
    - Coordenar as atividades de Gestão dos Riscos de Negócio;
    - Consolidar os relatórios sobre riscos;
    - Coordenar e Manter o "*Framework"* de Gestão dos Riscos de Negócio;
    - Defender a criação da Gestão dos Riscos de Negócio;
    - Desenvolver estratégias de Gestão dos Riscos de Negócio para aprovação da direção da empresa.
- Funções que a Auditoria Interna, não deve desempenhar.
    - Estabelecer o apetite pelo risco;
    - Impor processos de Gestão dos Riscos de Negócio;
    - Garantir a Gestão dos Riscos de Negócio;
    - Tomar decisões em resposta aos riscos;
    - Implementar respostas aos riscos em nome da administração;
    - Assumir a responsabilidade pela Gestão dos Riscos de Negócio.

Segundo o Relatório COSO ERM (COSO, 2004: p.96):

"Os auditores internos desempenham uma função essencial ao avaliar a eficácia da Gestão dos Riscos Negócio e ao recomendar melhorias."

Conforme citado por Pereira (2012: p.41), o auditor interno tem de ter em atenção à Gestão dos Risco de Negócio, ao efetuar o seu trabalho, tendo-a em consideração na fase do seu planeamento anual, avaliando a sua eficácia e o contributo para a instituição, nomeadamente a confiança e integridade das informações financeiras e operacionais, a eficácia e eficiência das operações, a salvaguarda dos ativos e o cumprimento com as leis, regulamentos e contractos, evitando a ocorrência de fraudes.

1.4.3. Cooperação com a atividade de Auditoria Interna

É comum numa organização a atividade de Auditoria Interna trabalhar em cooperação com a função de Gestão dos Riscos de Negócio. Algumas organizações não têm uma função formal de Gestão dos Risco de Negócio e, neste caso, a Auditoria Interna fornece muitas vezes de forma mais extensa, serviços de consultoria de Gestão de Risco de Negócio para a organização (Barros, 2012: p.51).

Como consultor do processo de Gestão dos Riscos de Negócio, o auditor interno disponibiliza à gestão, as ferramentas e técnicas utilizadas pela Auditoria Interna para examinar os riscos e os controlos; defende a introdução do ERM na entidade, dá consultoria, facilita "*workshops"*, forma a organização sobre o risco e o controlo e promove o desenvolvimento de uma linguagem comum, estrutura e compreensão; atua como ponte central de coordenação e apoia os gestores na forma como eles identificam a melhor maneira de mitigar o risco (Pereira 2012: p.42).

A Auditoria Interna pode fornecer serviços consultoria de Gestão dos Riscos de Negócio, desde que não conflitue com a sua independência e objetividade, e desde que se apliquem as seguintes condições (Barros, 2012: p.52):

- *"Deve ficar claro que a gestão continua a ser responsável pela Gestão dos Riscos de Negócio.*
- *Sempre que a Auditoria Interna, consulta a equipa de gestão para estabelecer ou melhorar os processos de Gestão dos Riscos de Negócio, o seu plano de trabalho deve incluir uma estratégia clara e cronograma para*

a migração da responsabilidade destas atividades para os membros da gestão.

- *A Auditoria Interna não pode dar garantia objetiva em qualquer parte da "framework" de Gestão dos Riscos de Negócio pela qual é responsável. Essa garantia deve ser fornecida por terceiros devidamente qualificados.*
- *A natureza de tais serviços prestados à organização deve ser documentada na Carta de Auditoria Interna e ser consistente com as suas outras responsabilidades.*
- *Qualquer aconselhamento de consultoria ou desafio (ou apoio) de gestão da decisão, não envolve a tomada de decisões próprias da Auditoria Interna na Gestão dos Riscos de Negócio."*

Conforme citado por Pereira (2012: p.43), qualquer trabalho além das atividades de garantia de Auditoria Interna deve ser reconhecido como um trabalho de consultoria e as normas de execução relativas a tais compromissos devem ser seguidas.

2. Capítulo II [Estudo de Caso]

2.1. Metodologia

2.1.1. Enquadramento Teórico

A metodologia é considerada como a disciplina instrumental que cria as condições propícias para que uma pesquisa se considere científica. De acordo com Fortin (1999: p.102), esta é uma fase de indiscutível importância, pois é ela que assegura a fiabilidade e a qualidade dos resultados da investigação.

A metodologia de investigação pode ser desenvolvida segundo uma perspetiva qualitativa ou quantitativa. A escolha entre os diferentes métodos deve depender da investigação em causa. O presente estudo tem como finalidade, perceber, analisar e sistematizar a questão de quem deverá assumir a responsabilidade pela Gestão dos Riscos de Negócio. Tendo em conta a análise proposta optou-se assim pela metodologia qualitativa. Segundo Creswell (2009: p.40), *existem variáveis que não podem ser medidas ou "vozes que não podem ser ouvidas"*, neste caso em específico, *"vozes que não podem ser ouvidas"*. Sendo este um estudo de carácter exploratório, a abordagem qualitativa revelou ser a escolha mais apropriada. Esta opção prende-se com a impossibilidade de obtenção de dados diretos através de entrevistas, que permitiriam complementar a análise de conteúdo, nomeadamente dos relatórios.

2.2. Estudo de Caso

O objetivo do presente estudo é compreender se a Gestão dos Risco de Negócio é da responsabilidade da Gestão da entidade ou da Auditoria Interna nas empresas cotadas no PSI-20 da Euronext de Lisboa. De acordo a Norma de Gestão de Riscos de Negócio (FERMA, 2002: p.13), o papel da Auditoria Interna pode diferir de organização para organização, na prática a função da Auditoria Interna, poderá fornecer garantias sobre a Gestão de Riscos de Negócio. Contudo o IIA (2004: p.5) apresenta uma visão contrária, e refere que a Auditoria Interna, não deve garantir a Gestão dos

Riscos de Negócio. É com base nesta controvérsia, que irá prosseguir a seguinte investigação.

A questão de partida para o presente trabalho é:

- Quem possui a responsabilidade pela Gestão dos Riscos de Negócio?

Em Portugal, as sociedades emitentes de ações admitidas à negociação em mercado regulamentado, são obrigadas a disponibilizar anualmente informação sobre o grau de acolhimento do Código de Governo das Sociedades, o qual consiste num conjunto de recomendações elaboradas pela Comissão do Mercado de Valores Mobiliários (CMVM).

A seguinte tabela projeta todas as variáveis que vão ser objeto do nosso estudo.

Q1	Existência de atividade de Auditoria Interna.
Q2	Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio.
Q3	A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento.
Q4.1	Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio.
Q4.2	Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio.
Q4.3	Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio.
Q4.4	Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio.
Q4.5	Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio.
Q5.1	Quem é o responsável pela Identificação/Avaliação dos riscos.
Q5.2	Quem é o responsável pela definição do grau de exposição ao risco.
Q6	Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio.
Q7	Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio.
Q8	Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio.
Q9	Quais as principais categorias de Riscos.

Tabela 2 - Variáveis em estudo.

2.3. Descrição do Universo

Para a elaboração deste projeto foram selecionadas as 18 empresas que integram o Índice PSI-20 da "*Euronext"* de Lisboa, sendo elas, as seguintes:

- Altri;
- BCP;
- Banco BPI;
- Banif;
- CTT;
- EDP;
- EDP Renováveis;
- Galp Energia;
- Impresa
- Jerónimo Martins;
- Mota-Engil;
- Portucel;
- Portugal Telecom;
- REN;
- Semapa;
- Sonae;
- Teixeira Duarte;
- ZON Optimus (Atual NOS).

2.4. Recolha de dados

Através do Sistema de Difusão de Informação do portal da CMVM (www.cmvm.pt), foram obtidos os últimos relatórios referentes ao Governo das Sociedades das empresas cotadas no Índice PSI-20 da "*Euronext"* de Lisboa, conforme apresenta a seguinte tabela:

Empresa	Ano
Altri	2013
Banco BPI	2013
Banif	2013
BCP	2013
CTT	2013
EDP	2013
EDP Renováveis	2013
Galp Energia	2013
Impresa	2011
Jerónimo Martins	2013
Mota-Engil	2012
ZON OPTIMUS (atual NOS)	2013
Portucel	2012
Portugal Telecom	2013
REN	2013
Semapa	2013
Sonae SGPS	2013
Teixeira Duarte	2013

Tabela 3 - Relatórios consultados.

2.5. Análise de Resultados

No ponto que se segue serão tratados e analisados os resultados obtidos neste estudo, de acordo com variáveis anteriormente mencionadas.

- **Q1 - Existência de atividade de Auditoria Interna**

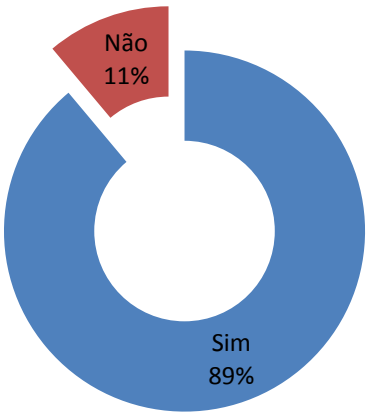


Figura 3 - Existência de atividade de Auditoria Interna.

Perante o universo selecionado, constatou-se que apenas 2 empresas não possuem atividade de Auditoria Interna, o caso da Altri e da Semapa.

- **Q2 - Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio**

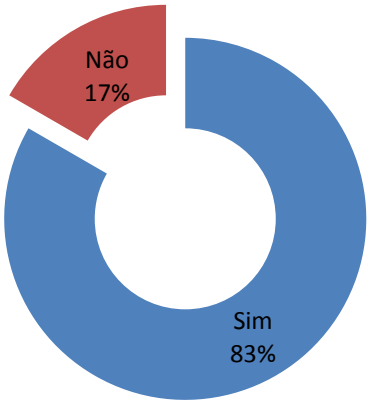


Figura 4 - Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio.

A existência de um gabinete ou departamento com funções no âmbito da Gestão dos Riscos de Negócio é comum na maioria das empresas e representa 83% do universo analisado. Só não se verifica a existência dessa função no caso da Semapa, Altri e Teixeira Duarte.

- **Q3 - A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento**

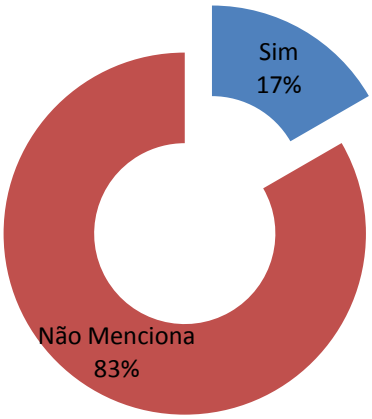


Figura 5 - A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento.

A afetação da atividade de Auditoria Interna e da atividade da Gestão dos Riscos de Negócio ao mesmo departamento ou unidade da organização é mencionado em

apenas 17% das empresas do universo analisado, como é o caso da Mota Engil, Sonae e Banif.

- **Q4.1 - Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio**

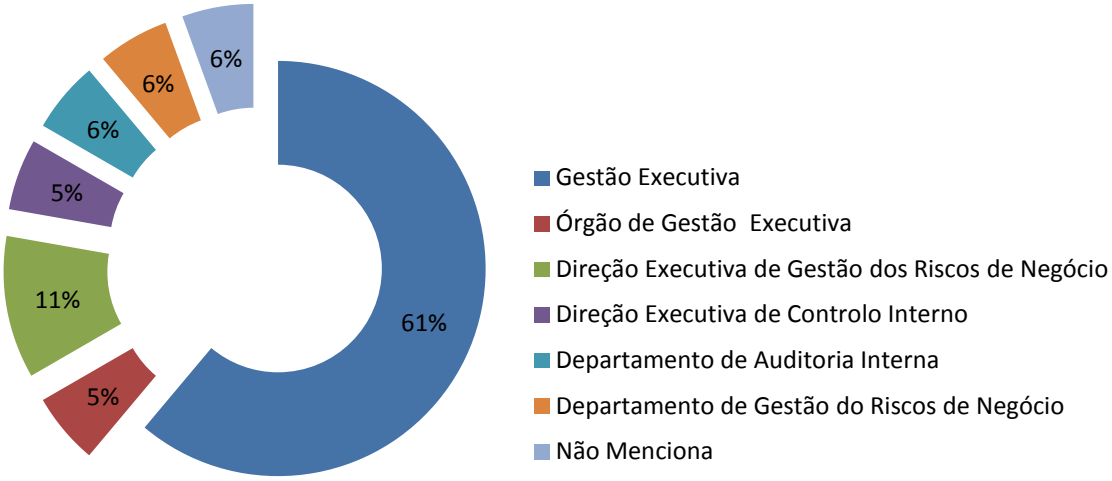


Figura 6 - Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio.

A responsabilidade pela implementação do processo de Gestão dos Riscos de Negócio é atribuída em 61% do universo analisado à Gestão Executiva e em 21% aos órgãos executivos e às direções executivas especializadas. Apenas em duas empresas essa responsabilidade é delegada a departamentos especializados (Sonae e BCP).

- **Q4.2 - Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio**

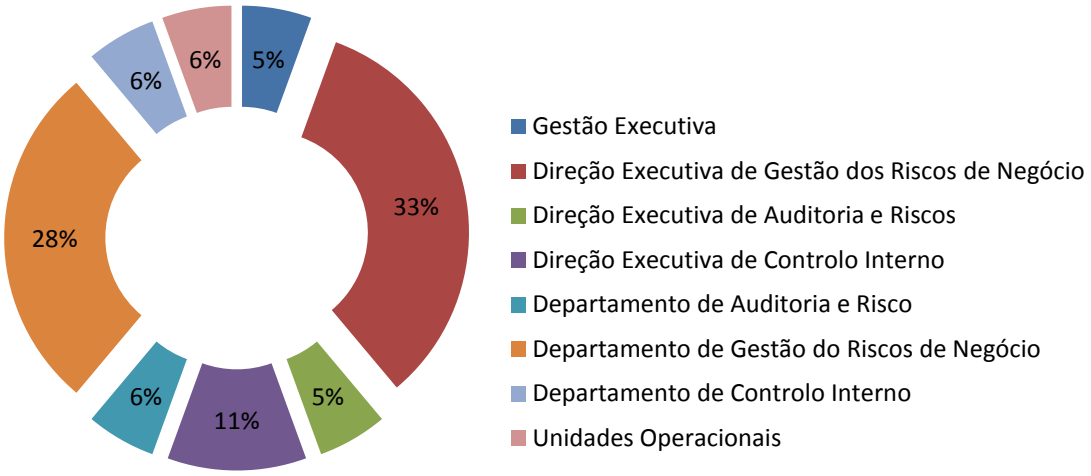


Figura 7 - Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio.

A responsabilidade pelo funcionamento do processo de Gestão dos Riscos de Negócio é atribuída em 61% do universo analisado à Direção Executiva de Gestão dos Riscos de Negócio e ao Departamento de Gestão dos Riscos de Negócio. É de salientar que no caso da Altri esta responsabilidade é assumida pelas unidades operacionais. No restante universo analisado a responsabilidade é imputada homogeneamente à gestão, restantes direções especializadas e departamentos especializados.

- **Q4.3 - Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio**

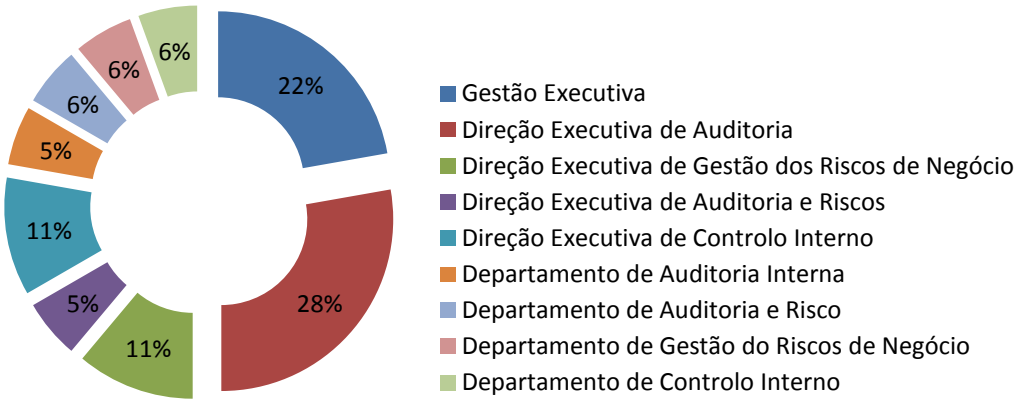


Figura 8 - Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio.

Quanto à responsabilidade pela monitorização do processo de Gestão dos Riscos de Negócio não é evidenciada nenhuma vantagem percentual em relação a nenhuma área específica das empresas do universo analisado. No entanto é da máxima

importância salientar que a gestão executiva e as direções executivas especializadas são em 77% da do universo analisado o órgão competente pela respetiva monitorização.

- **Q4.4 - Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio**

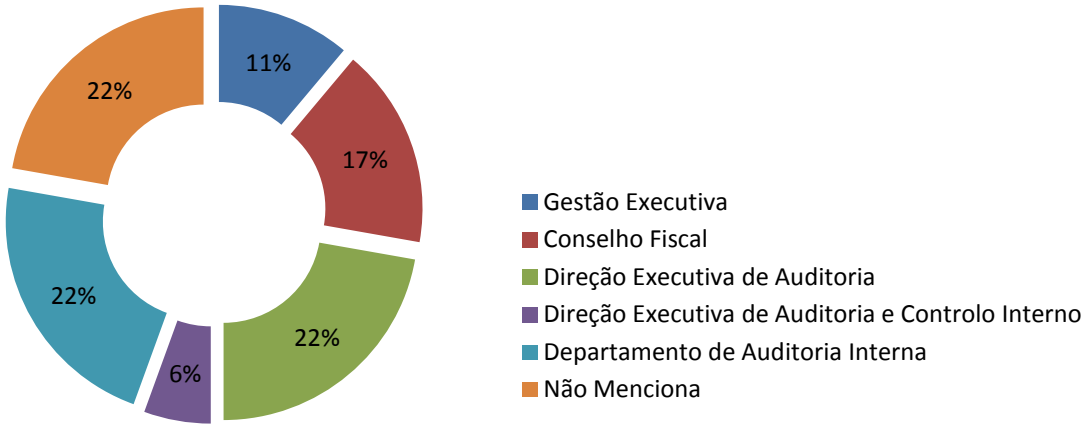


Figura 9 - Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio.

A Eficiência e Eficácia do processo de Gestão dos Riscos de Negócio são asseguradas em 44% do universo analisado pela Direção Executiva de Auditoria e pelo Departamento de Auditoria Interna. Importa ainda referir que em 17% do universo analisado é o Conselho Fiscal que garante as respetivas funções.

- **Q4.5 - Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio**

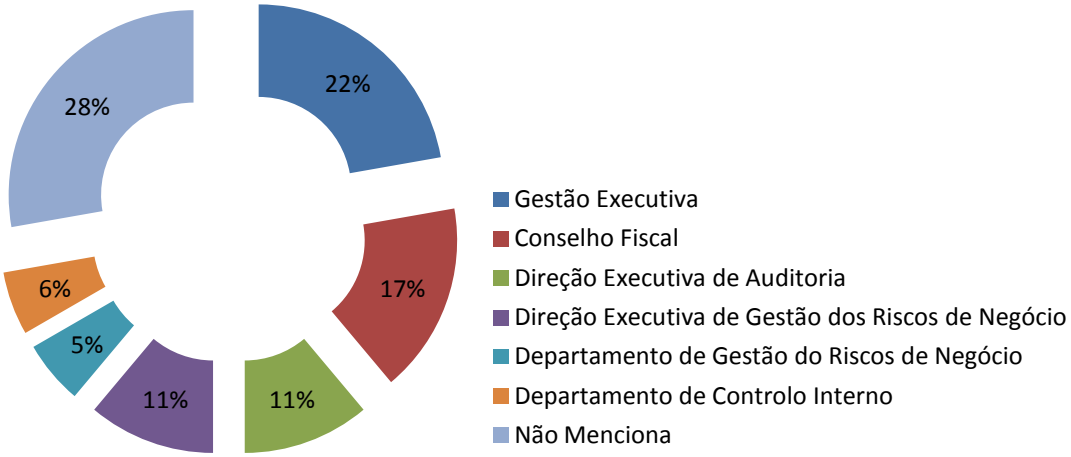


Figura 10 - Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio.

Quanto à responsabilidade pela revisão do processo de Gestão dos Riscos de Negócio não é evidenciada nenhuma vantagem percentual em relação a nenhuma das

áreas específicas das empresas do universo analisado. Contudo é importante salientar que para a variável em questão a gestão executiva, conselho fiscal e das direções executivas especializadas representam 61% do universo analisado. Verifica-se ainda que 28% das empresas selecionadas, não mencionam nos relatórios do governo das sociedades qual a área responsável pela revisão do processo.

Q5.1 - Quem é o responsável pela Identificação/Avaliação dos riscos

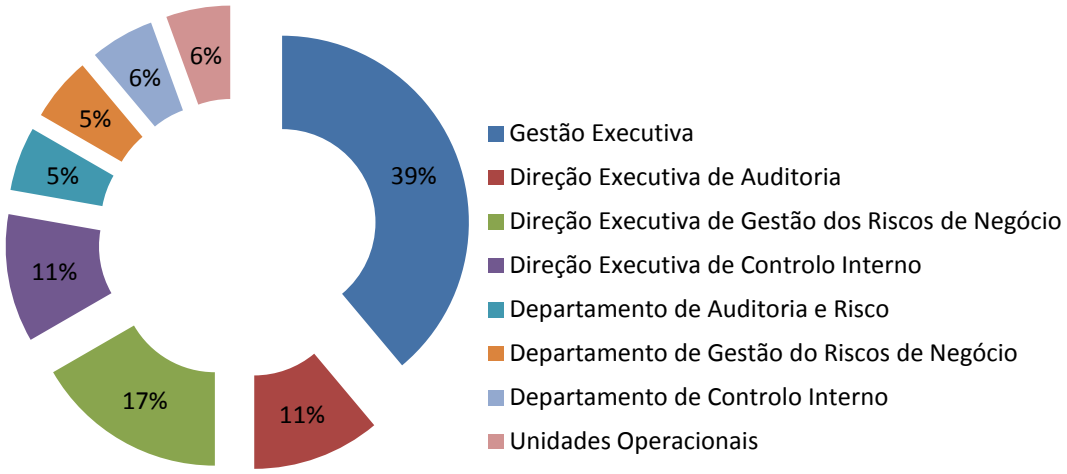


Figura 11 - Quem é o responsável pela Identificação/Avaliação dos riscos.

A responsabilidade da identificação e avaliação dos riscos é atribuída em 39% à Gestão Executiva, sendo a área da empresa mais evidenciada. É ainda de referir que o conjunto da gestão executiva e das direções executivas especializadas é mencionado por 72% das empresas.

- **Q5.2 - Quem é o responsável pela definição do grau de exposição ao risco**

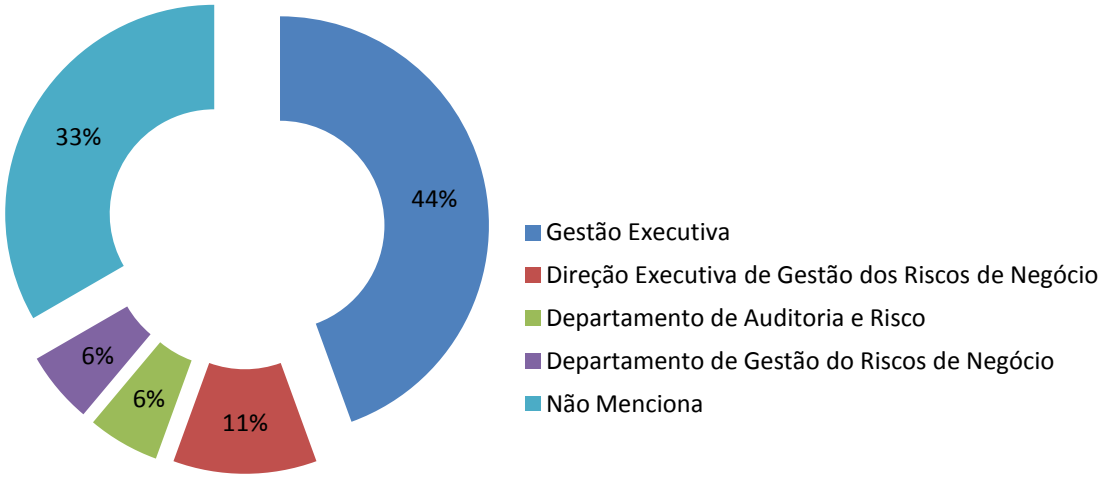


Figura 12 - Quem é o responsável pela definição do grau de exposição ao risco.

Em 44% dos casos é da responsabilidade da Gestão Executiva a definição do grau de exposição ao Risco. Contudo em 33% do universo analisado a mesma responsabilidade não é se quer identificada.

- **Q6 - Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio**

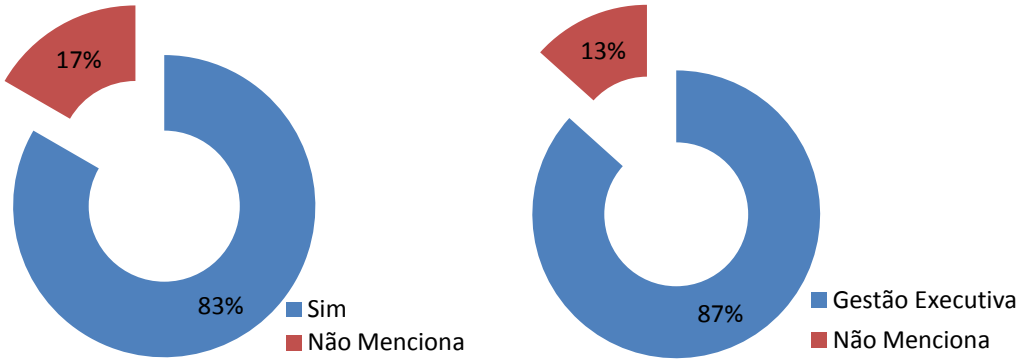


Figura 13 - Existência e Responsável pelas políticas de Gestão dos Riscos de Negócio.

Constata-se que em 83% das empresas analisadas são emitidas políticas de Gestão dos Riscos de Negócio. É importante referir que em 87% das empresas que emitem políticas de Gestão dos Riscos e Negócio essa emissão é efetuada pela Gestão executiva.

- **Q7 - Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio**

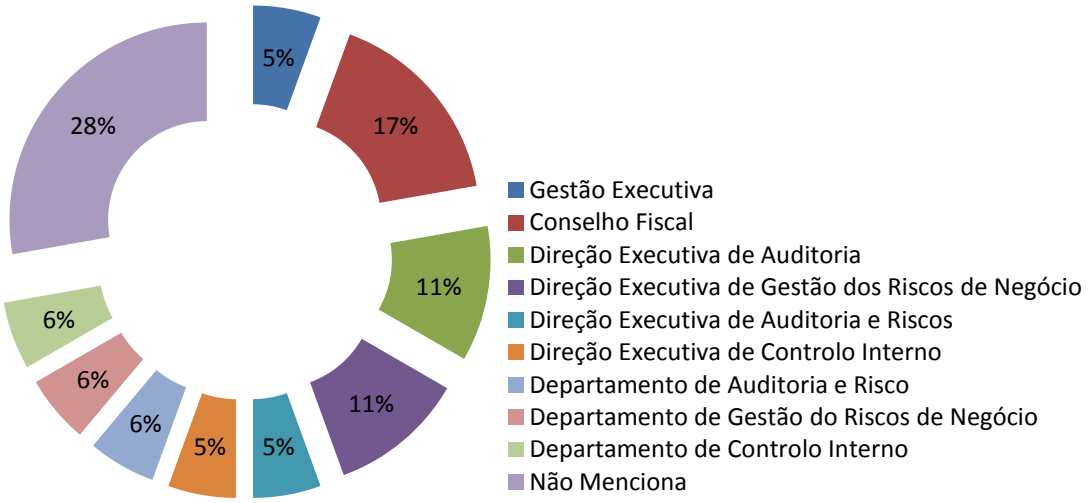


Figura 14 - Existência e Responsável pelas políticas de Gestão dos Riscos de Negócio.

No que diz respeito à responsabilidade pela emissão de recomendações sobre o processo de Gestão dos Riscos de Negócio, não é evidenciada nenhuma vantagem percentual, sobre alguma área específica das empresas analisadas. No entanto, a responsabilidade atribuída à gestão executiva, conselho fiscal e das direções executivas especializadas representa 54%. No total, 28% das empresas não refere nos relatórios do governo das sociedades de quem é a responsabilidade pela emissão de recomendações.

- **Q8 - Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio**

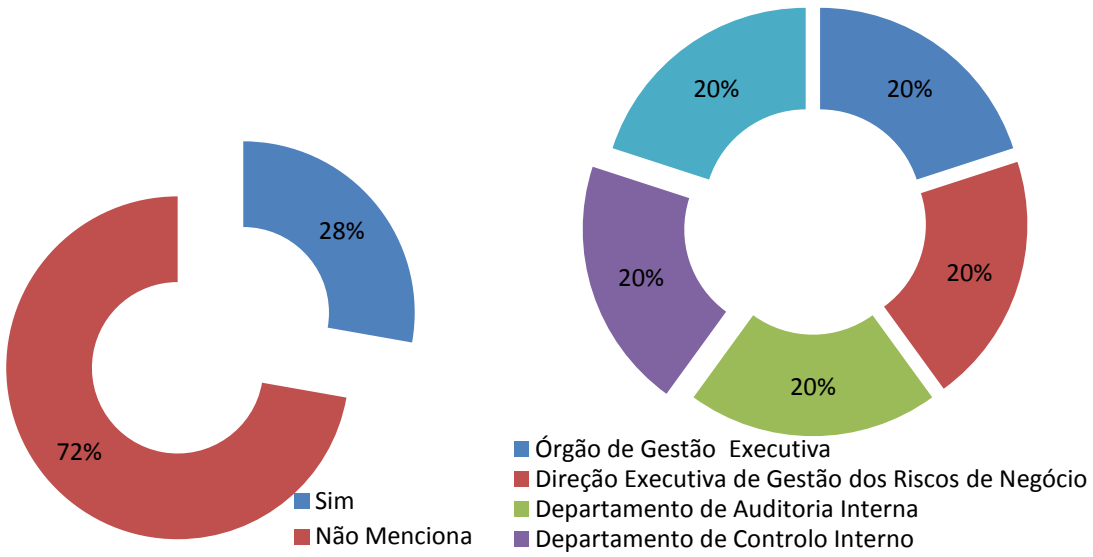


Figura 15 - Existência e Responsável pela formação da organização quanto à Gestão dos Riscos de Negócio.

Somente 28% das empresas refere a existência de formação na organização no âmbito da Gestão dos Riscos de Negócio. O restante universo analisado apresenta uma

distribuição homogénea quanto ao responsável por essa formação, o que não permite destacar nenhuma área da organização em específico.

- **Q9 - Quais as principais categorias de riscos**

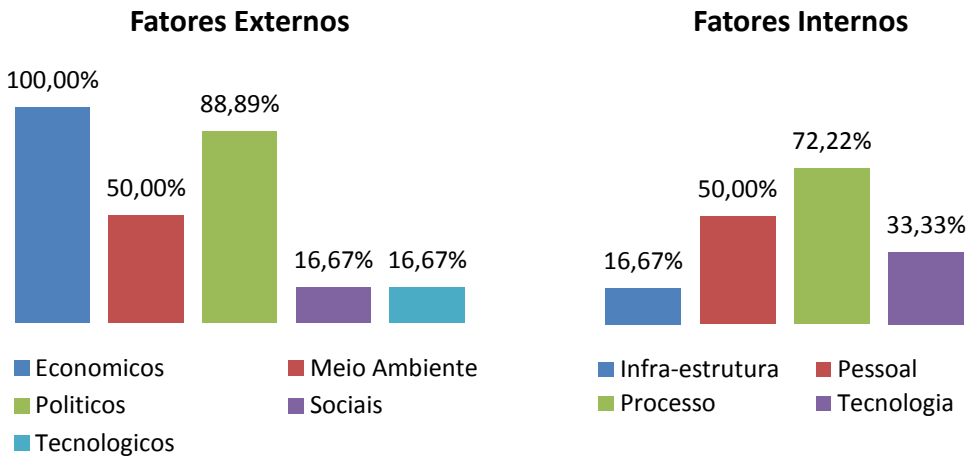


Figura 16 - Quais as principais categorias de riscos.

Apesar de não ser o tópico com maior relevância no respetivo estudo e atendendo às categorias dos eventos mencionados no COSO (2004: p.51), importa referir que todas as empresas identificaram como um dos principais riscos de negócio, o risco económico. Contudo o risco político e o risco do processo são também assumidos por 88,89% e 72,22% das empresas.

3. Capitulo III [Conclusão]

No final do século XX, os Estados Unidos da América deparam-se com uma crise originada por consecutivos escândalos financeiros, que acabaram por afetar conceituadas empresas americanas. As principais ilegalidades ocorridas foram protagonizadas pelos gestores das empresas, o que desencadeou uma crise de confiança no mercado global (Alves, 2009: p.15).

Em Portugal existem mecanismos para proteger os investidores que operam na Bolsa de Valores. O regulamento da CMVM N.º4/2013 descreve os requisitos gerais das sociedades cotadas. O Artigo nº 1 do referido regulamento, aborda a estrutura e práticas do governo da sociedade e solicita às empresas um relatório detalhado sobre a estrutura e as práticas do governo societário.

Uma vez que o principal objetivo do presente estudo é apurar de quem é a responsabilidade pelo processo de Gestão dos Riscos de Negócio, procedeu-se à recolha da informação descrita nos últimos relatórios de governo societário, publicados no Sistema de Difusão da Informação do portal da CMVM das 18 empresas cotadas no PSI-20 da "*Euronext"* de Lisboa.

Com base na análise efetuada é possível concluir que a maioria das empresas dispõe de atividade autónoma de Auditoria Interna, e de um departamento ou gabinete com funções no âmbito da Gestão dos Riscos de Negócio. Contudo, apenas 3 empresas mencionaram a afetação da atividade de Auditoria Interna à atividade de Gestão dos Riscos de Negócio.

No que respeita à implementação do processo de Gestão dos Riscos de Negócio este é assegurado na maioria dos casos pela gestão executiva (62%), estando garantido quase na totalidade pelo conjunto da gestão executiva, órgãos de gestão executiva e departamentos executivos especializados (82%). Este resultado é sustentado pelo COSO (2004: p.92:99) o qual refere que a gestão deve assumir a iniciativa pela implementação da Gestão dos Riscos de Negócio.

Quanto à responsabilidade pelo funcionamento do processo de Gestão dos Riscos de Negócio, a mesma é assegurada na maioria dos casos pelas direções executivas e departamentos de Gestão dos Riscos de Negócio (61%).

A responsabilidade pela monitorização do processo de Gestão dos Riscos de Negócio é assumida pelo conjunto da gestão executiva e das direções executivas especializadas (77%).

No que respeita à avaliação da eficácia e eficiência do processo de Gestão dos Riscos de Negócio, em 44% das empresas é assegurada pelas direções executivas de Auditoria e departamentos de Auditoria Interna. Conforme citado por Pereira (2012: p.41) a atividade de Auditoria Interna no espaço da Gestão dos Riscos de Negócio, tem como objetivo garantir a eficácia e eficiência do processo.

A responsabilidade pelo processo de Gestão dos Riscos de Negócio é assumida na maioria dos casos pelo conjunto da gestão executiva, conselho fiscal e as direções executivas especializadas (61%).

A identificação dos riscos é assumida pelo conjunto da gestão executiva e das direções executivas especializadas (72%). Estando em conformidade com o referido pelo IIA (2009: p.5:6), de que a principal responsabilidade na identificação e gestão dos riscos pertence aos administradores.

A definição do grau de exposição ao risco é determinada pela gestão executiva, o que sustenta o referido pelo IIA (2004), de que a Auditoria Interna não deve estabelecer o apetite pelo risco.

Verificou-se que 83% das empresas emitem políticas no âmbito da Gestão dos Riscos de Negócio e das quais 87% atribuem a responsabilidade pela sua emissão à gestão executiva.

A emissão de recomendações acerca do processo de Gestão dos Riscos de Negócio é assegurado na grande maioria pelo conjunto da gestão executiva, conselho fiscal e direções executivas especializadas.

Conforme referido pelo IIA (2009: p.5:6), a Gestão tem a responsabilidade global de assegurar que os riscos são geridos. Na prática, a Gestão irá delegar a

operacionalização da estrutura de Gestão de Riscos de Negócio aos diversos Gestores/Responsáveis. Acrescenta ainda que todos os membros de uma organização contribuem para o sucesso da Gestão de Risco empresarial. De um modo geral os resultados obtidos no presente estudo, permitem considerar que a responsabilidade pelo processo de Gestão dos Riscos de Negócio compete as unidades de gestão.

De outro modo, conforme referido pelo (COSO, 2004: p.92:99) é possível assumir que cabe aos Gestores/Responsáveis apoiar a filosofia de Gestão de Riscos de Negócio, incentivar a observação do apetite pelo risco e gerir os riscos dentro das suas esferas de responsabilidade, conforme as tolerâncias definidas pelo risco. Regra geral, cabe ao diretor de riscos, diretor-financeiro, auditor interno e outros, responsabilidades fundamentais de suporte. Os outros membros da organização são responsáveis pela execução da Gestão de Riscos de Negócio em cumprimento das diretrizes e dos protocolos estabelecidos. No caso da análise em questão e de forma sucinta:

- A implementação do processo é da responsabilidade da gestão executiva;
- O funcionamento do processo é da responsabilidade do departamento ou da direção executiva de Gestão de Riscos de Negócio;
- A monitorização do processo é da responsabilidade da gestão executiva ou das direções executivas especializadas;
- A avaliação da eficácia e eficiência do processo é da responsabilidade da direção executiva de auditoria ou do departamento de Auditoria Interna;
- A revisão do processo é da responsabilidade da gestão executiva, ou do conselho fiscal ou dos departamentos especializados;
- A emissão de políticas de Gestão dos Riscos de Negócio é da responsabilidade da gestão executiva;
- A emissão de recomendações acerca do processo é da responsabilidade da gestão executiva, ou do conselho fiscal ou dos departamentos especializados.

Por fim, importa referir que o processo da Gestão dos Riscos de Negócio não é da responsabilidade de um único interveniente ou de uma única área da empresa, derivando da fase do processo. Convém realçar, que as entidades ligadas à administração da empresa asseguram quase a totalidade do processo.

Limitações do Estudo

A principal limitação deste estudo prende-se com a impossibilidade de obtenção de dados diretos através de entrevistas, os quais permitiriam complementar e validar a análise de conteúdo, nomeadamente dos relatórios.

Pistas para futuras investigações

Atendendo ao facto de neste estudo só terem sido recolhidos os relatórios referente as empresas do PSI-20 da "*Euronext"* de Lisboa, sugere-se que o número da universo analisado seja alargado a todas as sociedades emitentes de ações admitidas à negociação em mercado regulamentado.

Referências Bibliográficas

- ABNT (2009). *"NBR ISSO 31000:2009"*.
- Almeida, Domingos M. S. (2008). *"Gestão de Risco nas Organizações"*. Jornadas Regionais da Qualidade. Funchal.
- Almeida, Maria A.P.N. (2005). *"Aprender a Gerir as Organizações no Século XXI"*. Áreas Editora S.A.
- Alves, Ana C. M. R. (2009). *"A Evolução da Lei Sox – Impactos Indirectos no caso português"*. Dissertação de Mestrado em Contabilidade – Ramo Auditoria, Instituto Superior de Contabilidade e Administração da Universidade de Aveiro.
- Barros, Ana J. N. (2012). *"O Processo de Gestão de Risco nas Organizações"*. Dissertação de Mestrado em Auditoria, Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- Carneiro, Sílvia E. S. M. (2013). *"Quais os Atributos que um Auditor Interno deve ter"*. Dissertação de Mestrado em Auditoria, Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- CMVM – Comissão de Mercado de Valores Mobiliários (2007). *"Recomendações da CMVM sobre o Governo das Sociedades Cotadas".*
- CMVM – Comissão de Mercado de Valores Mobiliários (2010). *"Código do Governo das Sociedades - Recomendações"*.
- CMVM – Comissão de Mercado de Valores Mobiliários (2013). *"Regulamento N.º4/2013"*.
- COSO (2004). *"Gestão de Riscos Corporativos – Estrutura Integrada".*
- Creswell, J. W. (2007). *"Qualitative inquiry and research design: Choosing among five approaches"*. Thousand Oakes. CA: Sage Publications.
- FERMA - *Federation of European Risk Mangement Associations* (2003). *"Norma de Gestão de Risco".*
- Ferreira, Albertina C. C. F. (2010). *"A Gestão de Risco Aplicada à Auditoria Interna"*. Dissertação de Mestrado em Contabilidade e Auditoria, Universidade de Aveiro.
- Fonseca, Jaime Raúl Seixas (2008). "*Os Métodos Quantitativos na Sociologia: Dificuldades de uma Metodologia de Investigação*". VI Congresso Português de Sociologia. Universidade Nova de Lisboa.

- Fortin, Marie-Fabienne (1999). "*O processo de Investigação: da concepção à realização"*. 2ª Edição. Loures: Lusociência.
- Gonçalves, Cristina D. T. N. (2009). "*SOX – Sarbanes Oxley Act – O Desemvolvimento e impacto nas Organizações"*. Projeto de Mestrado em Gestão. Instituto Superior de Ciências do Trabalho e da Empresa.
- Holanda, A. (2006). "*Questões sobre pesquisa qualitativa e pesquisa fenomenológica"*. Análise Psicológica. 3 (XXIV).
- Humphrey C., Jones J. & Khalifa R. (2004). *"Business Risk Auditing And The Auditing Profession Status, Identity and Fragmention*". Federal School of Business and Mangment – University of Manchester.
- IFAC (2009). "*International Standard on Auditing - ISA 610 (Revised)"*.
- IIA (2004). "*The Role of Internal Auditing in Enterprise-wide Risk Management*",
- IIA (2004). "*El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial"*.
- IIA (2009). "*Declaração de Posicionamento do IIA: O papel da Auditoria Interna no suprimento de recursos para a Atividade de Auditoria Interna"*.
- IIA (2009). "*IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management"*.
- ISO (2009). "*ISO/Guide 73:2009"*. Consultado a 5 de Janeiro de 2014 em https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en .
- Instituto Português de Auditoria Interna (2009b). *"Enquadramento Internacional das Praticas Profissionais de Auditoria Interna"*. Norma 2120 – Gestão do Risco.
- Instituto Português de Auditoria Interna (2009a). *"Enquadramento Internacional das Praticas Profissionais de Auditoria Interna*". Norma 2210 – Governação.
- Livian, Yves-Frédéric (1987). *"Gérer le pouvoir dans les entreprises et les organisations: l'analyse des comportements politiques"*. Les Editions LSF.
- Marques, Carlos A.F. (2012). *"A Gestão dos Gestores".* Universidade de Évora.
- Marques, M. (1997). *"Auditoria e Gestão".* 1.ºEdição, Editorial Presença.
- Martins, I. & Morais, G. (1999). *"Auditoria Interna – Função e Processo".* 1.ºEdição. Áreas Editora.

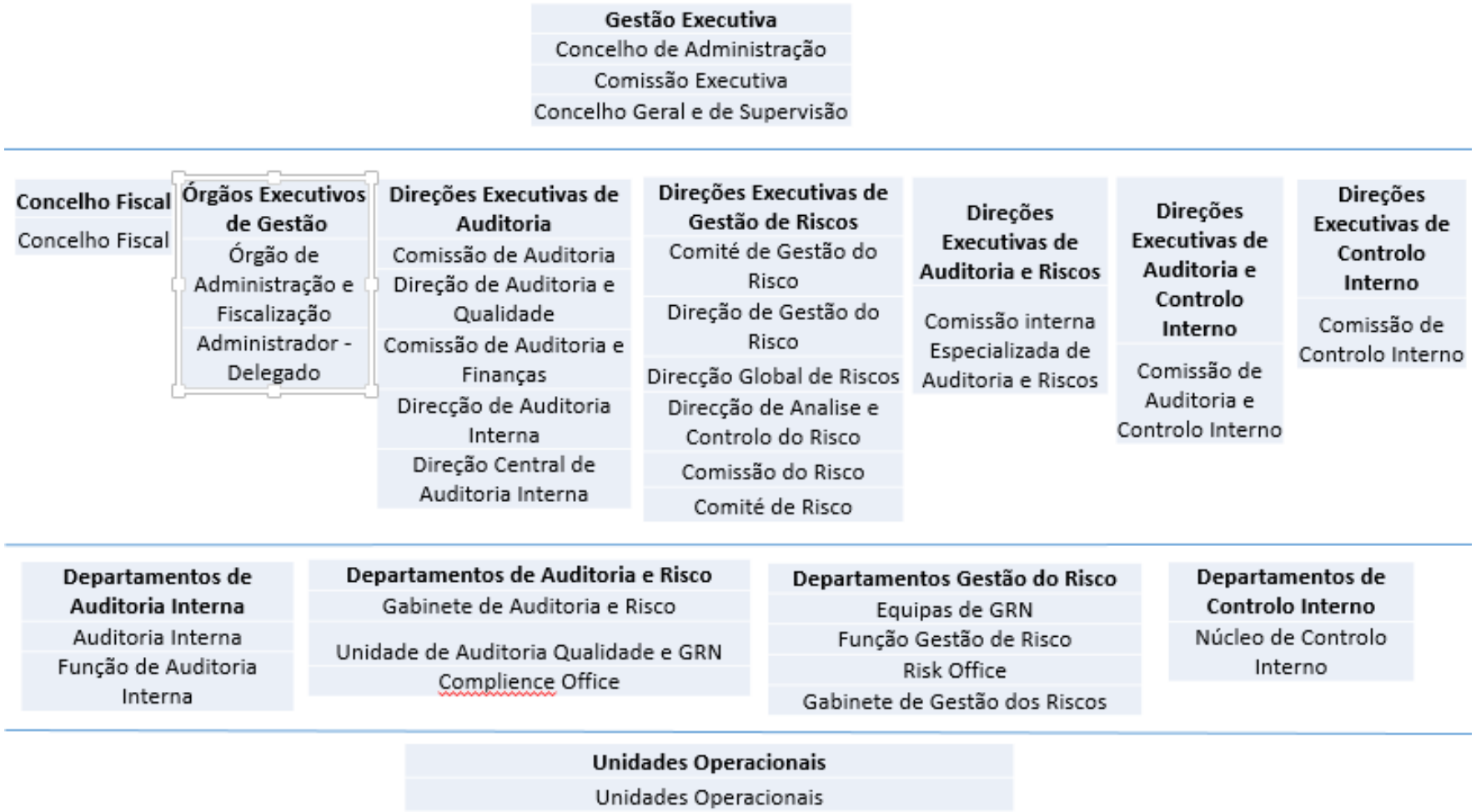
- Martins, Sandra A. M. (2013). *"A Importância da Auditoria Interna e a Avaliação do Desempenho da Organização".* Dissertação de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- Mendes, Carlos M. A. (2010). "*Projecto Odisseia - Implementação de Processo de Gestão de Riscos de Negócio no Grupo Portugal Telecom".*
- Moresi, Eduardo (2003). "*Metodologia de Pesquisa*". Universidade Católica de Brasília.
- Morse, J. M. (1994). "*Designing Funded Qualitative Research".* Denzin, N. & Lincoln , Y. Handbook of qualitative research. USA: Sage Publications.
- Nelson, Bob & Economy, Peter (2005). "*A Bíblia da Gestão*". Editora Pergaminho. 1.ºEdição.
- Oda, Erico & Marques, Cícero (2008). "*Gestão das Funções Organizacionais*". IESDE Brasil.
- Pereira, Joana S. R. (2012). "A Auditoria e Gestão do Risco Empresarial". Dissertação de Mestrado em Auditoria e Análise Financeira. Escola Superior de Gestão de Tomar - Instituto Politécnico de Tomar.
- Pinheiro, Catarina G. A. (2013). *"Acrescentar valor á Organização com a Auditoria Interna"*. Dissertação de Mestrado em Auditoria, Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- Pinheiro, Joaquim L. (2010). "*Auditoria Interna*". 2.º Edição, Reis Livros.
- Pinheiro, Juliano L. (2005). *"Mercado de Capitais: Fundamentos e Técnicas"*. São Paulo: Atlas.
- Pinto, Juarez (2012). "*Auditoria Interna como Instrumento de Gestão na Organização: Um estudo nas empresas do estado de São Paulo listadas na BM&FBOVESPA"*. Dissertação de Mestrado em Ciências Contábeis. Fundação Escola de Comercio Alvares Penteado.
- Pires, Ana I.M. P. (2008). "*Impacto da Lei Sarbanes Oxley no Sistema de Controlo Interno das Empresas cotadas nos EUA"*. Dissertação de Mestrado em Contabilidade e Auditoria. Universidade Aberta.
- Pires, José P. F. A. S. (2010). *"Contributo da Auditoria Interna na Detecção e Mitigação de Riscos Empresariais"*. Dissertação de Mestrado em Auditoria.

Instituto Superior de Contabilidade e Administração de Lisboa – Instituto Politécnico de Lisboa.

- Quivy, R. &. (1995). *"Manuel de Recherche en Sciences Sociales"*. Paris: Gradiva.
- Santos, António R. (2008). *"Gestão Estratégica"*. Escolar Editora. 1.º Edição.
- Santos, Malvina M. (2013). *"O Controlo Interno e a Gestão de Risco nas Empresas da Área Metropolitana do Porto"*. Dissertação de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- Sousa, Mária V. (2012). "A Gestão de Risco nas Empresas – Comparação das Práticas de Gestão do Risco no sector da construção em Portugal e no Reino Unido". Dissertação de Mestrado em Gestão. Universidade Lusófona do Porto.
- Stoner, James A.F. & Freeman, Edward R. (1985). *"Administração".* Editora Prentice Hall do Brasil. 5.ºEdição.
- Teixeira, Mária F. (2006). *"O contributo da Auditoria Interna para uma Gestão eficaz"*. Dissertação de Mestrado em Contabilidade e Auditoria". Universidade Aberta.
- Teixeira, Sebastião (2005). *"Gestão das Organizações".* McGrawHill, 2.ºEdição.
- Tribunal de Contas (2011). *"A Função de Auditoria Interna no SEE".* Relatório N.º08/2011 – 2.º Secção.
- Vale, Carla A. M. P. (2011). *"Gestão de Risco – Caso da Sonae Industria".* Dissertação de Mestrado em Auditoria. Instituto Superior de Contabilidade e Administração do Porto – Instituto Politécnico do Porto.
- Yin, R. K. (2003). "*Case study research: Design and methods"*. 3. º Edição. Thousand Oaks. CA**.**

Anexos

Categorias de Resultados



	Empresa:	EDP	SEMAPA	MOTA ENGIL	CTT	ZON OPTIMUS
Q1	Existência de atividade de Auditoria Interna	**Sim**	**Não**	**Sim**	**Sim**	**Sim**
Q2	Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio	**Sim**	**Não**	**Sim**	**Sim**	**Sim**
Q3	A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento	**Não Menciona**	**Não Menciona**	**Sim**	**Não Menciona**	**Não Menciona**
Q4.1	Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Direção Executiva de Controlo Interno**	**Gestão Executiva**	**Gestão Executiva**	**Gestão Executiva**
Q4.2	Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Controlo Interno**	**Departamento de Auditoria e Risco**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**
Q4.3	Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Direção Executiva de Controlo Interno**	**Gestão Executiva**	**Departamento de Auditoria e Risco**	**Departamento de Auditoria Interna**
Q4.4	Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Conselho Fiscal**	**Conselho Fiscal**	**Direção Executiva de Auditoria**	**Departamento de Auditoria Interna**
Q4.5	Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Conselho Fiscal**	**Conselho Fiscal**	**Gestão Executiva**	**Gestão Executiva**
Q5.1	Quem é o responsável pela Identificação/Avaliação dos riscos	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Controlo Interno**	**Departamento de Auditoria e Risco**	**Gestão Executiva**	**Gestão Executiva**
Q5.2	Quem é o responsável pela definição do grau de exposição ao risco	**Gestão Executiva**	**Gestão Executiva**	**Departamento de Auditoria e Risco**	**Não Menciona**	**Gestão Executiva**
Q6 (a)	Existem Politicas de Gestão dos Riscos de Negócio	**Sim**	**Não Menciona**	**Sim**	**Sim**	**Sim**
Q6 (b)	Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Não Menciona**	**Gestão Executiva**	**Não Menciona**	**Gestão Executiva**
Q7	Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio	**Não Menciona**	**Conselho Fiscal**	**Departamento de Auditoria e Risco**	**Conselho Fiscal**	**Não Menciona**
Q8 (a)	Existe formação na organização quanto à Gestão dos Riscos de Negócio	**Sim**	**Não Menciona**	**Não Menciona**	**Não Menciona**	**Não Menciona**
Q8 (b)	Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio	**Não Menciona**	**Não Menciona**	**Não Menciona**	**Não Menciona**	**Não Menciona**
Q9	Quais as principais categorias de riscos					
	Fatores Externos					
	Económicos	x	x	x	x	X
	Meio Ambiente	x	x			
	Políticos	x	x	x	x	
	Sociais				x	
	Tecnológicos				x	X
	Fatores Internos					
	Infraestrutura	x				
	Pessoal				x	X
	Processo	x	x			X
	Tecnologia				x	X

	Empresa:	ALTRI	TEIXEIRA DUARTE	SONAE	PORTUCEL	REN	BANIF
Q1	Existência de atividade de Auditoria Interna	**Não**	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Q2	Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio	**Não**	**Não**	**Sim**	**Sim**	**Sim**	**Sim**
Q3	A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento	**Não Menciona**	**Não Menciona**	**Sim**	**Não Menciona**	**Não Menciona**	**Sim**
Q4.1	Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Gestão Executiva**	**Departamento de Auditoria Interna**	**Órgão de Gestão Executiva**	**Gestão Executiva**	**Não Menciona**
Q4.2	Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio	**Unidades Operacionais**	**Gestão Executiva**	**Departamento de Gestão do Riscos de Negócio**	**Direção Executiva de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Auditoria e Riscos**
Q4.3	Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Gestão Executiva**	**Direção Executiva de Auditoria**	**Direção Executiva de Controlo Interno**	**Gestão Executiva**	**Direção Executiva de Auditoria e Riscos**
Q4.4	Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Não Menciona**	**Departamento de Auditoria Interna**	**Não Menciona**	**Direção Executiva de Auditoria**	**Departamento de Auditoria Interna**
Q4.5	Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio	**Não Menciona**	**Gestão Executiva**	**Conselho Fiscal**	**Não Menciona**	**Direção Executiva de Auditoria**	**Direção Executiva de Gestão dos Riscos de Negócio**
Q5.1	Quem é o responsável pela Identificação/Avaliação dos riscos	**Unidades Operacionais**	**Gestão Executiva**	**Departamento de Gestão do Riscos de Negócio**	**Direção Executiva de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Gestão Executiva**
Q5.2	Quem é o responsável pela definição do grau de exposição ao risco	**Gestão Executiva**	**Gestão Executiva**	**Não Menciona**	**Não Menciona**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Não Menciona**
Q6 (a)	Existem Politicas de Gestão dos Riscos de Negócio	**Sim**	**Não Menciona**	**Não Menciona**	**Sim**	**Sim**	**Sim**
Q6 (b)	Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Não Menciona**	**Não Menciona**	**Gestão Executiva**	**Gestão Executiva**	**Gestão Executiva**
Q7	Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio	**Gestão Executiva**	**Não Menciona**	**Não Menciona**	**Direção Executiva de Controlo Interno**	**Direção Executiva de Auditoria**	**Direção Executiva de Auditoria e Riscos**
Q8 (a)	Existe formação na organização quanto à Gestão dos Riscos de Negócio	**Não Menciona**	**Não Menciona**	**Sim**	**Não Menciona**	**Sim**	**Não Menciona**
Q8 (b)	Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio	**Não Menciona**	**Não Menciona**	**Departamento de Auditoria Interna**	**Não Menciona**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Não Menciona**
Q9	Quais as principais categorias de riscos						
	Fatores Externos						
	Económicos	x	x	x	x	x	x
	Meio Ambiente	x		x	x		
	Políticos	x	x	x	x	x	x
	Sociais			x			
	Tecnológicos						
	Fatores Internos						
	Infraestruturas						
	Pessoal				x	x	x
	Processo			x		x	x
	Tecnologia			x		x	

	Empresa:	PORTUGAL TELECOM	BPI	BCP	EDP RENOVAVEIS	IMPRESA
Q1	Existência de atividade de Auditoria Interna	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Q2	Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Q3	A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento	**Não Menciona**	**Não Menciona**	**Não Menciona**	**Não Menciona**	**Não Menciona**
Q4.1	Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Gestão Executiva**	**Departamento de Gestão do Riscos de Negócio**	**Gestão Executiva**	**Gestão Executiva**
Q4.2	Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio	**Departamento de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**
Q4.3	Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**
Q4.4	Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Direção Executiva de Auditoria e Controlo Interno**	**Departamento de Auditoria Interna**	**Não Menciona**	**Não Menciona**
Q4.5	Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Não Menciona**	**Departamento de Controlo Interno**	**Não Menciona**	**Departamento de Gestão do Riscos de Negócio**
Q5.1	Quem é o responsável pela Identificação/Avaliação dos riscos	**Direção Executiva de Auditoria**	**Gestão Executiva**	**Departamento de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Auditoria**
Q5.2	Quem é o responsável pela definição do grau de exposição ao risco	**Não Menciona**	**Não Menciona**	**Gestão Executiva**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**
Q6 (a)	Existem Politicas de Gestão dos Riscos de Negócio	**Sim**	**Sim**	**Sim**	**Sim**	**Sim**
Q6 (b)	Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Não Menciona**	**Gestão Executiva**	**Gestão Executiva**	**Gestão Executiva**
Q7	Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Não Menciona**	**Departamento de Controlo Interno**	**Direção Executiva de Gestão dos Riscos de Negócio**	**Departamento de Gestão do Riscos de Negócio**
Q8 (a)	Existe formação na organização quanto à Gestão dos Riscos de Negócio	**Não Menciona**	**Não Menciona**	**Sim**	**Não Menciona**	**Não Menciona**
Q8 (b)	Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio	**Não Menciona**	**Não Menciona**	**Departamento de Controlo Interno**	**Não Menciona**	**Não Menciona**
Q9	Quais as principais categorias de riscos					
	Fatores Externos					
	Económicos	x	x	x	x	x
	Meio Ambiente	x			x	
	Políticos	x	x		x	x
	Sociais			x		
	Tecnológicos	x				
	Fatores Internos					
	Infraestrutura	x				x
	Pessoal	x				x
	Processo	x	x	x	x	x
	Tecnologia					x

	Empresa:	JERONIMO MARTINS	GALP ENERGIA
Q1	Existência de atividade de Auditoria Interna	**Sim**	**Sim**
Q2	Existência de um gabinete/departamento com funções no âmbito da Gestão de Riscos de Negócio	**Sim**	**Sim**
Q3	A atividade de Auditoria Interna e Gestão dos Riscos de Negócio estão afetas ao mesmo departamento	**Não Menciona**	**Não Menciona**
Q4.1	Quem é o responsável pela implementação do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Gestão dos Riscos de Negócio**
Q4.2	Quem é o responsável pelo funcionamento do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Gestão dos Riscos de Negócio**	**Direção Executiva de Gestão dos Riscos de Negócio**
Q4.3	Quem é o responsável pela monitorização do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Direção Executiva de Auditoria**
Q4.4	Quem é o responsável pela eficiência/eficácia do processo de Gestão dos Riscos de Negócio	**Direção Executiva de Auditoria**	**Conselho Fiscal**
Q4.5	Quem é o responsável pela revisão do processo de Gestão dos Riscos de Negócio	**Não Menciona**	**Direção Executiva de Gestão dos Riscos de Negócio**
Q5.1	Quem é o responsável pela Identificação/Avaliação dos riscos	**Gestão Executiva**	**Gestão Executiva**
Q5.2	Quem é o responsável pela definição do grau de exposição ao risco	**Gestão Executiva**	**Gestão Executiva**
Q6 (a)	Existem Politicas de Gestão dos Riscos de Negócio	**Sim**	**Sim**
Q6 (b)	Quem é o responsável pela emissão de políticas de Gestão dos Riscos de Negócio	**Gestão Executiva**	**Gestão Executiva**
Q7	Quem é o responsável pela emissão de recomendações acerca da Gestão dos Riscos de Negócio	**Direção Executiva de Gestão dos Riscos de Negócio**	**Conselho Fiscal**
Q8 (a)	Existe formação na organização quanto à Gestão dos Riscos de Negócio	**Sim**	**Não Menciona**
Q8 (b)	Quem é o responsável pela formação da organização quanto à Gestão dos Riscos de Negócio	**Órgão de Gestão Executiva**	**Não Menciona**
Q9	Quais as principais categorias de riscos		
	Fatores Externos		
	Económicos	x	**x**
	Meio Ambiente	x	**x**
	Políticos	x	**x**
	Sociais		
	Tecnológicos		
	Fatores Internos		
	Infraestrutura		
	Pessoal	x	x
	Processo	x	x
	Tecnologia	x	