Risco e Gestão de Risco - o caso de uma empresa do setor têxtil

por

Hélder Barbosa Braga

Dissertação de Mestrado em
Contabilidade e Controlo de Gestão

Orientada por
Professor Doutor Rui Couto Viana

Setembro 2013

Nota Biográfica

Hélder Braga nasceu a 3 de Janeiro de 1987, na cidade de Montreux, na Suíça. Em 2011 concluiu a Licenciatura em Economia pela Faculdade de Economia do Porto, ano no qual ingressou no Mestrado em Contabilidade e Controlo de Gestão, na mesma Faculdade.

A nível profissional, iniciou em abril de 2012 a sua atividade profissional numa empresa do setor têxtil, onde exerceu, até agosto de 2013, funções no departamento de Contabilidade e Controlo. Esta experiência profissional, motivou-o a desenvolver a dissertação de mestrado de tema "Risco e Gestão de Risco - o caso de uma empresa do setor têxtil", orientado pelo Professor Doutor Rui Couto Viana.

Desde setembro de 2013, Hélder Braga exerce a função de auditor numa empresa do ramo.

Agradecimentos

Agradeço a todas as pessoas que ao longo da minha vida me ajudaram a atingir os meus sonhos.

Quero deixar um agradecimento especial à minha família pelo apoio que sempre me deu e à Mariana pela paciência, dedicação e sensatez que me transmitiu em todos os momentos.

A todos os professores com que me cruzei, por tudo o que me conseguiram ensinar, em particular ao Professor Doutor Rui Couto Viana por todo o apoio, atenção, disponibilidade e celeridade com que atendeu aos meus pedidos.

A todos os colaboradores e às amizades que fiz na empresa sobre a qual este estudo se debruça, em especial ao departamento de contabilidade pelo acolhimento e momentos que me proporcionaram ao longo da minha passagem pela organização.

"*If I have seen further it is by standing on the shoulders of giants*"
Isaac Newton

Resumo

No atual contexto de incerteza e de mudança a que as organizações estão sujeitas, o papel da gestão de risco assume uma importância crescente. Em Portugal, a utilização de modelos de gestão de risco é ainda residual apesar de as empresas terem consciência da sua relevância.

Neste sentido, o objetivo deste estudo é o de fornecer uma revisão de literatura sobre risco e gestão de risco, as principais metodologias de gestão de risco (COSO-ERM, ISO31000 e FERMA) e ainda discutir o papel da auditoria interna e do controlo interno na gestão de risco. Para além desta revisão teórica, será apresentado um caso de estudo com a aplicação dos princípios de gestão de risco numa empresa.

Este estudo desenvolve-se numa grande empresa do setor têxtil do norte de Portugal e a técnica de recolha de dados é baseada em entrevistas face a face. Nestas entrevistas foram identificados os principais riscos a que a empresa está sujeita, os controlos existentes e os controlos a implementar para reduzir a exposição aos riscos anteriormente identificados.

As principais conclusões deste estudo prendem-se com: a importância de haver uma formalização da informação gerada pela gestão de risco na organização em causa; a atribuição de diferentes classificações quanto ao mesmo risco, por parte dos *risk owners* e da gestão de topo; e a necessidade de se incutir uma cultura de risco na organização, através de uma sessão de debate sobre os conceitos de risco e gestão de risco numa fase de pré-implementação de um modelo de gestão de risco.

Palavras-chave

Risco, Gestão de risco, Auditoria Interna, Controlo Interno

Abstract

Taking into account the changing and uncertain environment that companies face nowadays, risk management is a key area for the success of any organization. In Portugal, the use of risk management models is residual, although, companies are more and more realizing the relevance of this area.

That said, the purpose of this study is to provide a literature review regarding risk and risk management, the main risk management methodologies (COSO-ERM, ISO31000 and FERMA) and to discuss the role of internal audit and internal control within risk management. Furthermore, it will be presented a case study where the author applies the main risk management principles in a company.

This study was developed in a large textile company that it is located in the north of Portugal and the technique to collect the data was based through face-to-face interviews. In these interviews, the author identified the main risks that the company is currently facing, the existent controls that the company relies on and the controls that should be implemented so that the company can reduce its exposure to the risks previously mentioned.

The major conclusions of this study are: it is not enough to identify the risks, the company should also care about the way it reports them; for the same risk we have risk owners giving different risk ratings; and finally, the author identified the need that this company has in developing a risk management culture, through a debate of risk concepts and risk management in a pre-implementation phase of a risk management model.

Keywords

Risk, Risk Management, Internal Audit, Internal Control

Índice

Índice de Figuras

I. Introdução

Nos finais da década de noventa e início do século XXI, uma série de fraudes financeiras[1] que ocorreram nos Estados Unidos da América e na Europa puseram em causa a credibilidade dos dados apresentados pelas empresas, o que afastou investidores e abalou a confiança que estes e o público em geral tinham nos mercados e nos instrumentos que os regulavam.

Estas fraudes tiveram origem na manipulação das demonstrações financeiras com o objetivo de ir ao encontro das expectativas do mercado, empolando resultados e/ou escondendo prejuízos.

Neste contexto, surgiu a *Sarbanes-Oxlet Act* (SOX) em 2002, conhecida publicamente como a *Public Company Accounting Reform and Investor Protection Act*, que impôs novas obrigações a todas as empresas norte americanas cotadas, no sentido de recuperar a confiança dos investidores e proteger os seus investimentos. Entre as diversas obrigações a cumprir, destacam-se as exigências da secção 404 que estipula a criação e manutenção de controlos internos eficazes e adequados. Para além destas exigências ao nível do controlo interno e para evitar que ninguém fosse responsabilizado pelas ações fraudulentas que viessem a ocorrer nas organizações, a secção 302 responsabiliza os administradores executivos (em especial o *Chief Executive Officer* e o *Chief Financial Officer*) pela exatidão e fidelidade das demonstrações financeiras (Anand, 2007).

No sentido de facilitar o cumprimento da SOX, a *Securities and Exchange Commission* (SEC) aconselhou a utilização de um *framework* que permita avaliar os controlos internos existentes, com o objetivo de gerir os diversos riscos a que a empresa esteja exposta (Tarantino, 2006).

Existem diversos modelos de controlo e gestão de risco, no entanto, o *framework* mais utilizado pelas empresas norte americanas e o que é expressamente citado na versão final da SOX é o modelo apresentado em 2004 pelo *Committee of Sponsoring Organizations* (COSO), o ERM - *Entreprise Risk Management* (Cenker e Nagy, 2004). Este modelo permite às empresas identificar os riscos, definir os controlos internos necessários, em função do perfil de risco que pretendem adotar, e garantir um efetivo controlo sobre os procedimentos e bens da empresa (Tarantino, 2006).

[1] As maiores fraudes financeiras relacionaram-se com as empresas americanas *WorldCom, Enron,* e *Tyco International* e com o caso europeu da *Parmalat.*

Em 2009, a *International Organization for Standardization* (ISO) publicou a ISO31000, que surgiu como um *framework* alternativo ao ERM, propondo uma "standardização" do modelo de gestão de risco, isto é, um modelo com uma linguagem e conceitos simples e bem definidos, que o tornam flexível e aplicável a todos os modelos de negócio.

Em Portugal, a CMVM (2005) recomendou às sociedades a criação de um sistema interno de controlo, para a deteção eficaz de riscos ligados à atividade da empresa, em salvaguarda do seu património e em benefício da transparência do seu governo societário, implementando equipas orgânicas dedicadas à auditoria interna e/ou gestão de riscos para apoiar a administração na deteção de riscos relevantes (financeiros, ambientais, jurídicos, de entre outros). O acolhimento desta recomendação promoveria uma maior qualidade da informação divulgada ao mercado e ajudaria a tornar mais transparente o governo societário.

No entanto, não existem muitas empresas a aplicar metodologias de gestão de risco em Portugal, nem é muito frequente encontrar-se o tema da gestão de risco, na perspetiva deste estudo, como parte integrante dos programas letivos nas universidades.

Assim sendo, surge a necessidade de realizar um estudo e aprofundar conhecimentos nesta área, devido à crescente relevância do tema no atual contexto económico e social.

Como tal, no presente estudo pretende-se realizar um estudo sobre as principais metodologias de gestão de risco e aplicar os princípios destas metodologias a uma empresa portuguesa do setor têxtil. É objetivo deste trabalho apurar os principais riscos que a organização em estudo enfrenta e, através da gestão de risco, determinar a melhor resposta a dar a estes mesmos riscos.

Para tal, pretende-se desenvolver um trabalho de pesquisa da literatura relevante sobre o tema e, posteriormente, implementar uma proposta de um modelo de gestão de risco na organização afeta ao estudo.

Assim, este trabalho contempla as seguintes divisões lógicas: nos capítulos 2 e 3, é realizado um estudo acerca do risco e da gestão de risco, das diferentes metodologias de gestão de risco e das diferentes respostas a dar ao risco; no quarto capítulo, estão detalhadas as questões de investigação, a metodologia e as técnicas de recolha de dados que levaram à realização deste estudo; o capítulo 5 descreve a aplicação prática de uma metodologia de gestão de risco na empresa selecionada para o estudo; por último, no

sexto capítulo, são apresentadas as conclusões do estudo efetuado, bem como a proposta de questões de investigação futura.

II. Risco e Gestão de Risco

No presente capítulo apresenta-se uma revisão de literatura aos temas do risco e gestão de risco. Assim sendo, primeiramente são abordadas algumas das definições existentes para o conceito de risco bem como uma categorização das fontes de incerteza passíveis de influenciar o risco nas organizações. Seguidamente, aborda-se o conceito de gestão do risco, bem como a sua evolução ao longo dos tempos. Por último, neste capítulo, apresentam-se ainda os vários modelos de gestão de risco existentes na literatura, bem como o tipo de respostas a dar aos diversos riscos a que uma organização possa estar sujeita.

2.1. Risco

Segundo Bernstein (1996), a palavra risco deriva da palavra italiana *risicare*, que significa arriscar ou ousar, devendo ser entendido como uma escolha e não como uma fatalidade do destino. Neste sentido, Moore (1983) defende que o risco engloba uma possibilidade de ganho e uma possibilidade de perda. Isto é, risco é também sinónimo de explorar uma oportunidade, arriscar-se a obter ganhos, no entanto, usualmente a palavra risco tem uma conotação negativa, sendo associada à possibilidade de perda ou dano.

Segundo o *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards*, da *International Organization for Standardization* (ISO), risco é definido como o efeito da incerteza nos objetivos. Segundo as notas do mesmo guia, "efeito" é o desvio face à expectativa, podendo este ser positivo ou negativo; "incerteza" é um estado, ainda que parcial, de deficiente informação relativa a um evento, às suas consequências ou à sua ocorrência; os "objetivos" podem ser de diversa ordem (financeiros, de saúde e segurança, ambientais) e podem aplicar-se a diferentes níveis (estratégicos, comuns à organização, de um projeto, produto ou processo). Ainda relativamente ao risco, a ISO refere que este é muitas vezes caracterizado por se referir aos potenciais eventos, às suas consequências, ou à combinação de ambos.

Para a *Federation of European Risk Management Associations* (FERMA) risco é definido como a combinação da probabilidade de um acontecimento e das suas consequências. Também para Moore (1983) risco é composto por dois componentes: o resultado e a probabilidade desse resultado.

Deste modo, o risco pode ser expresso através das consequências de um evento e da probabilidade da sua ocorrência (Hodges, 2000). Para uma melhor perceção do risco, o COSO (2012b) aconselha a sua apresentação através de mapas de risco, nos quais o risco é definido como uma função da probabilidade e do impacto, conforme o exemplo da figura 1).

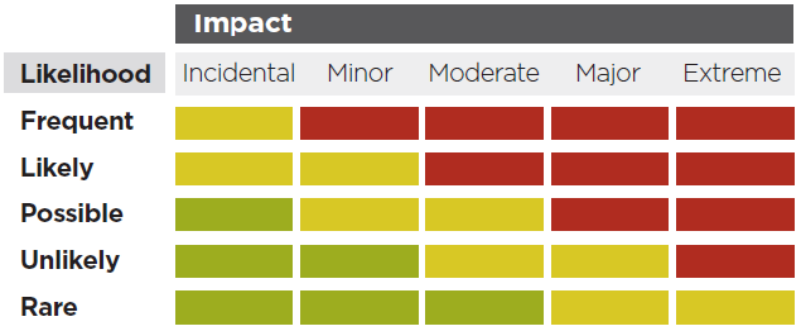

Figura 1 - Mapa de risco
Fonte: Adaptado de COSO (2012b)

2.2. Categorização das Fontes de Incerteza

Miller (1992) defende que a incerteza associada às variáveis do ambiente externo e interno das organizações reduz a previsibilidade da sua performance, isto é, aumenta o risco. Deste modo, este autor identifica vários tipos de incertezas que podem influenciar os resultados das organizações:

- Incertezas Gerais
- Incertezas da Indústria
- Incertezas da Organização

Cada um dos tipos de incertezas identificados por Miller (1992) é depois desagregado em vários sub-tipos de incertezas abrangendo todas as possíveis variáveis passíveis de influenciar a *performance* das empresas.

O primeiro tipo de incerteza (Incertezas Gerais) refere-se a fatores que são transversais às empresas que operam num determinado contexto. Estas incertezas incluem a incerteza política, a incerteza das políticas governamentais, a incerteza macroeconómica, a incerteza social e as incertezas naturais.

Por Incerteza Política entendem-se as ameaças e oportunidades associadas a uma potencial ou efetiva mudança no sistema político de correntes de uma revolução, um golpe de estado ou a substituição de atores políticos, por exemplo

A Incerteza das Políticas Governamentais aumenta o risco na medida em que modificações na política fiscal ou aduaneira ou a criação de barreiras à expatriação dos lucros alteram de modo significativo o contexto de atuação das empresas.

Relativamente à Incerteza Macroeconómica, esta ocorre devido à flutuação dos níveis de atividade económica e dos preços. Exemplos de incerteza macroeconómica são a flutuação das taxas de juro e das taxas de câmbio ou o nível de inflação.

No que se refere às Incertezas Sociais, estas incertezas são um fator de risco na medida em que os valores, crenças ou atitudes da população podem diferir das atuais políticas do governo ou das práticas correntes nos negócios. Um exemplo deste tipo de incertezas é o boicote a produtos cujo método ou local de produção os consumidores não aprovam.

As Incertezas Naturais referem-se a fenómenos naturais que afetam a capacidade produtiva das organizações numa determinada região. Exemplos destes fenómenos são a ocorrência de cheias e sismos. As condições climatéricas também afetam todos as organizações, especialmente aquelas ligadas ao setor agrícola.

O segundo grande grupo de incertezas identificadas por Miller (1992) é o das Incertezas da Indústria que estão ligadas ao contexto de mercado no qual as organizações se inserem, afetando um determinado setor de negócio ou indústria. Miller (1992) identificou três tipos de incertezas: Incertezas no Mercado dos Inputs, Incertezas no Mercado dos Produtos e Incertezas Competitivas.

As Incertezas no Mercado dos Inputs são as incertezas que a organização enfrenta com a aquisição de matérias-primas, serviços e outros bens necessários ao processo produtivo. A incerteza é maior quanto mais reduzido for o número de fornecedores a operar no mercado. A flutuação dos níveis de produção de um fornecedor chave da indústria ou um aumento da procura de uma determinada matéria-prima são exemplos de incertezas no mercado dos inputs que afetam as organizações.

As Incertezas ao nível do Mercado dos Produtos estão relacionadas com alterações na procura dos bens produzidos por uma certa indústria. Exemplos deste tipo de incertezas são as mudanças nos gostos dos clientes e o surgimento de produtos substitutos.

Relativamente às Incertezas Competitivas, estas derivam do nível de concorrência existente na indústria onde as organizações operam. Esta incerteza é tanto maior quanto maior for o nível de concorrência entre as empresas e a facilidade de entrar no mercado. Ainda dentro deste tipo de incertezas podem ser encontradas as incertezas decorrentes da evolução tecnológica nos produtos e nos processos de produção.

O terceiro tipo de incertezas que Miller (1992) refere é as Incertezas da Organização, que estão relacionadas com fatores específicos da organização em causa, nomeadamente incertezas operacionais, incertezas de fiabilidade, incerteza na Investigação e Desenvolvimento (I&D), incerteza no crédito e incerteza comportamental.

Ao nível das incertezas operacionais, estas podem ser decompostas em incertezas ao nível laboral, decorrentes de acidentes de trabalho, greves ou a saída de colaboradores chave da empresa; incertezas ao nível dos fornecimentos, com uma redução da quantidade ou qualidade dos inputs necessárias à produção; e incertezas na produção, com paragens não programadas na produção ou avarias.

As Incertezas de Fiabilidade resultam das consequências negativas não previstas na produção ou consumo dos bens produzidos pela organização. Estes efeitos não previstos podem dar lugar a litígios com vista à responsabilização da organização.

A incerteza na I&D resulta da própria natureza da atividade, uma vez que não existe uma correspondência perfeita entre os gastos em I&D e a introdução de novos produtos no mercado.

A Incerteza no Crédito reflete a incerteza inerente à concessão de crédito ao cliente. A falência de um cliente ou esforços de cobrança demasiado custosos para a organização podem trazer consequências negativas na sua performance.

A Incerteza Comportamental refere-se ao não alinhamento dos valores da organização com os valores dos colaboradores, que pode levar a comportamentos não desejados, pondo em causa o desempenho da organização.

Apresenta-se de seguida um quadro resumo das incertezas identificadas por Miller (1992):

Incertezas Gerais	Incertezas Políticas
	Incertezas das Políticas Governamentais
	Incertezas Macroeconómicas
	Incertezas Sociais
	Incertezas Naturais
Incertezas da Indústria	Incertezas no Mercado dos Inputs
	Incertezas no Mercado dos Produtos
	Incertezas Competitivas
Incertezas da Organização	Incertezas Operacionais
	Incertezas de Fiabilidade
	Incertezas na Investigação e Desenvolvimento
	Incertezas no Crédito
	Incertezas Comportamentais

Figura 2 - Tipos de incerteza
Fonte: Miller (1992)

Os dois primeiros tipos de incertezas identificadas por Miller (1992) podem, de certa forma, assemelhar-se a uma combinação das análises estratégicas PEST[2] e das 5 Forças de Porter[3], que foram largamente divulgadas e são ainda muito utilizadas na avaliação estratégica das empresas, ao passo que o último tipo de incertezas está ligado a questões do foro interno da organização.

2.3. Gestão de Risco

Existem diversas definições para o conceito de Gestão de risco. O COSO (2004) apresenta a seguinte proposta:

> "*Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*", em COSO (2004), pp.2.

Segundo o COSO (2004) esta definição é propositadamente ampla, de modo a conseguir abarcar todos os modelos de negócio, sectores e indústrias mantendo, no entanto, os conceitos chave da gestão de risco.

Quanto à *European Foundation for Quality Management* (EFQM, 2005), esta define gestão de risco de uma forma mais simples e direta: gestão de risco é um processo sistemático e transversal à organização que permite identificar, gerir e monitorizar riscos de forma que a informação gerada possa ser utilizada para proteger e criar valor.

Segundo o *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards* desenvolvido pela ISO, gestão de risco é definida como "*coordinated activities to direct and control an organization with regard to risk*" em ISO Guide 73 (2009), pp.2.

A gestão de risco foi evoluindo ao longo do tempo, no sentido de ir dando resposta aos novos desafios que as organizações enfrentavam. A gestão de risco surgiu como uma atividade que permitia lidar os riscos através da transferência dos mesmos, recorrendo a seguros, *headging* ou outros instrumentos. Numa fase posterior, a gestão

[2] Modelo com origem nos anos sessenta que propõe uma análise estratégica de uma organização em quatro fatores: Político, Económico, Social e Tecnológico.

[3] Modelo estratégico que se destina a analisar a competitividade das empresas considerando cinco forças competitivas: Concorrência entre empresas, Poder negocial dos clientes, Poder negocial dos fornecedores, Ameaça de produtos Substitutos e Entrada no mercado de potenciais concorrentes.

de risco evoluiu para uma gestão de risco avançada/integrada: os riscos passaram a ser tratados, prevenindo a sua ocorrência e/ou diminuindo o seu impacto (desenvolvendo-se, por exemplo, programas de segurança no trabalho, áreas de análise de reclamações). Na atual fase, a função da gestão de risco lida com os riscos numa perspectiva mais ampla, profunda e proativa, incluindo riscos estratégicos, operacionais, financeiros entre outros, numa perspectiva de riscos inter-relacionados. Esta abordagem foca-se na tomada de decisões informadas acerca das incertezas que afetam o futuro da organização (IIA & RIMS, 2012).

Deste modo, segundo a IIA & RIMS (2012), a gestão de risco passou de uma gestão de risco defensiva, isto é, de uma análise custo/benefício, para uma gestão de risco ofensiva, baseada na dicotomia risco/recompensa.

Evolução da Gestão de Risco	
Tradicional	Questão: Quais são os riscos contratuais e seguráveis que enfrentamos, e o que estamos a fazer para os mitigar?
	Atividade: Identificação dos riscos pelo impacto/perigo
	Objetivo: Tratamento de riscos encarado como uma despesa; riscos geridos por seguros e/ou *hedging*
Integrado	Questão: Quais são as ameaças chave que enfrentamos para atingir os objetivos do negócio e qual deve ser a nossa resposta?
	Atividade: Identificação dos riscos, análise com a coordenação de outras funções de gestão de risco
	Objetivo: Estabelecer um processo para gerir proativamente as ameaças operacionais para o negócio
***Enterprise Risk Management* (ERM)**	Questão: Como melhorar as decisões relativamente às incertezas que afetam o nosso futuro?
	Atividade: Estabelecer um *framework* abrangente para gerir os riscos mais significativos da organização
	Objetivo: Aumentar o alcance dos objetivos estratégicos e a supervisão de risco

Figura 3 - Evolução da gestão de risco
Fonte: IIA & RIMS (2012)

De uma forma geral pode-se concluir que a gestão de risco permite à gestão, através de uma abordagem sistemática, lidar com o risco e a incerteza (Roger Williams *el al.*, 2006) para que esta tome as melhores decisões na prossecução dos objetivos da organização (Kallman e Maric, 2004).

Dos vários *frameworks* existentes ao nível da gestão de risco, serão apresentados de seguida alguns dos modelos com maior divulgação e aplicação por parte das organizações.

2.4. Modelos de Gestão de Risco

i. Modelo COSO - ERM

O *Committee of Sponsoring Organizations* (COSO) foi fundado em 1985 por cinco grandes associações sedeadas nos Estados Unidos da América: a *American Accounting Association* (AAA), o *Americam Institute of Certified Public Accountants* (AIPCA), a *Financial Executives International* (FEI), o *Institute of Internal Auditors* (IIA) e *o Institute of Management Accountants* (IMA). A sua missão é a de desenvolver *frameworks* e fornecer orientação sobre temas como gestão de risco empresarial, controlo interno e a dissuasão da fraude, de modo a melhorar o desempenho e reduzir a fraude nas organizações.

O modelo apresentado em 2004 pelo COSO, o ERM - *Entreprise Risk Management*¸ é um modelo amplamente divulgado e preenche os requisitos exigidos pela *Securities and Exchange Commission* (SEC) no cumprimento da *Sarbanes-Oxlet Act* (SOX).

Segundo o COSO, a adoção deste modelo de gestão de risco permite:

- Alinhar o apetite pelo risco com a estratégia da organização - a análise de alternativas estratégicas, o estabelecimento de objetivos e o desenvolvimento de mecanismos de gestão de risco permitem determinar o perfil de risco a adotar;
- Melhorar as decisões de resposta ao risco - a gestão de risco capacita as organizações para darem respostas alternativas ao risco: evitar, reduzir, partilhar e aceitar;
- Reduzir perdas operacionais - a identificação de eventos potenciais e o estabelecimento de respostas prepara a organização, reduzindo situações inesperadas e perdas;
- Identificar e gerir riscos múltiplos e transversais à organização - a gestão de risco permite à organização responder eficientemente e de forma integrada a múltiplos riscos;
- Aproveitar oportunidades - a consideração de potenciais eventos permite à gestão identificar e aproveitar oportunidades;
- Melhorar a utilização do capital - uma maior e melhor informação sobre os riscos possibilita à gestão avaliar as necessidades de capital e melhorar a sua alocação.

A figura 4 representa o cubo da estrutura do ERM, cujas faces visíveis correspondem às três dimensões abordadas no modelo: categorias de objetivos, componentes do processo de gestão de risco e níveis de atuação.

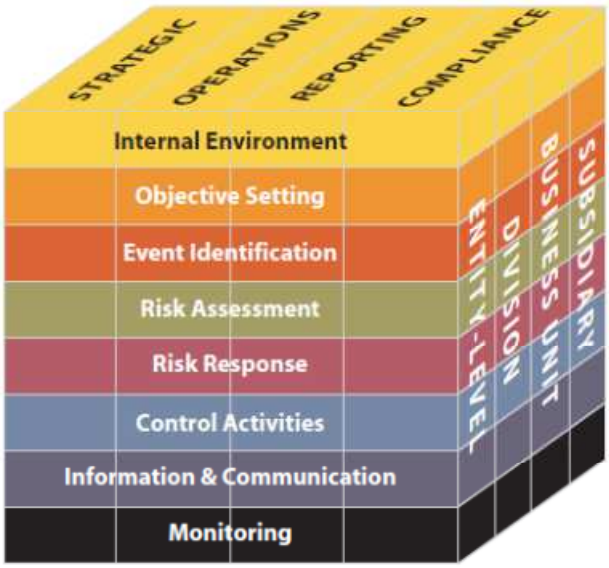

Figura 4 - Cubo COSO - ERM
Fonte: COSO (2004)

A aplicação de uma estratégia por parte da gestão implica a definição de objetivos para os diferentes níveis da organização, de acordo com a missão e com os valores desta. Este modelo de gestão de risco propõe a separação destes objetivos em quatro categorias:

I. *Strategic* (Estratégicos) - de mais elevado nível, alinhados com a missão;
II. *Operations* (Operacionais) - de utilização eficiente e efetiva dos recursos;
III. *Reporting* (de Reporte) - de fiabilidade dos relatórios;
IV. *Compliance* (de Conformidade) - de conformidade com leis e regulação.

A categorização permite uma maior facilidade de leitura quanto à importância relativa de cada objetivo, possibilitando à gestão focalizar e separar diferentes aspetos da gestão de risco.

Relativamente ao processo de gestão de risco, o modelo ERM considera as seguintes oito componentes inter-relacionadas:

1) *Internal Environment* (Ambiente Interno) - nesta fase é feita a avaliação do ambiente onde a organização opera, quais os seus valores éticos, a filosofia de gestão, a cultura empresarial e a atitude face ao risco;
2) *Objective Setting* (Estabelecimento de Objetivos) - a fixação clara de objetivos por parte da gestão, alinhados com a missão e consistentes com o perfil de risco da organização, são um pré-requisito para a aplicação do modelo ERM;
3) *Event Identification* (Identificação de Eventos) - eventos internos e externos à organização que afetem a concretização dos objetivos delineados devem ser identificados e classificados em ameaças e oportunidades. Os eventos classificados como oportunidades devem ser

alvo de uma avaliação por parte da gestão para uma possível redefinição da estratégia e dos objetivos a alcançar;

4) *Risk Assessment* (Avaliação do Risco) - os riscos são analisados segundo a sua probabilidade de ocorrência e possível impacto, para determinar o tipo de tratamento a efetuar;
5) *Risk Response* (Resposta ao Risco) - é definido o tipo de resposta a dar ao risco para que esta se enquadre no perfil de risco definido para a organização;
6) *Control Activities* (Atividades de Controlo) - são implementados procedimentos para assegurar que as respostas ao risco são aplicadas;
7) *Information and Communication* (Informação e Comunicação) - a informação é transmitida nos termos previamente determinados e de forma tempestiva de modo a permitir o cumprimento das obrigações por parte de todos os colaboradores;
8) *Monitoring* (Monitorização) - avaliações independentes e/ou a atividade contínua de gestão permitirão monitorizar a gestão de risco e, se necessário, efetuar os devidos ajustamentos.

A gestão de risco não deve ser percebida como um conjunto de fases a serem seguidas de modo sequencial, devendo ser entendida como um processo multidirecional e iterativo, em que cada componente afeta todos as outras. Tendo em vista o topo do cubo, isto é, os objetivos estratégicos, operacionais, de reporte e de conformidade, as oito componentes devem ser implementadas em todos os níveis de atuação da organização, ao nível da entidade, divisão, unidade de negócio e subsidiárias.

O COSO (2004) refere, ainda, que em pequenas entidades, o modelo poderá ser menos formal e menos estruturado e, mesmo assim, haver uma efetiva gestão de risco, desde que os componentes estejam presentes e funcionem devidamente.

Relativamente às limitações, o COSO (2004) alerta para o facto do modelo ERM se basear: em julgamentos e asserções pessoais, que poderão estar incorretos; na relação custo benefício na implementação de controlos e definição de respostas a eventuais eventos; e nos controlos, que poderão ser ultrapassados pelo conluio de dois ou mais colaboradores. Para além disso, refere também a possibilidade de a gestão simplesmente ignorar as políticas de risco estabelecidas.

ii. ISO31000

A ISO (*International Organizations for Standardization*) foi fundada em 1947 e tem por objetivo a publicação/definição de *standards* internacionais. Estes *standards* abrangem diversos aspetos tecnológicos e de negócio que tornam a indústria mais eficiente e eficaz. A ISO já publicou mais de 19000 *standards* internacionais nas mais diversas áreas: segurança alimentar, saúde, linguagem de programação, agricultura, gestão de qualidade, entre outros.

A publicação da ISO31000 teve como grande mais-valia a definição de conceitos que ajudam a resolver certos problemas que surgem nas organizações. Por exemplo, o processo de aplicação de modelos de gestão de risco está sujeito às diferentes interpretações que os colaboradores das empresas atribuem a conceitos como risco ou nível de risco. Deste modo, e para minimizar a subjetividade ligada aos processos de aplicação de um modelo de gestão de risco, a ISO desenvolveu:

- um vocabulário para a gestão de risco (ISO *Guide 73:2009*);
- critérios de *performance*/avaliação dos modelos de gestão;
- um processo abrangente de identificação, análise, avaliação e de tratamento de riscos;
- um guia de implementação e integração de um sistema de gestão de risco num sistema de gestão.

A implementação de sistemas de gestão de risco pressupõe que todos os intervenientes partilhem a mesma definição/noção dos conceitos utilizados. Desta forma, e de modo a facilitar essa mesma implementação, a ISO elaborou um conjunto de definições (ISO *Guide 73:2009*) para o vocabulário utilizado na gestão de risco (Grant Purd, 2010).

Para que a gestão de risco seja eficaz e efetiva, a organização deve assegurar que a gestão de risco esteja de acordo com os seguintes princípios:

- Proteja e crie valor - a gestão de risco deve ajudar a organização a atingir os seus objetivos;
- Integre todos os processos da organização - a gestão de risco não pode ser uma atividade isolada dos outros processos de uma organização;
- Participe no processo de decisão;
- Aborde explicitamente a incerteza - a gestão de risco deve mensurar o grau de incerteza, a natureza dessa incerteza e a gestão da mesma;

- Seja sistemática, estruturada e oportuna - o que permitirá obter resultados fiáveis, comparáveis e consistentes;
- Se baseie na melhor informação disponível - eventuais limitações das informações recolhidas devem ser tidas em conta;
- Seja adaptada - a gestão de risco deve estar alinhada com o contexto interno e externo da organização e com o seu perfil de risco;
- Tenha em atenção fatores culturais e humanos - é fundamental conhecer as capacidades, perceções e interesses de agentes internos e externos que possam facilitar ou comprometer os objetivos organizacionais;
- Seja transparente e inclusiva - a gestão de risco deve ter em conta todos os *stakeholders* da empresa assim como a sua perspetiva acerca dos diversos riscos a que a empresa está sujeita;
- Responda à mudança - o modelo de gestão de risco deve ser dinâmico, de forma a responder a eventos internos e externos, a novas informações e a mudanças no perfil de risco da empresa;
- Facilite a melhoria contínua.

O modelo de gestão de risco apresentado pela ISO31000 assenta num *framework* constituído por cinco componentes essenciais para uma gestão de risco eficiente e efetiva: *Mandate and commitment, Design of framework for managing risk, Implementing risk management, Monitoring and review of the framework* e *Continual improvement of the framework*. A norma não tem por objetivo prescrever este *framework* a todas as organizações que adotem a ISO31000. Ao invés, propõe que as diferentes componentes sejam adaptadas às necessidades específicas de cada negócio.

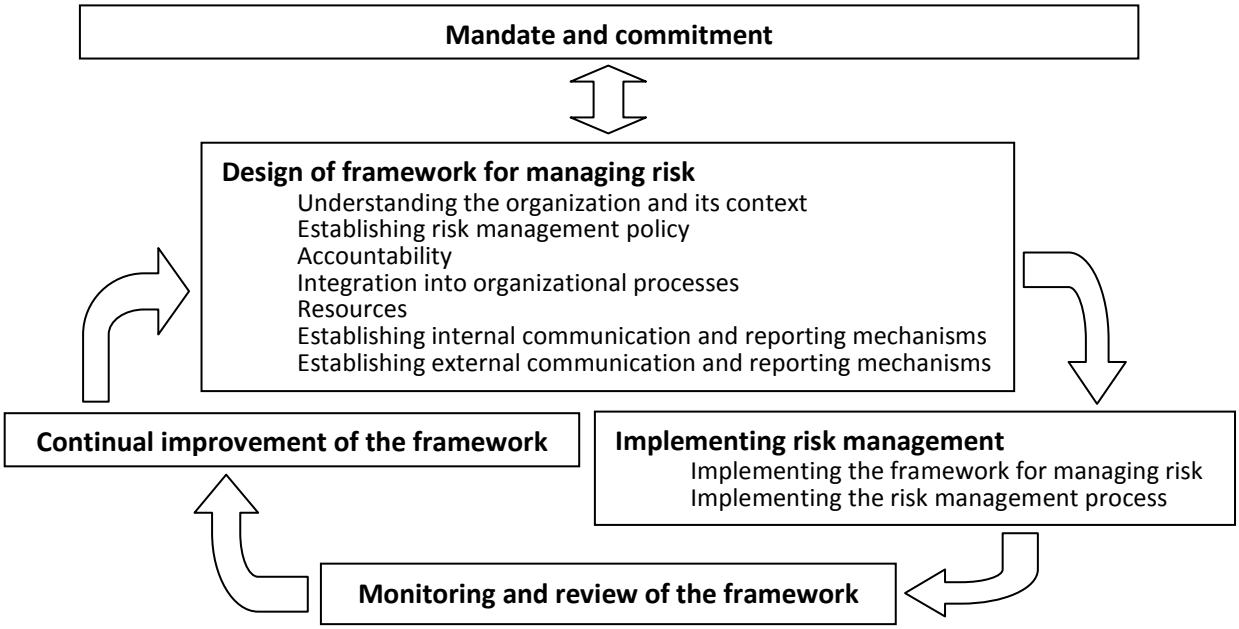

Figura 5 - *Framework* da gestão de risco
Fonte: ISO31000

Na figura 5 é possível identificar estas mesmas componentes e a relação iterativa que estabelecem entre si.

A aplicação deste modelo de gestão de risco exige um forte compromisso por parte da gestão de uma organização ao nível da definição de uma estratégia e de um planeamento cuidado, no sentido de assegurar o empenho dos colaboradores a todos os níveis. O *framework* deve ser desenhado tendo em conta o negócio da organização e a sua envolvente, estabelecendo uma política de gestão de risco adequada ao seu perfil de risco. Devem ser identificados os *Risk Owners* e atribuidas responsabilidades pela gestão dos riscos a que a organização está exposta. Esta gestão deve estar dotada de recursos adequados e integrar os processos da organização. O estabelecimento de mecanismos de comunicação interna, externa e de *report* permitirá aumentar o nível de envolvimento dos colaboradores assim como dos *stakeholders* externos à organização.

A ISO31000 sugere ainda a desagregação do anterior componente *Implementing risk management*. A implementação de um processo de gestão de risco deve respeitar as seguintes atividades apresentadas no esquema da figura 6.

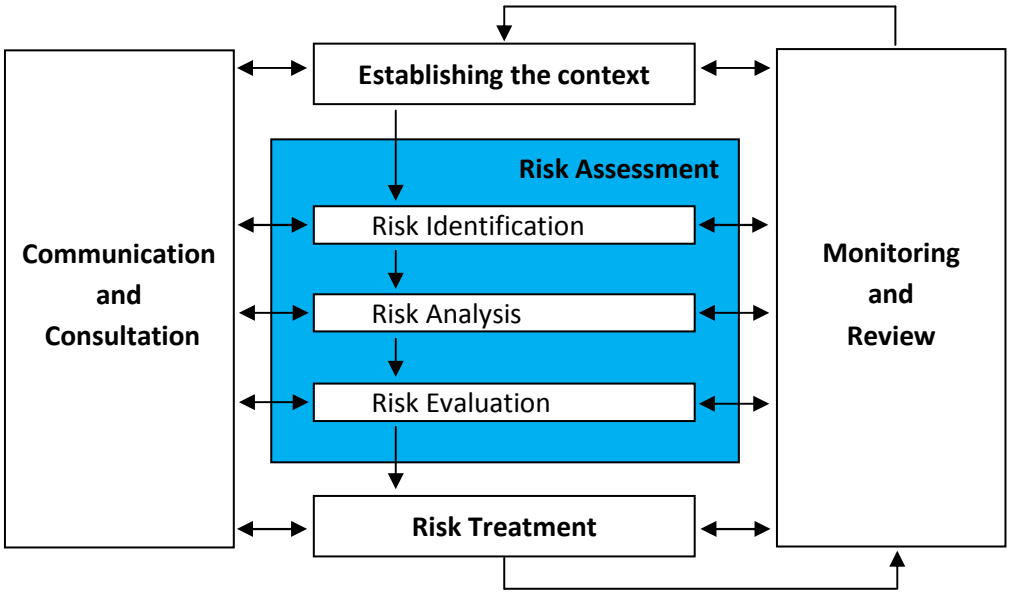

Figura 6 - Processo da gestão de risco
Fonte: ISO31000

Segundo a ISO31000, o processo de gestão de risco é composto por cinco atividades: *Communication and Consultation*, *Establishing the context*, *Risk Assessment*, *Risk Treatment* e *Monitoring and Review*.

A atividade de *Communication and Consultation* refere-se à necessidade de haver um contacto e uma discussão permanentes com os *stakeholders*, para que as

diferentes perspetivas do risco sejam levadas em conta ao longo do processo de gestão de risco contribuindo, desta forma, para uma melhor tomada de decisão.

Establishing the context trata da definição dos objetivos e estratégia(s) a aplicar na gestão do risco e da compreensão do contexto interno e externo da organização. Nesta fase do processo de gestão de risco são, também, determinados os critérios de avaliação dos riscos, que deverão estar de acordo com a política de risco da organização.

A fase de *Risk Assessment* decorre em três sub-fases: *Risk Identification*, *Risk Analysis* e *Risk Evaluation*. A primeira sub-fase consiste na identificação do risco, determinando a sua origem, as suas causas e as potenciais consequências da sua ocorrência nos objetivos da organização. Em *Risk Analysis* pretende-se compreender um determinado risco e os fatores que determinam a extensão das consequências e a probabilidade de ocorrência desse mesmo risco. Por último, será realizada uma avaliação (*Risk Evaluation*) para determinar os riscos que necessitam de tratamento, e destes, definir os que são prioritários para a aplicação imediata de um plano de ação.

Risk Treatment refere-se à implementação ou modificação de controlos que permitam uma gestão eficaz do risco em causa, tendo em conta o perfil de risco definido pela organização e as exigências legais, sociais, ambientais e outras existentes.

Relativamente à atividade de *Monitoring and Review*, esta é transversal ao processo de gestão de risco. Esta fase pressupõe a reavaliação dos riscos e a tomada de ações à medida que novos riscos surgem e que os riscos, objetivos e as condições existentes se alteram.

iii. Modelo FERMA

A *Federation of European Risk Management Associations* (FERMA) foi fundada em 1974 com o objetivo de coordenar as ações das associações nacionais de profissionais de gestão de risco a nível europeu, sendo considerada a principal instituição europeia dedicada às questões da gestão de risco.

O modelo proposto pela FERMA procurou utilizar a terminologia utilizada no *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards* da *International Organization for Standardization* (ISO).

Segundo a FERMA (2003), a gestão de risco e o processo de gestão de riscos protege e acrescenta valor à organização, permitindo ainda:

- Criar uma estrutura que desenvolva a atividade futura e a desenvolva de forma consistente e controlada;
- Melhorar a tomada de decisão, o planeamento e a definição de prioridades interpretando a atividade de negócio, a volatilidade, as oportunidades e as ameaças;
- Utilizar o capital e os recursos mais eficientemente;
- Reduzir a volatilidade de áreas não essenciais do negócio;
- Proteger os ativos e melhorar a imagens da entidade;
- Desenvolver e ampliar o conhecimento dos colaboradores e da organização;
- Otimizar a eficiência operacional.

Partindo dos objetivos definidos para a organização e tendo em conta a sua estratégia, devem ser estudados os potenciais riscos e os fatores internos e externos que possam amplificar ou minimizar esses riscos. Esta avaliação do risco é composta por dois componentes: a análise do risco e a comparação do risco.

Para uma correta análise do risco, o modelo FERMA exige que seja identificada a exposição da organização à incerteza, o que exige um conhecimento detalhado do modelo de negócio assim como da envolvente jurídica, social, política, económica e cultural. Uma vez identificadas as atividades mais relevantes e os seus riscos, estas devem ser classificadas em cinco naturezas:

- Estratégicas - relacionadas com objetivos estratégicos da organização de longo prazo;
- Operacionais - relativas a questões quotidianas com o propósito de assegurar o cumprimento dos objetivos estratégicos;
- Financeiras - referentes à gestão e controlo dos meios financeiros;
- Gestão do Conhecimento - que se relacionam com o conhecimento gerado internamente, a sua utilização não autorizada por terceiros ou com a manutenção de colaboradores chave;
- Conformidade - que se referem ao cumprimento, por exemplo, de normas laborais, ambientais, de saúde e de proteção do consumidor.

Relativamente à descrição do risco, o modelo FERMA propõe a utilização de suportes padronizados, por exemplo tabelas, que permitam identificar riscos chave e

determinar prioridades dos esforços de tratamento. Para além da descrição do risco é, também, importante realizar uma estimativa dos riscos em termos qualitativos ou quantitativos. Após a análise dos riscos será necessário proceder a uma comparação destes com o nível de risco determinado pela organização como nível ideal.

A fase de Reporte do Risco - Ameaças e Oportunidades refere-se à categorização de risco nos seus aspetos positivos, isto é, aqueles que potenciam a concretização dos objetivos (oportunidades); e nos seus aspetos negativos, ou seja, aqueles que diminuem a probabilidade de êxito da organização (ameaças).

Após uma análise dos riscos, e contrapondo com o nível de risco que a entidade entende ser o ótimo, haverá uma decisão quanto ao tratamento a dar ao risco em causa.

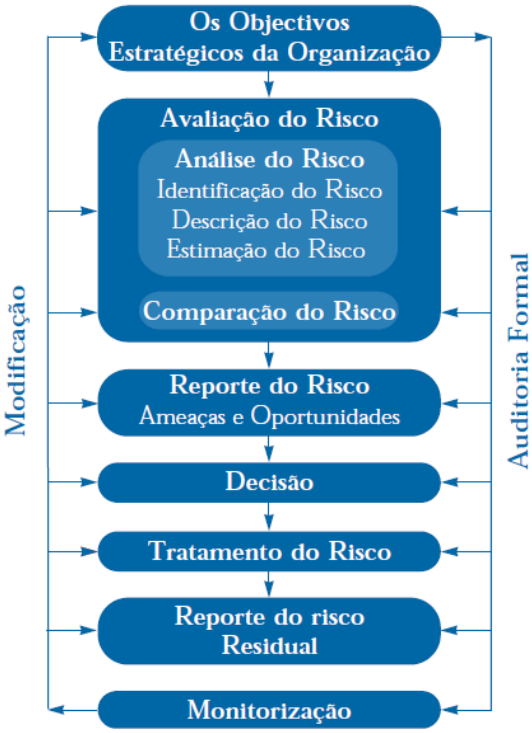

Figura 7 - Processo de gestão de risco
Fonte: FERMA (2003)

O tratamento do risco é a implementação de medidas que permitam modificar o risco, passando a haver um maior controlo ou diminuição do mesmo. Poderá também significar uma transferência ou partilha do risco, por exemplo, com a celebração de um seguro. Um aspeto a ter em conta será uma análise da relação custo/benefício: custo da implementação dos controlos *versus* o benefício obtido na mitigação do risco.

Ao nível da comunicação e do reporte do risco residual, existem duas vertentes com diferentes necessidades de informação: interna e externa. A comunicação interna deve focar-se em dar a conhecer as responsabilidades de cada um, garantir o *feedback* sobre novos riscos ou falhas e colocar à disposição, atempadamente, a informação necessária que permita reações adequadas por parte do conselho de administração, das unidades de negócio e dos colaboradores. A comunicação externa deve focar-se em organizar a informação e transmiti-la aos agentes externos, aos quais a entidade tem de apresentar provas de uma gestão eficaz.

Por último, a fase de Monitorização relaciona-se com a aferição do grau de cumprimento das políticas e dos procedimentos de controlo implementados pelo modelo

de gestão de risco. Eventuais desvios devem ser corrigidos e revisões regulares do sistema de controlo devem ser realizadas no sentido de garantir o seu correto funcionamento.

2.5. Respostas ao Risco

Após se terem apresentado os conceitos de risco, gestão de risco e principais modelos de gestão de risco existentes, importa agora referir a importância do tipo de respostas a dar aos riscos a que uma organização está sujeita.

A *European Foundation for Quality Management* (2005) desenvolveu o modelo dos "4T's" que, após a identificação e análise dos riscos, permite categorizar os mesmos em quatro formas diferentes de tratamento:

- *Terminate* - cessar as atividades relacionadas com o risco (por exemplo, abandonar ou alienar um negócio);
- *Treat* - adicionar/melhorar controlos ou desenvolver planos de contingência para reduzir a probabilidade de ocorrência ou as consequências de um evento;
- *Tolerate* - aceitar/incorporar o risco, não efetuando qualquer ação (quando a implementação de controlos tem um custo superior ao benefício esperado);
- *Transfer* - partilhar as consequências do risco com outra entidade (por exemplo, contratualizar um seguro, realizar o *outsourcing* de atividades, recorrer a *joint-ventures*).

Estas respostas ao risco apenas devem ser aplicadas depois de ter sido definido previamente pela gestão o apetite pelo risco. Segundo o COSO (2012a) o apetite pelo risco é definido como o nível de risco, determinado pela gestão, que uma organização está disposta a aceitar na busca de valor. Cada organização possui vários objetivos que lhe acrescem valor, devendo procurar entender o risco que a organização está disposta a correr para atingir esses objetivos.

A gestão de risco não deve ser limitada a uma remoção ou redução da exposição ao risco, mas deve ser também entendida numa ótica de exploração e de tomada de riscos estratégicos que possam potenciar o valor das organizações. As empresas de sucesso que hoje conhecemos como a Microsoft, Wal-Mart e a Google, chegaram ao

topo por terem descoberto que conseguem explorar melhor certos tipos de risco do que os seus concorrentes (Damodaran, 2008).

A resposta ao risco deve ser dada tendo em conta que os riscos estão interligados e que por vezes existem *trade-off's* entre riscos, isto é, a tomada de ações tendo em vista a diminuição da exposição a um determinado risco, pode aumentar outro. Por exemplo, se um dos objetivos estratégicos de uma dada organização passa a ser "garantir a disponibilidade imediata dos produtos aos clientes", poderá fazer sentido encetar uma política de aumento do nível de inventários, pois diminuirá o risco de atrasos no cumprimento de encomendas e diminuirá o risco de rutura de inventários. No entanto, esta política poderá também aumentar o risco de perdas, caso o valor de mercado dos inventários esteja em queda, ou aumentar o risco de obsolescência dos produtos. Para além destes riscos diretamente identificáveis, também se deve ter em atenção que um aumento de inventários poderá aumentar a probabilidade de ocorrência de acidentes no manuseamento dos produtos ou aumentar o impacto de um incêndio no armazém geral, aumentando, deste modo, outros riscos.

Conforme é possível ver na figura 8, Berkowitz (2001) aconselha a utilização de gráficos do tipo *spider web* no sentido de por em destaque as lacunas existentes entre o nível dos riscos e o nível das respostas (controlos) existentes numa organização, de forma a melhor se perceber a exposição aos riscos.

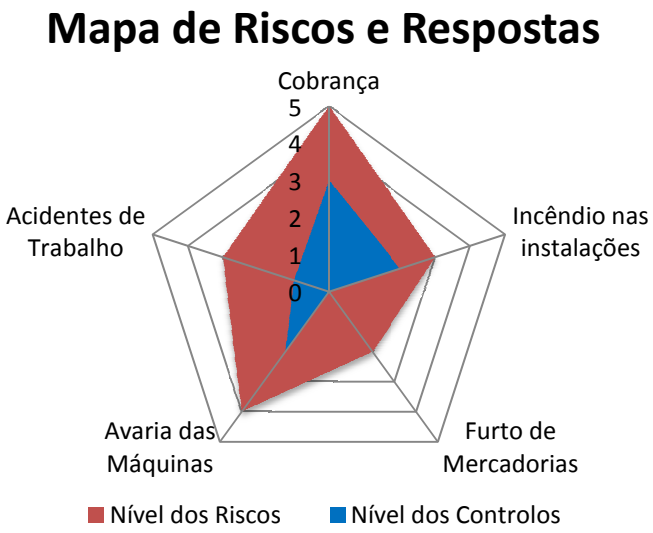

Figura 8 - Mapa de riscos e respostas
Fonte: Berkowitz (2001) Adaptado

III. O papel da Auditoria Interna e do Controlo Interno na Gestão de Risco

Neste capítulo será abordada a problemática existente sobre o papel da auditoria interna e do controlo interno nas atividades de gestão de risco. Para tal, apresenta-se primeiramente uma definição de auditoria interna bem como os princípios em que a mesma se baseia. De seguida, são clarificadas as funções que a auditoria interna deve desempenhar, nomeadamente, no que diz respeito aos processos de gestão de risco. Relativamente ao papel do controlo interno na gestão de risco, são apresentadas uma definição de controlo interno, bem como as dimensões em que o mesmo se deve focar. Posteriormente aborda-se o papel que o controlo interno assume nos processos de gestão de risco, bem como uma categorização do nível de maturidade que as organizações podem apresentar quanto à eficiência e eficácia do seu controlo interno.

3.1. O Papel da Auditoria Interna na Gestão de Risco

Uma das definições de auditoria interna com maior aceitação é a definição dada pela organização com sede nos Estados Unidos da América, o IIA (*The Institute of Internal Auditors*) segundo a qual:

> *"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."* em sítio da *internet* do IIA[4]

De acordo com esta definição, os princípios da independência e da objetividade são valores fundamentais para o auditor interno quer este desempenhe funções de garantia ou consultoria. Ainda segundo o IIA, importa definir os valores de independência e objetividade:

> *"Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner."*
>
> *"Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others."* em sítio da *internet* do IIA[5]

[4] https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

[5] https://na.theiia.org/standards-guidance/topics/Pages/Independence-and-Objectivity.aspx

O objetivo da atividade da auditoria interna é o de avaliar a exposição ao risco da gestão, das operações e dos sistemas de informação das organizações no que se refere à:

- Eficácia e eficiência das operações;
- Fiabilidade e integridade da informação financeira e operacional;
- Salvaguarda dos ativos;
- Observância das leis, regulações e controlos.

Quando se iniciou a adoção por parte das organizações de *frameworks* de gestão de risco, a COSO (2004) recomendou às organizações que as equipas de auditoria interna assistissem a gestão e os comités de auditoria a examinar, avaliar, relatar e recomendar melhorias no que respeita à adequação e eficácia da gestão de risco da organização. Apesar da responsabilidade direta pela gestão de risco ser dos diretores e dos gestores (em especial dos *Chief Executive Officer* e *Chief Financial Officer*), os auditores internos são vistos como contribuidores chave enquanto consultores e garantes dos processos e sistemas de gestão de risco (Stewart & Subramaniam, 2010).

No entanto, segundo a análise realizada por Thompson (2013), diversos autores levantam questões relativamente ao envolvimento da auditoria interna (quanto à sua independência e objetividade) nos processos de gestão de risco, uma vez que, os auditores internos podem entrar numa situação de conflito de interesses: por um lado, prestam serviços de garantia e, por outro lado, prestam consultoria à gestão na implementação de sistemas de gestão de risco (Brody & Lowe, 2000; Fraser & Henry, 2007; Hermanson & Rittenberg, 2003; Krell, 2005; McCall, 2002; Selim, Woodward & Allegrini, 2009).

Na revisão de literatura efetuada por Stewart & Subramaniam (2010) relativa à perda de objetividade e independência por parte dos auditores internos, foram referidos estudos nos quais existe evidência que:

- As atividades de consultoria diminuem a objetividade dos auditores internos (Brody and Lowe, 2000);
- O envolvimento da auditoria interna na gestão de risco afeta negativamente a objetividade percebida (Zwaan, Stewart e Subramaniam, 2009);
- Existem ameaças à sua independência ao se considerar a auditoria interna como “parceira” da gestão (Chrisopher, Sarens e Leung, 2009);

Ou seja, segundo alguns autores, apesar da auditoria interna poder acrescentar valor na gestão de risco, existe a possibilidade de esta comprometer a sua independência e objetividade.

Deste modo, o IIA (2009) clarificou as funções que a auditoria interna deve desempenhar, dividindo-as em três categorias:

(I) Atividades principais	Prestar garantia nos processos de gestão de risco Prestar garantia na correta avaliação dos riscos Avaliar os processos de gestão de risco Avaliar o relato dos principais riscos Rever a gestão dos principais riscos
(II) Atividades legítimas, com salvaguardas	Facilitar a identificação e avaliação dos riscos Orientar a gestão na resposta aos riscos Coordenar atividades de gestão de risco Consolidar o relato de riscos Manter e desenvolver o *framework* de gestão de risco Dirigir a implementação do modelo de gestão de risco Desenvolver a estratégia de gestão de risco a aprovar pela gestão
(III) Atividades a não desempenhar	Definição do apetite pelo risco Impor processos de gestão de risco Tomar decisões sobre a resposta ao risco Implementar respostas ao risco em nome da gestão Responsabilizar-se pela gestão de risco

Figura 9 - Funções da auditoria interna
Fonte: IIA (2009)

As salvaguardas que o IIA (2009) refere na categoria **(II)** dizem respeito às seguintes condições:

- Deve ser claro que a gestão é responsável pela gestão de risco;
- A natureza das responsabilidades do auditor interno deve ser documentada e aprovada pelo comité de auditoria;
- A auditoria interna não deve gerir nenhum dos riscos em nome da gestão;
- A auditoria interna deve aconselhar, desafiar e suportar as tomadas de decisão por parte da gestão, não devendo tomar decisões sobre a gestão de risco;
- A auditoria interna não pode garantir os objetivos de qualquer parte do modelo de gestão de risco do qual seja responsável;
- Qualquer trabalho para além das atividade de garantia devem ser reconhecidos como consultoria e devem ser seguidos os *standards* apropriados para essas atividades.

Segundo esta divisão, os auditores internos devem realizar as funções da categoria **(I),** podendo realizar algumas das atividades da categoria **(II)**, com as devidas salvaguardas. No entanto, apenas em situações excecionais ou em casos muito específicos (como, por exemplo, a pequena dimensão da organização) poderão realizar atividades da categoria **(III)**.

Num inquérito realizado pelo *The Institute of Internal Auditors Research Foundation* (IIARF, 2011) a 321 membros da *Global Audit Information Network* (GAIN) no sentido de apurar o envolvimento da auditoria interna nos processos de gestão de risco, foram obtidos os seguintes resultados:

Atividades especificamente desenvolvidas pela auditoria interna nos processos de gestão de risco	
1. Facilitar a identificação e avaliação de riscos chave	65%
2. Participar na identificação de riscos emergentes	62%
3. Prestar garantia através de relatórios escritos sobre a gestão de riscos chave	49%
4. Orientar a gestão na resposta aos riscos	43%
5. Prestar garantia através de relatórios escritos de auditoria sobre a adequada identificação e avaliação de riscos	38%
6. Prestar relatórios de consultoria para melhorar ou implementar processos de gestão de risco	29%
7. Prestar garantia através de relatórios escritos de auditoria sobre o processo de gestão de risco	28%
8. Realizar o relato consolidado de riscos	17%
9. Participar na definição do apetite pelo risco da organização	11%
10. Desenvolver políticas organizacionais para o processo de gestão de risco	8%
11. Implementar respostas ao risco em nome da gestão	4%
12. Tomar decisões sobre respostas ao risco	3%

Figura 10 - Atividades desenvolvidas pela auditoria interna nos processos de gestão de risco
Fonte: IIARF (2011)

Quase dois terços das respostas indicam que a auditoria interna é responsável pela identificação e avaliação de riscos (atividades 1 e 2), área na qual os auditores internos têm algum nível de experiência e que devem assumir dentro da sua organização. As atividades 3, 5 e 7 são atividades de garantia, nas quais a auditoria interna poderia ter uma maior intervenção, dado o seu papel nas organizações, devendo procurar melhorar a sua participação, nomeadamente na formalização de uma opinião sobre o processo de gestão de risco. Relativamente às atividades 4 e 6, atividades de consultoria que requerem um maior envolvimento com a gestão, estas podem também ser desenvolvidas pela auditoria interna, com as devidas salvaguardas, para não prejudicar a sua independência e objetividade. A atividade 8 com 17% de respostas

afirmativas, apesar de poder ser realizada pela auditoria interna, normalmente é efetuada pela gestão. Segundo as orientações da IIA (2009), as últimas quatro atividades não devem ser desempenhadas pela auditoria interna. Segundo os resultados do inquérito efetuado, pode-se considerar que estas atividades são realizadas pela auditoria interna de uma forma residual.

Ainda no mesmo inquérito da IIARF (2011), concluiu-se que os comités de auditoria das organizações não tinham grandes expectativas quanto ao papel que a auditoria interna poderia desenvolver: menos de metade (41%) dos comités pediram à auditoria interna aconselhamento sobre processos de gestão de risco e apenas 28% dos inquéritos indicaram que o comité de auditoria solicitou à auditoria interna uma revisão específica sobre componentes da gestão de risco. No entanto, quando questionados quanto à necessidade de os comités de auditoria terem um melhor conhecimento dos processos de gestão de risco, 75% dos membros concordam que esta necessidade é emergente. Através destes dados pode-se concluir que os comités de auditoria não se apercebem dos potenciais contributos que a auditoria interna pode trazer para a implementação e suporte da gestão de risco, ou por outro lado, não reconhecem à auditoria interna as capacidades ou experiência necessárias para assegurar atividades de gestão de risco.

Num artigo do IIA & RIMS (2012) resultante do estudo de casos[6], estas instituições defendem que a auditoria interna e a gestão de risco têm todo o interesse em colaborar, uma vez que o seu trabalho em conjunto é realizado de forma mais eficiente e com vantagens para a organização ao nível da:

- Partilha do resultado do seu trabalho e da importância da ligação entre o plano de auditoria (realizado pela auditoria interna) e a avaliação dos riscos (realizado pela gestão da organização): esta partilha de resultados permite eliminar os trabalhos redundantes efetuados por ambas as equipas, destacar áreas de interesse comum e reduzir a sobreposição de análises e avaliação de riscos, o que permite alinhar e construir uma visão comum na organização;
- Partilha dos recursos disponíveis: a utilização da equipa de auditoria interna nos processos de gestão de risco permite obter ganhos ao nível de tempo, pessoal e custos;

[6] Estudo realizado nas organizações Cisco Systems, Hospital Corporation of America, TD Ameritrade e Whirlpool Corporation

- Alavancagem das competências e responsabilidades de ambas as funções: um aumento da comunicação entre a auditoria interna e a gestão de risco permite desenvolver uma linguagem comum e um maior conhecimento dos *frameworks* sobre risco;
- Avaliação e monitorização dos riscos estratégicos: a auditoria interna garante a eficácia da gestão no que se refere aos riscos estratégicos e a gestão de risco fornece as técnicas e os métodos para que a gestão seja eficaz.

O mesmo artigo defende ainda que um dos pontos fortes do trabalho conjunto da auditoria interna e da gestão de risco poderá ser no preenchimento de lacunas na identificação de riscos aos quais não é possível associar/identificar um responsável pelo risco ou pelo controlo.

3.2. O Controlo Interno e a Gestão de Risco

Segundo o COSO (1992), controlo interno significa diferentes coisas para diferentes pessoas o que provoca confusão e erros de comunicação. Deste modo, importa definir em primeiro lugar o que é controlo interno. De acordo com o COSO (2013) controlo interno é definido da seguinte forma:

> *"Internal control is a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."* em COSO (2004), pp.3.

Ainda relativamente ao controlo interno, COSO (2013) defende que este é um processo contínuo de tarefas e atividades, realizado por pessoas (não se tratando de meros manuais de procedimentos, mas sim de pessoas e ações que elas tomam) destinado a fornecer uma garantia razoável à gestão e que é adaptável a toda a organização. Cabe ao controlo interno focar-se em três dimensões:

- Objetivos Operacionais - garantir a eficácia e eficiência das operações, incluindo a performance operacional, financeira e a salvaguarda dos ativos contra perdas;
- Objetivos de Reporte - assegurar o reporte financeiro interno e externo e o reporte não financeiro de um modo transparente, fiável e atempado;
- Objetivos de Conformidade - acautelar a observância das leis e regulações às quais a organização está sujeita.

Ao controlo interno cabe a implementação e monitorização de controlos necessário para garantir os objetivos descritos. O *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards*, da *International Organization for Standardization* (ISO), define controlo como "uma medida que modifica o risco", podendo ser formado por processos, políticas, dispositivos, práticas ou outras ações.

Em muitas empresas os controlos são informais, manuais e pouco rigorosos (PriceWaterhouseCoopers, 2010). A gestão pode acreditar que os controlos estão a funcionar, no entanto, estes podem não estar completamente implementados ou não estar a funcionar do modo pretendido. Outro dos problemas que pode afetar as organizações é o caso de estas terem implementados controlos detetivos (controlos destinados a identificar problemas após a sua ocorrência) e terem ignorado controlos preventivos, isto é, controlos que permitam evitar potenciais problemas. Este último tipo de controlos pode, por exemplo, reduzir o risco de transações não autorizadas, o risco de furto ou fraudes e a compra de inventários em excesso.

Neste sentido, o controlo interno apenas pode fornecer uma garantia razoável na realização dos objetivos da organização uma vez que não pode prevenir julgamentos ou decisões erradas, nem evitar que eventos externos à organização causem uma falha e comprometa os seus objetivos. Outra das limitações do controlo interno pode resultar da capacidade da gestão ou outros colaboradores evitarem os controlos existentes (por exemplo, através do conluio) ou de sobreporem esses mesmos controlos, escondendo práticas fraudulentas ou conflitos de interesse.

Dos modelos anteriormente revistos (COSO-ERM, ISO310000 e FERMA), em todos existe uma etapa consignada ao tratamento a dar ao risco (respetivamente *Control Activities, Risk Treatment* e Tratamento do Risco) na qual são avaliados os controlos existentes e implementados novos controlos. Neste sentido, pode concluir-se que o controlo interno é algo que está subjacente à gestão de risco.

De acordo com a IFAC (2012), o controlo interno é uma parte integral do sistema de gestão de uma organização e da capacidade de gerir riscos, o qual é entendido, efetivado e ativamente monitorizado pela gestão, para tirar vantagens das oportunidades e contrariar as ameaças, no sentido de se atingir os objetivos da organização.

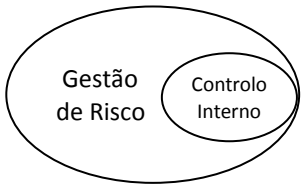

Figura 11 - O controlo interno e a gestão de risco
Fonte: IFAC (2012) Adaptado

A PriceWaterhouseCoopers (2010) desenvolveu uma escala que permite às organizações identificar o estado de maturidade dos seus programas de controlo:

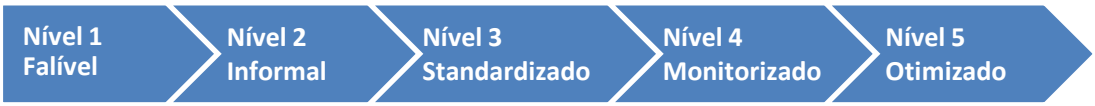

Figura 12 - Níveis de maturidade do programa de controlo
Fonte: PriceWaterhouseCoopers (2010) Adaptado

No primeiro nível (nível 1) encontram-se as organizações onde os controlos não estão designados aos seus responsáveis nem estão em funcionamento. O nível 2 (nível informal) significa que os controlos e as atividades de reporte estão designados e em funcionamento, no entanto, não estão documentados adequadamente. Os controlos dependem fortemente das pessoas e não existe uma comunicação formal das atividades de controlo. No terceiro nível (standardizado), as atividades de controlo estão atribuídas, em funcionamento, devidamente documentadas e comunicadas aos colaboradores. No entanto, os desvios e as sobreposições aos controlos não são detetados. As organizações que se encontram no nível 4 (monitorizado) têm os seus controlos padronizados e testados periodicamente, com reporte para a gestão e recorrem de forma limitada a automatismos e ferramentas para suportarem as atividades de controlo. No último estádio de maturidade dos sistemas de controlo (nível 5 - Otimizado), o modelo integrado de controlo interno permite a monitorização em tempo real dos controlos pela gestão e a melhoria contínua dos mesmos, isto é, uma gestão de risco transversal à organização (*entreprise-wide risk management*). A automatização suporta o controlo da atividade e permite à organização realizar mudanças rápidas ao controlo.

Deste modo, controlos apropriados e a funcionar adequadamente trazem benefícios para as organizações, não só monitorizam o ambiente interno (por exemplo, reduzindo a probabilidade da ocorrência de erros), como criam e preservam valor (PriceWaterhouse Coopers, 2010).

Desde finais de 2008, a agência de *rating Standard&Poor's* (S&P) começou a incorporar nas notações de risco que atribui às organizações uma componente de análise/revisão dos sistemas de gestão de risco. Esta revisão foca-se predominantemente em dois aspetos universais da gestão de risco: na cultura de gestão de risco e na gestão de risco estratégica.

De acordo com a *Standard&Poor's* (2008), a introdução da sua opinião relativamente à capacidade da gestão compreender, articular e gerir o risco, permite aos investidores e obrigacionistas usufruir de uma maior transparência.

IV. Metodologia

Neste capítulo da metodologia apresenta-se em primeiro lugar qual a questão de investigação que sustenta esta dissertação, assim como a explicação sobre a seleção da empresa em estudo. Por último, apresenta-se a metodologia utilizada na elaboração deste estudo bem como a técnica de recolha de dados escolhida para a execução do caso prático.

4.1. Questão de Investigação

No que se refere a Portugal, não parece haver ainda uma grande preocupação no que diz respeito à divulgação e implementação de metodologias de gestão de risco, o que poderá estar relacionado com a própria estrutura do tecido empresarial português, composto essencialmente por pequenas e médias empresas, com pouca capacidade para suportarem os custos de uma equipa de gestão de risco e/ou auditoria interna. Ao nível das grandes empresas cotadas em Portugal[7] existe alguma informação nos sites institucionais onde apenas é feita uma abordagem muito superficial ao tema, com exceção da Portugal Telecom que aprofunda a análise dos riscos a que está sujeita e que revela as medidas/ações tomadas perante os riscos identificados.

Relativamente à literatura sobre gestão de risco, apesar da discussão promovida em diversos ensaios e artigos sobre o tema, não existem ainda muitos estudos baseados na análise de casos, nomeadamente no setor têxtil onde não foi possível apurar a existência de algum estudo.

Neste sentido, este estudo tem por principal objetivo elaborar uma proposta de implementação de um modelo de gestão de risco numa organização, baseada na ISO31000. Esta norma tem a vantagem de fornecer orientações na implementação de um modelo de gestão de risco, não tentando impor uma estrutura de gestão de riscos pré-definida, ainda que ajustável, o que permite à organização definir a sua própria metodologia. Isto é, enquanto o modelo COSO-ERM é mais prescritivo e rígido, cingindo as organizações às fases existentes no modelo, a ISO31000 dá uma maior liberdade às organizações quanto ao estabelecimento de um processo de gestão de risco adaptado às suas necessidades.

[7] Pesquisa realizada nos sites das quatro maiores empresas portuguesas segundo a capitalização bolsista (Galp, Jerónimo Martins, EDP e Portugal Telecom).

Outro dos aspetos que levou à escolha da ISO31000 foi o facto de esta norma ser mais amiga do utilizador, fácil de entender, relativamente simples e linear, ao contrário da complexidade existente na ligação entre as diferentes dimensões do cubo COSO-ERM.

Ainda relativamente à ISO31000, esta norma consegue relacionar de uma forma mais eficaz os riscos com os objetivos e a estratégia da organização face ao modelo COSO-ERM. Dado que o modelo COSO-ERM surgiu como uma solução que as organizações poderiam adotar face às exigências da *Sarbanes-Oxlet Act* (SOX), é natural que este esteja direcionado para o controlo e mitigação do risco e para a observância da conformidade com as leis, enquanto as orientações da ISO31000 são mais dinâmicas no que se refere ao processo de gestão de risco e na sua ligação com a estratégia que a organização pretende seguir.

Relativamente ao modelo FERMA, este pode ser entendido como uma fusão entre a norma ISO31000 e o modelo COSO-ERM, uma vez que, por um lado, utiliza os conceitos de risco definidos pelo *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards,* da *International Organization for Standardization* (ISO) e, por outro lado, propõe um modelo de gestão de risco relativamente simples e linear.

Assim, dados os aspetos acima descritos, entendeu-se que o modelo da ISO31000 seria o mais adequado face às necessidades e objetivos deste estudo.

Deste modo, e utilizando a abordagem que o modelo selecionado sugere, este estudo pretende alcançar ainda os seguintes objetivos:

- Obter informação sobre os riscos que cada departamento da organização enfrenta;
- Perceber as causas de eventuais dificuldades na identificação, análise e avaliação dos riscos existentes na organização;
- Identificar os eventuais controlos existentes e os eventuais controlos a implementar como forma de mitigar os riscos;
- Confrontar a sensibilidade aos riscos revelada pelos *risk owners* (diretores de departamento) com a perceção dos riscos demonstrada pela gestão/administração.

4.2. Seleção do Caso de Estudo

A organização escolhida para a proposta de implementação de um *framework* de gestão de risco é uma empresa de referência do setor têxtil, cuja gestão mostrou

interesse e disponibilidade para que fosse desenvolvido um estudo que realizasse um levantamento dos riscos e dos controlos existentes na organização, no sentido de os evidenciar com maior detalhe e, sobretudo, de formalizar esse levantamento.

Uma das causas que possibilitou o desenvolvimento deste estudo foi a relação que desenvolvi com a organização, dado que à data de início do estudo eu era colaborador na área da contabilidade. No entanto, esta relação não afetou o estudo uma vez que, para além do *risk owner* do departamento financeiro, não tinha estabelecido contacto prévio com outros diretores departamentais.

4.3. Metodologia e Técnicas de Recolhas de Dados

Numa fase inicial, a metodologia passou pela recolha de informação relevante junto de entidades representativas do sector têxtil em Portugal, no sentido de ser possível enquadrar a situação da empresa em estudo na situação global do sector. Paralelamente, foi levada a cabo uma pesquisa documental relativa ao tema do risco e da gestão de risco, que permitisse perceber o *state of the art* dos modelos de gestão de risco existentes.

Numa segunda fase, foi necessário recolher informação específica da empresa em estudo. Para tal, e tendo em conta a natureza do tema abordado, foram realizadas entrevistas semi-estruturadas, isto é, entrevistas com questões pré-definidas, mas às quais os inquiridos puderam responder abertamente. De acordo com Ghauri, *et al.* (2010), este modelo de entrevista permite, por um lado, controlar a entrevista de acordo com a informação que se pretende obter e, ao mesmo tempo, permite que seja possível conseguir-se uma explicação detalhada das respostas auferidas. As entrevistas iniciaram-se com uma questão de resposta aberta ("Que eventos[8] podem por em causa a concretização dos objetivos do departamento/organização?"), aprofundando-se as informações sobre os riscos com questões gradualmente mais específicas, de modo a assegurar uma recolha de dados detalhada.

Neste sentido, foi realizada uma entrevista a um dos administradores da organização para se obter uma contextualização do ambiente interno e externo da empresa e realizar uma primeira abordagem aos principais riscos enfrentados pela organização, de modo a tornar possível a construção de modelo de gestão de risco.

[8] O *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards*, desenvolvido pela ISO, define evento como "a ocorrência ou alteração de um conjunto particular de circunstâncias".

Posteriormente foram encetadas entrevistas com os responsáveis dos vários departamentos da organização de modo a formalizar as opiniões que estes tinham acerca dos riscos e dos controlos. Durante as entrevistas foram utilizados suportes em formato de tabelas (conforme anexos 2 a 10) que serviram de fio condutor e auxiliaram na avaliação desses riscos e controlos. As entrevistas realizadas tiveram a duração máxima de sessenta minutos por sessão, de forma a controlar possíveis enviesamentos na informação recolhida, resultante da diminuição dos níveis de atenção dos entrevistados. No máximo foram realizadas três sessões por cada *risk owner* departamental. Relativamente à técnica de avaliação dos riscos e dos controlos optou-se por uma técnica qualitativa, uma vez que esta permite uma avaliação relativamente rápida e fácil, permite obter uma informação mais rica (considerando aspetos como por exemplo a reputação da organização, não traduzíveis num valor monetário) e é facilmente compreendida por todos os colaboradores da empresa. Apesar de a técnica ter desvantagens (pode revelar-se algo imprecisa e limita a resposta dos diretores aos nível de diferenciação definidos), esta demonstra ser a mais adequada face aos objetivos estudo em questão.

Numa fase seguinte, após ter sido consolidada a informação obtida, foram apresentadas as tabelas resumo da informação aos *risk owners* e foi dada a oportunidade de se ajustarem as avaliações atribuídas e complementarem a informação fornecida.

Por último, foi realizada uma nova entrevista com o mesmo administrador ao qual foi realizada a entrevista inicial, com o objetivo de: apurar os riscos considerados confidenciais e não passíveis de serem divulgados no presente estudo; e, também, de se ajustar a classificação dos riscos e dos controlos identificados.

V. O Estudo de Caso: Proposta de um Modelo de Gestão de Risco

No presente capitulo, apresenta-se, primeiramente, a metodologia de gestão de risco selecionada para elaborar a proposta de um modelo de gestão de risco para a organização em estudo.

De seguida, são descritos e aplicados ao caso de estudo, cada um dos 5 componentes que devem reger um modelo de gestão de risco.

Mais concretamente no ponto que se refere à construção de um modelo de gestão de risco (um dos cinco componentes), é apresentada uma proposta de modelo de gestão de risco a aplicar à organização, decorrente da aplicação da metodologia de gestão de risco à organização em estudo e da análise das necessidades da mesma.

Importa também referir que no componente de implementação do modelo, apresenta-se uma análise da envolvente interna e externa da organização, a sua estratégia e principais objetivos e, por último, são enumerados os principais riscos, controlos e respostas identificados em cada departamento, assim como de uma análise das lacunas identificadas entre riscos e controlos existentes.

***

De la Rosa (2007) defende que se deve ter em atenção três aspetos essenciais na implementação de um modelo de gestão de risco, de modo a evitar atrasos desnecessários e acréscimo de custos:

1) Manter o modelo simples no início;
2) Planear as etapas a seguir;
3) Saber o que é importante.

Tendo em conta as recomendações de De la Rosa (2007) e dado que a organização não tem implementado um modelo formal de gestão de risco, tal como será demonstrado adiante, decidiu-se pela aplicação da ISO31000,

Assim, na figura 13, apresentam-se os cinco componentes que devem constituir um modelo de gestão de risco, aplicados ao caso de estudo.

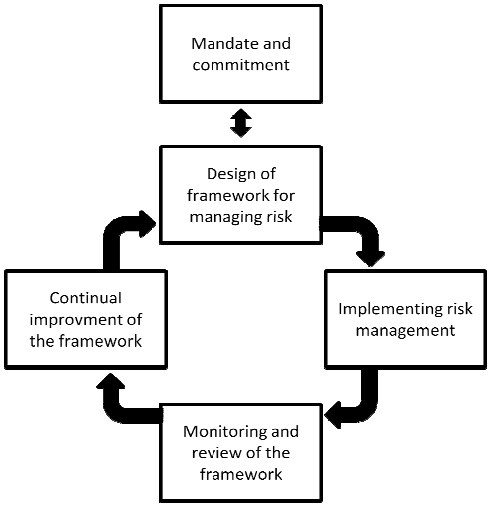

Figura 13 - Componentes de um modelo de gestão de risco
Fonte: ISO31000 (Adaptado)

O primeiro componente a verificar passa pelo compromisso da gestão na sua implementação.

5.1. Compromisso e Legitimidade

Um projeto dificilmente consegue atingir os seus objetivos dentro de uma organização se não tiver o apoio por parte da gestão. Deste modo, e de acordo com as orientações da ISO31000, a primeira entrevista realizada com o administrador da organização permitiu estabelecer um compromisso por parte da gestão de analisar uma proposta de implementação de um modelo integrado de gestão de risco e de legitimar junto dos colaboradores o interesse do presente estudo. Foram, também, comunicados aos *risk owners* os objetivos do presente estudo e agendadas as entrevista exploratórias com os mesmos.

5.2. Construção do modelo de gestão de risco

Numa segunda fase deste estudo, foi feita uma contextualização da empresa, uma vez que o contexto interno e externo de uma organização pode influenciar o *design* do modelo de gestão de risco. Esta contextualização será apresentada aquando da fase da implementação da gestão de risco.

Foram ainda definidos os recursos a utilizar por este estudo, identificados os *risk owners* com os quais se desenvolveriam as entrevistas e definido o caderno de encargos a desenvolver.

Por último, nesta segunda etapa, foi feita ainda uma avaliação da situação da empresa no que se refere às atuais atividades de gestão de risco.

Atualmente a gestão de risco realizada pela empresa consiste numa avaliação e tratamento dos riscos a um nível departamental. Esta avaliação e tratamento são realizados pelo responsável do departamento que reporta hierárquica e funcionalmente aos administradores/ gestão de topo.

De um modo geral, a comunicação das atividades de controlo e de gestão de riscos são realizadas informalmente, não estando documentadas de forma adequada em relatórios escritos e periódicos. A maior parte dos controlos existentes são manuais ou dependem do conhecimento das pessoas e do negócio, com exceção de alguns controlos automáticos implementados no sistema informático SAP.

Existe também o entendimento por parte da administração / gestão de topo que não há uma necessidade premente de desenvolver organizacionalmente uma equipa dedicada às atividades de gestão de risco ou à auditoria interna dado a relativa facilidade

e proximidade com que os diferentes níveis hierárquicos comunicam. Uma equipa especializada nas atividades referidas teria ainda de possuir um conhecimento detalhado do negócio e necessitaria de um orçamento próprio, investimento este, que a gestão acredita poder rentabilizar de modo mais eficiente noutras áreas.

De acordo com as características acima referidas, pode-se classificar o nível de maturidade dos sistemas de controlo na escala desenvolvida pela PriceWaterhouseCoopers (2010) no nível 2 - Informal.

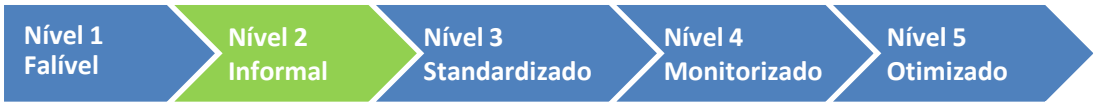

Figura 14 - Níveis de maturidade do programa de controlo
Fonte: PriceWaterhouseCoopers (2010) Adaptado

Deste modo, após uma reflexão sobre a informação recolhida nesta etapa, foi desenvolvido o seguinte modelo de gestão de risco a aplicar na organização:

Figura 15 - Proposta de um modelo de gestão de risco
Fonte: Elaboração Própria

Este modelo contempla todas as recomendações da ISO31000 e revela-se adequado tendo em conta a realidade da organização acima descrita.

Assim, a primeira componente do modelo proposto consiste numa análise da envolvente interna e externa da organização, a qual permitirá facilitar toda a aplicação

do modelo. Deste modo, nesta fase será levada a cabo uma caraterização da organização e do setor onde se insere.

A segunda componente - "Estratégia e Objetivos" - passa pela descrição da estratégia e dos objetivos da organização tendo em conta a análise efetuada anteriormente na componente "Envolvente Interna e Externa".

Na "Determinação dos Riscos" serão identificados os potenciais riscos a que a organização está exposta, a sua análise e avaliação.

Na etapa seguinte - "Controlos e Respostas" - deverão ser avaliados os controlos existentes face aos riscos anteriormente identificados, a resposta a dar a esses mesmos riscos e a implementação de novos controlos e/ou a melhoria dos existentes.

Após a implementação dos controlos, segue-se a etapa de "Revisão e Monitorização", a qual consiste na verificação, análise e possível revisão da eficácia e eficiência dos controlos.

Por último, o componente central do modelo é a "Informação e Formalização". Esta, está sempre presente em todas as fases anteriores e pretende que as principais conclusões e informações obtidas em cada etapa sejam introduzidas num suporte adequado, de forma a poderem ser consultadas e revistas periodicamente.

Dado que a gestão de risco é um processo iterativo e contínuo, o modelo foi construído de forma circular, uma vez que cada uma das etapas impacta nas etapas seguintes. Quanto ao seu núcleo, este propõe-se a elevar a gestão de risco na organização ao patamar seguinte (Nível 3 - Standardizado) da escala de maturidade dos sistemas de controlo proposta por PriceWaterhouseCoopers (2010).

5.3. Implementação do modelo proposto de gestão de risco

Neste capítulo será implementado o modelo de gestão de risco anteriormente proposto à organização em estudo.

i. Envolvente Interna e Externa

a. Enquadramento do Setor Têxtil e do Vestuário

O que normalmente é entendido por setor têxtil, é na realidade composto por dois setores distintos: o setor têxtil e o setor de vestuário. O primeiro é associado aos

processos de fabrico de tecido: obtenção das fibras e posteriores transformações (fiação, tecelagem, tingimento e acabamentos), assim como à produção de têxteis lar e têxteis técnicos, caraterizado por ser capital intensivo. Já o setor do vestuário consiste na transformação de materiais têxteis em vestuário (*design*, corte e confeção) e é normalmente associado a uma forte componente de mão-de-obra intensiva. Quando à produção da indústria têxtil e do vestuário, esta tem como destino dois mercados distintos:

- Mercados de consumo - mercado ligado à moda e à decoração de interiores é composto pelo vestuário, pelos têxteis-lar (tapeçaria, cortinados) e pelos têxteis para interiores (roupa de banho, roupa de cama);
- Mercados industriais/profissionais - este mercado está ligado à utilização dos têxteis em aplicações industriais e profissionais (têxteis para a indústria automóvel, aeronáutica, para profissionais de saúde).

Segundo o Centro de Inteligência Têxtil - CENIT (2009), a indústria do têxtil e do vestuário assistiu, no plano internacional, a diversas e significativas alterações desde a década de sessenta com a implementação do sistema de quotas de importação pelos países desenvolvidos (União Europeia e Estados Unidos da América). Este mecanismo pretendia a limitar a importação de têxteis e vestuários, protegendo, dessa forma, a indústria existente nesses países.

No entanto, ao longo das décadas de 70 e 80, a crescente concorrência dos produtores dos países em vias de desenvolvimento (especialmente em produtos de mão-de-obra intensivos) começou a criar dificuldades a alguns segmentos dos setor têxtil e do vestuário até agora protegidos, tendo gerado um consenso sobre a necessidade de eliminar gradualmente as restrições comerciais que afetavam o desenvolvimento do mercado.

Deste modo, no final de 2004, procedeu-se à eliminação das restrições quantitativas às importações no âmbito do Acordo sobre Têxteis e Vestuário (ATC - *Agreement on Textiles and Clothing*[9]) celebrado na Organização Mundial do Comércio (OMC). Esta eliminação das barreiras alfandegárias possibilitou aos países em vias de

[9] O acordo previa um período de 10 anos (de 1995 até ao final de 2005) para a supressão gradual das quotas alfandegárias de importação.

desenvolvimento um crescimento das exportações, reforçando a sua vantagem competitiva sobretudo em produtos de mão-de-obra intensiva.

No que se refere à indústria do têxtil e do vestuário em Portugal, o acordo relativo à supressão das barreiras alfandegárias:

a) Aumentou a concorrência (livre entrada de produtos têxteis e de vestuário de países como a China, Índia e Paquistão e de países de Leste com o progressivo alargamento da União Europeia);
b) Obrigou ao reposicionamento do setor (apesar de a indústria têxtil e do vestuário ser uma das indústrias portuguesas mais especializadas, em 1996 a sua vantagem competitiva baseava-se nos baixos custos salariais).

Apesar de a sua importância ter vindo a diminuir ao longo dos últimos vinte anos, a indústria têxtil e do vestuário em Portugal continua a ser um dos setores mais representativos da economia portuguesa (Amador e Opromolla, 2009).

De acordo com a ATP (Associação Têxtil e Vestuário de Portugal, 2013), o setor é constituído por cerca de cinco mil empresas (na sua maioria pequenas e médias empresas), conhecidas pela sua flexibilidade, resposta rápida, *know-how* e inovação. Estas empresas estão concentradas sobretudo na região do Norte de Portugal (nos concelhos do Porto, Braga, Guimarães e Famalicão) e na zona da Covilhã e representam cerca de:

- 9% das exportações totais;
- 20% do emprego da indústria transformadora;
- 8% do volume de negócios da indústria transformadora;
- 8% da produção da indústria transformadora.

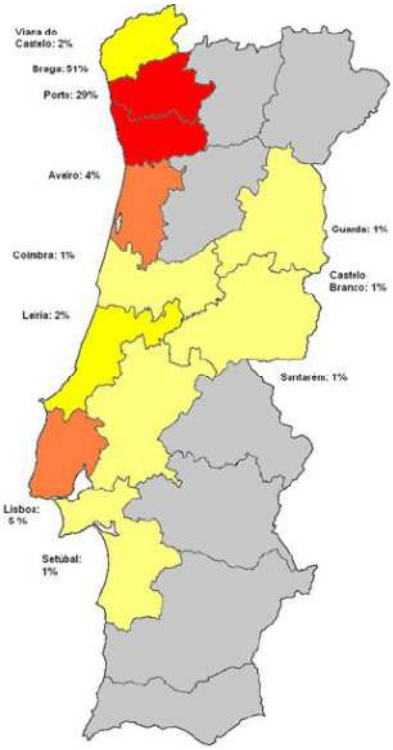

Figura 16 - Distribuição geográfica das empresas do setor têxtil e do vestuário. Fonte: ATP (2013)

Apresentam-se de seguida alguns dados setoriais mais relevantes da fileira têxtil portuguesa:

	2004	2005	2006	2007	2008	2009	2010	2011	2012
Produção*	7.215	6.595	6.608	6.660	6.132	5.123	5.631	5.102	4.905
Volume de negócios*	7.471	6.857	6.827	6.895	6.358	5.349	5.829	6.075	5.774
Exportações*	4.546	4.097	4.229	4.352	4.088	3.501	3.844	4.152	4.130
Importações*	3.286	3.017	3.297	3.417	3.295	3.038	3.424	3.388	3.045
Emprego	201.064	191.714	180.379	176.226	168.117	148.059	138.124	133.100	127.976
Balança Comercial*	1.260	1.080	932	935	793	463	420	764	1.085

Figura 17 - Dados do setor têxtil e do vestuário
Fonte: ATP (2013)

NOTA: *Valores em milhões (€)
Campos sublinhados são estimativas ATP

Conforme é possível verificar na tabela anterior, a indústria do têxtil e do vestuário regista uma tendência negativa ao longo de todo o período, com os dados relativos à produção (-32%), ao volume de negócios (-23%) e ao emprego sustentado por este setor (-36%) a indicarem perdas significativas. No ano de 2009, ano do despoletar da atual crise financeira, foi um ano de evidente quebra em todos os indicadores, apesar de se ter verificado na sua maioria uma ligeira recuperação no ano de 2010. Salienta-se ainda a evolução do contributo do setor para a balança comercial nos anos de 2011 e 2012, que inverteram a tendência de quebra que se vinha a registar em anos anteriores.

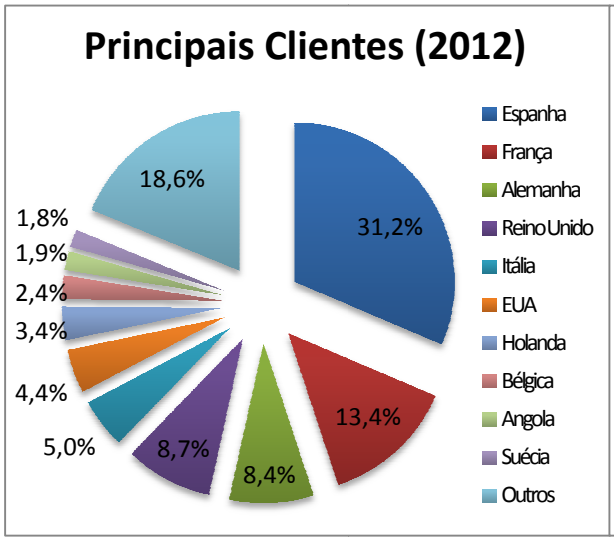

Figura 18 - Principais clientes
Fonte: ATP (2013)

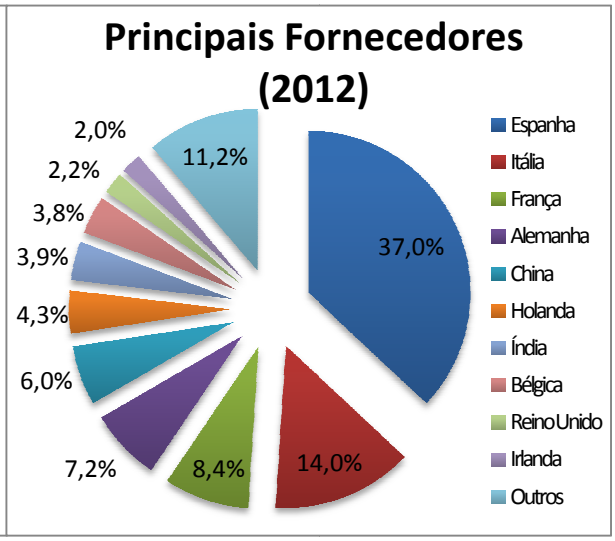

Figura 19 - Principais fornecedores
Fonte: ATP (2013)

Nas figuras 18 e 19 é possível verificar uma listagem dos dez principais clientes e fornecedores da indústria têxtil e do vestuário. Em ambos os casos, o comércio intra-europa (União Europeia a 27) representa mais de 80% do valor gerado pela indústria, o que demonstra a estreita ligação e dependência do mercado europeu, principalmente dos países da Europa ocidental (ver anexo 1).

A análise SWOT é uma ferramenta muito útil na avaliação estratégica de uma indústria ou negócio, auxiliando a gestão a desenvolver de uma estratégia competitiva para a organização. A sigla SWOT resulta do acrónimo *Strength*s (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades), *Threats* (ameaças).

Segundo a ATP (2013), a análise da fileira têxtil portuguesa é a seguinte:

Forças *(Strengths)*	**Fraquezas** (*Weaknesses*)
➢ Tradição e "know-how" industrial têxtil; ➢ Equipamento e tecnologias modernas; ➢ Flexibilidade e grande reatividade; ➢ Fileira Têxtil e do Vestuário completa, estruturada e dinâmica; ➢ Fileira apoiada em consistentes e desenvolvidos centros de competências (CITEVE E MODATEX); ➢ Proximidade geográfica e cultural dos mercados tradicionais.	➢ Baixa produtividade da mão-de-obra; ➢ Baixo nível educacional e formativo dos recursos humanos a todos os níveis da empresa; ➢ Reduzida dimensão das empresas; ➢ Descapitalização das empresas; ➢ Baixa terciarização do tecido empresarial; ➢ Individualismo empresarial.
Oportunidades (*Opportunities*)	**Ameaças** (*Threats*)
➢ Nichos de mercado; ➢ Mercados Emergentes; ➢ Especialização industrial; ➢ Têxteis técnicos e funcionais; ➢ Concentração e cooperação empresarial para ganhar dimensão crítica e competitividade; ➢ Clientes de proximidade e pequenas séries de alto valor acrescentado; ➢ Moda, marcas e distribuição "*made in* Portugal".	➢ Endurecimento da concorrência internacional nos produtos básicos, mas também em gamas de maior valor acrescentado; ➢ Dificuldade no acesso ao crédito e o custo do financiamento; ➢ Persistência da crise económica nos mercados tradicionais da ITV portuguesa; ➢ Falta de atratividade do setor para jovens profissionais, que optam por outras atividades; ➢ Fecho de cursos superiores e declínio da formação profissional especializada; ➢ Risco de desestruturação da Fileira Têxtil e do Vestuário.

Figura 20 - Análise SWOT do setor têxtil em Portugal
Fonte: ATP (2013)

b. Caraterização da Empresa

A organização sobre a qual se realizou uma proposta para a aplicação de um modelo de gestão de risco é uma grande empresa de referência da região norte de Portugal e dedica-se à produção de tecido. A empresa apresenta uma estrutura verticalmente integrada com diversas valências nas áreas de fiação, torcedura, tecelagem, tinturaria e acabamentos. Possui forte capacidade exportadora (98% da produção de tecido é exportada) com os Estados Unidos da América, Alemanha, Itália, França e Reino Unido entre os seus principais mercados. O volume de negócios é superior a 50 milhões de euros e a organização conta com cerca de 850 colaboradores.

A empresa possui uma grande experiência e tradição no fabrico de tecidos e está dotada da mais recente tecnologia, o que lhe permite produzir tecidos de uma gama média-alta a preços competitivos e com rapidez colocá-los à disposição dos seus

clientes nos principais mercados. Esta capacidade de resposta traduziu-se num estreitar de relações com os principais *players* de moda.

O facto de a produção ser realizada em Portugal garante à organização uma vantagem na capacidade de resposta face às solicitações dos clientes dos mercados da Europa e dos Estados Unidos da América, e o selo "*made in Europe*" transmite ao cliente uma maior confiança na qualidade dos produtos que adquire. Ainda, pode referir-se que a empresa aposta fortemente na inovação, considerando-a como uma vantagem competitiva.

Na primeira entrevista com o administrador da organização foi também possível apurar as seguintes grandes ameaças para a organização:

- Crescente importância dos produtores asiáticos no mercado europeu;
- Crescente competição por parte das empresas concorrentes do setor têxtil na Turquia (oferecem melhores preços, mas menores capacidades de *design*).

ii. Estratégia e Objetivos

De acordo com a entrevista realizada com o administrador da organização, e face à envolvente anteriormente analisada, a gestão desenvolveu uma estratégia de crescimento focada na qualidade e no serviço e assente nos seguintes objetivos:

- ✓ Oferecer preços competitivos nos seus tecidos;
- ✓ Melhorar os prazos de entrega das encomendas;
- ✓ Melhorar o prazo de desenvolvimento do produto;
- ✓ Reforçar o acompanhamento dos principais clientes;
- ✓ Aumentar a flexibilidade e capacidade de resposta da empresa;
- ✓ Oferecer produtos inovadores ao mercado.

Para além destes grandes objetivos, foram também atribuídos e desdobrados objetivos departamentais para cada área, alinhados com a estratégia, a visão e missão da organização.

iii. Determinação dos Riscos, os Controlos e Respostas

Para efeitos de apresentação e para um maior entendimento da dinâmica da gestão de risco, decidiu-se apresentar em conjunto o resultado das fases "Determinação dos Riscos" e "Controlos e Respostas", apesar de as fases surgirem como etapas

distintas na proposta do modelo de gestão de risco para a organização. Esta apresentação permite obter vantagens no momento de comparação dos riscos e dos controlos e na deteção de eventuais lacunas.

Nas entrevistas realizadas com os *risk owners* indicados pela gestão de topo foi pedido aos entrevistados que abordassem os seguintes tópicos:

i. Identificação e detalhe dos eventos que poderiam por em causa os objetivos do departamento e da organização;
ii. Avaliação qualitativa dos eventos/riscos quanto à probabilidade de ocorrência e quanto ao seu impacto;
iii. Identificação dos controlos existentes e em funcionamento na organização;
iv. Classificação dos controlos existentes quanto à eficácia e eficiência do mesmo na prevenção e deteção do evento gerador de risco;
v. Definição da resposta mais adequada a aplicar ao risco;
vi. Definição de eventuais melhorias a aplicar aos controlos existentes.

A avaliação qualitativa pedida aos entrevistados consistiu numa classificação dos riscos e dos controlos existentes numa escala entre 1 e 5 (Berkowitz, 2001), na qual o nível 1 significa baixa probabilidade ou impacto do risco (baixo grau do controlo) e o nível 5 como indicador de alta probabilidade ou impacto do risco (alto grau do controlo). Quando não era possível apurar a existência de algum controlo, foi atribuído o valor 0.

Como referido na metodologia, esta avaliação permitirá construir gráficos do tipo *spider web* conforme proposto por Berkowitz (2001).

Segundo o COSO (2012b), os riscos podem ainda ser dispostos em mapas de riscos, de acordo com a probabilidade de ocorrência e o seu nível de impacto na organização.

Após o preenchimento das tabelas resumo e da consolidação da informação recolhida, foi dada oportunidade aos *risk owner* de ajustarem os níveis atribuídos aos riscos, os controlos e as respostas a dar aos mesmos. Concluída esta fase, os resultados foram apresentados e submetidos à administração para revalidação e consolidação da informação gerada e para retirada da informação considerada sensível/confidencial.

Deste modo, foi apurada a seguinte informação relativa aos seguintes departamentos:

Departamento de Recursos Humanos

Foram identificados os seguintes riscos:

R1) Contratação inadequada;
R2) Saída de elementos-chave da organização;
R3) Acidentes de trabalho;
R4) Formação inadequada;
R5) Comunicação deficitária com os colaboradores;
R6) Subcontratação de pessoal;
R7) Absentismo.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

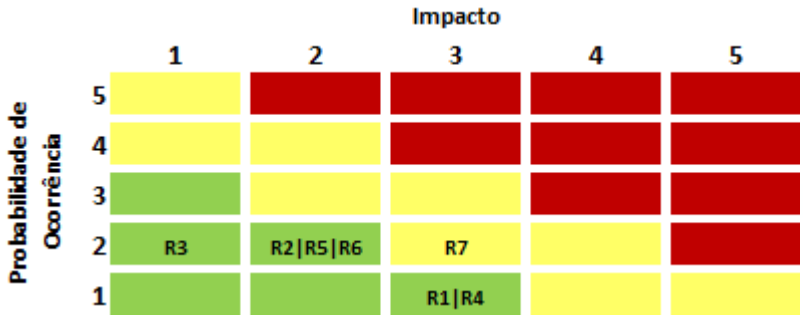

Figura 22 - Mapa de risco - departamento de Recursos Humanos

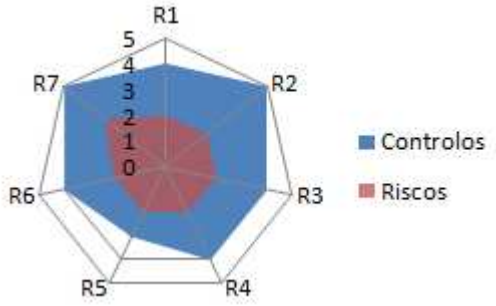

Figura 21 - Riscos e controlos existentes - departamento de Recursos Humanos

Destacam-se, ainda, as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Realizar inquéritos de satisfação aos colaboradores;
- Melhorar os equipamentos de proteção individuais e coletivos e incutir uma cultura de segurança;
- Definir um plano de comunicação interno.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 2.

Departamento Comercial e de Marketing

Foram identificados os seguintes riscos:

C1) Erros de transmissão de informação;
C2) Incumprimento de prazos acordados;
C3) Presença *online* limitada;
C4) Perda de informação sobre mercados;
C5) Desadequação de propostas feitas a clientes;

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

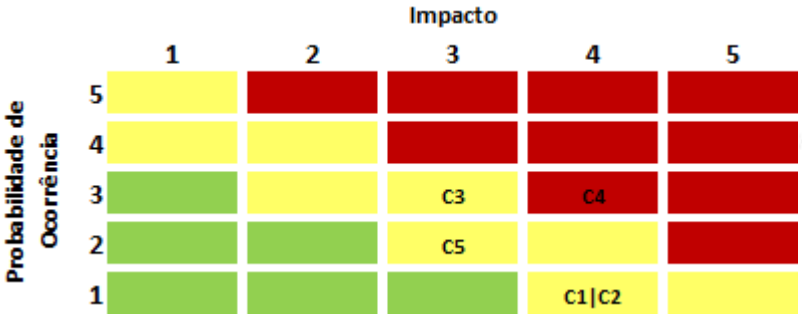

Figura 24 - Mapa de risco - departamento Comercial e de Marketing

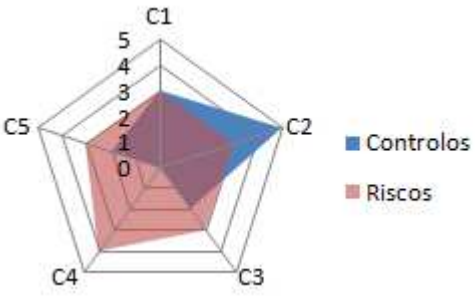

Figura 23 - Riscos e controlos existentes - departamento Comercial e de Marketing

Destacam-se, ainda, as seguintes propostas de controlos a implementar com vista a melhorar o controlo de alguns dos riscos identificados:

- *Standardizar* documentos e procedimentos;
- Implementar um APO (*advanced planning optimizer*);
- Definir um plano de comunicação interno;
- Desenvolver a função de Marketing.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 3.

Departamento de Planeamento e Compras

Foram identificados os seguintes riscos:

P1) Quebra de encomenda;
P2) Incumprimento de prazos de entrega;
P3) Aprovisionamento incorreto de matérias-primas e stocks;
P4) Lançamento de telas ou tecidos acabados;
P5) Não qualidade de fornecedores;
P6) Falha de informação nas listas técnicas de produtos;
P7) Falha de informação aos clientes.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

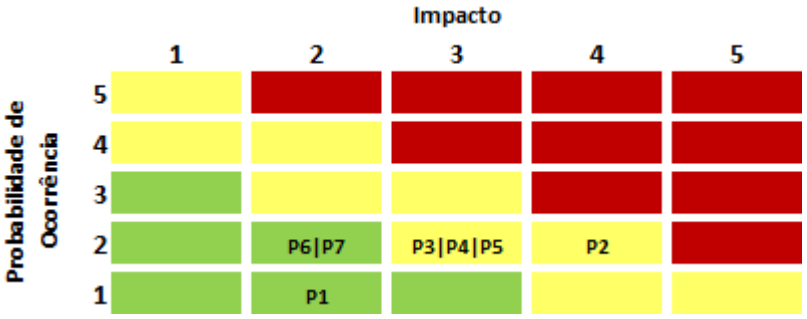

Figura 25 - Mapa de risco - departamento de Planeamento e Compras

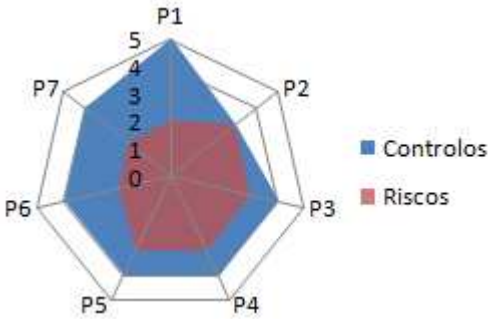

Figura 26 - Riscos e controlos existentes - departamento de Planeamento e Compras

Destacam-se, ainda, as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Melhorar relação com clientes e fornecedores;
- Melhorar o processo e o *reporting* da produção;
- Obter informação sobre previsões de vendas;
- Revalidar parâmetros das fichas técnicas.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 4.

Departamento Financeiro

Foram identificados os seguintes riscos:

F1) Redução de linhas de financiamento;
F2) Volatilidade do preço de matérias-primas;
F3) Crédito concedido a clientes;
F4) Não fiabilidade das demonstrações financeiras;
F5) Não cumprimento das obrigações fiscais;
F6) Não fiabilidade dos indicadores de gestão;
F7) Fuga de informação sensível;
F8) Utilização das plataformas *online* de gestão bancária/tesouraria;
F9) Pagamento indevido devido a erro;
F10) Não cumprimento dos prazos de pagamento a fornecedores;
F11) Assunção de *plafonds* internos de crédito a clientes;
F12) Risco cambial e de taxa de juro.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

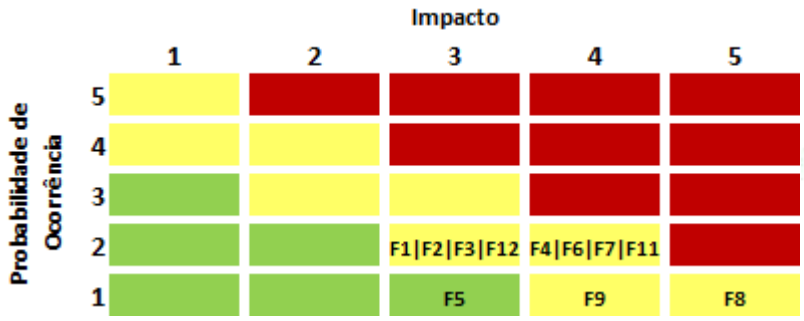

Figura 28 - Mapa de risco - departamento Financeiro

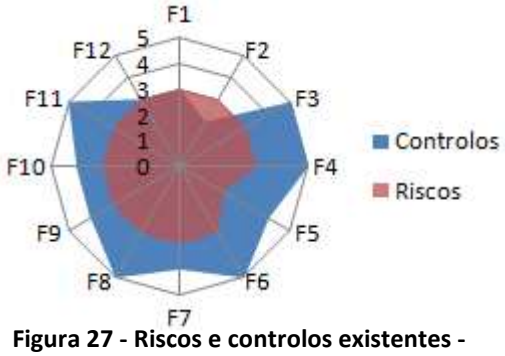

Figura 27 - Riscos e controlos existentes - departamento Financeiro

Destacam-se ainda as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Integrar planeamento;
- Auditar processos de concessão de descontos a clientes;
- Reforçar automatização de produção de informação a partir do SAP;
- Estabelecer um código de ética e confidencialidade;
- Estabelecer uma política formal de crédito.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 5.

Departamento de Sistemas de Informação

Foram identificados os seguintes riscos:

I1) Incêndio;
I2) Perda de dados;
I3) Furto de informação.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

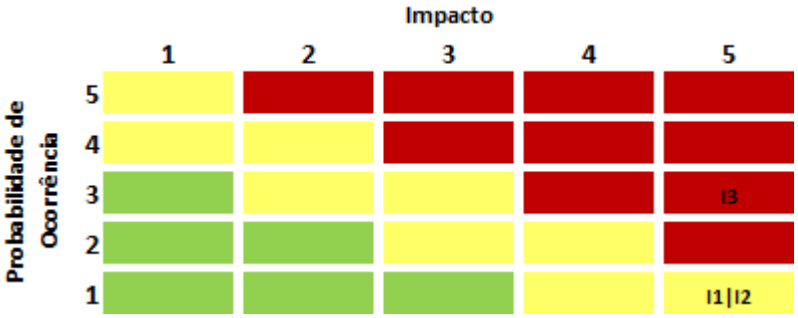

Figura 30 - Mapa de risco - departamento de Sistemas da Informação

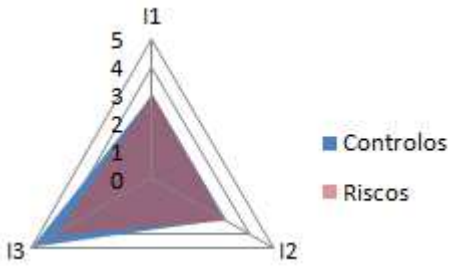

Figura 29 - Riscos e controlos existentes - departamento de Sistemas da Informação

Destacam-se ainda as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Instalação de sistemas anti-fogo;
- Aquisição de um sistema contínuo de *backups*;
- Estabelecer níveis de autorizações.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 6.

Departamento de Logística

Foram identificados os seguintes riscos:

L1) Contaminação de produtos;
L2) Furto de mercadorias;
L3) Criação de monos;
L4) Aumento de custos de transporte;
L5) Incumprimento do prazo de entrega.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

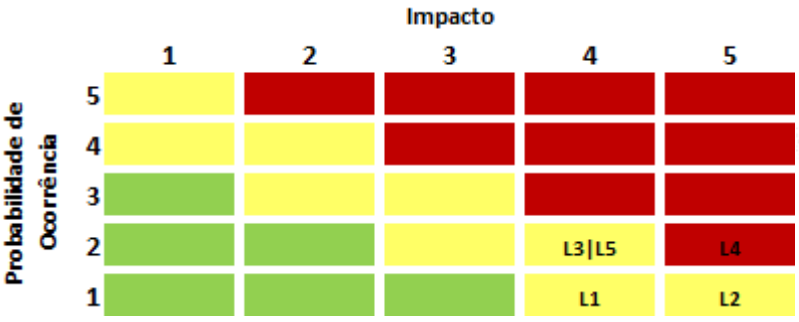

Figura 32 - Mapa de risco - departamento de Logística

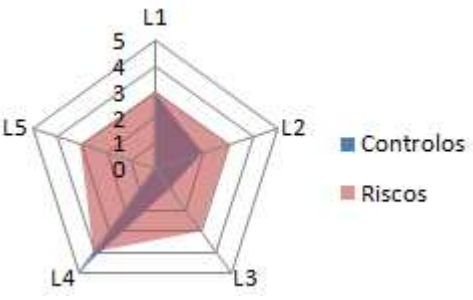

Figura 31 - Riscos e controlos existentes - departamento de Logística

Destacam-se, ainda, as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Instalação de um sistema de vídeo vigilância nos locais de carga/descarga;
- Implementar política comercial de abate de monos;
- Automatização do processo de acompanhamento de encomendas.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 7.

Departamento de Desenvolvimento

Foram identificados os seguintes riscos:

D1) Produtos sem sucesso comercial;
D2) Falha do sistema informático;
D3) Disparidade no custeio teórico/real;
D4) Incoerência dos processos desenvolvimento/produção.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

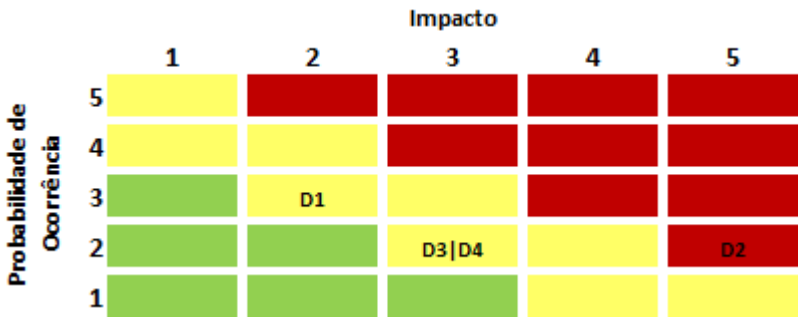

Figura 34 - Mapa de risco - departamento de Desenvolvimento

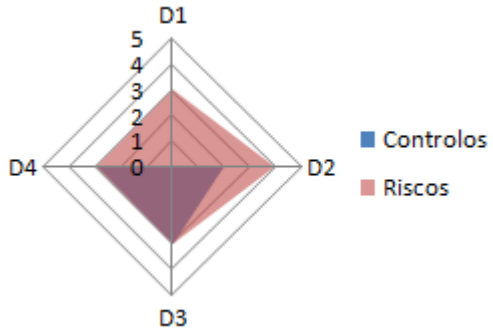

Figura 33 - Riscos e controlos existentes - departamento de Desenvolvimento

Destacam-se ainda as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Desenvolvimento da função de Marketing;
- Aquisição de um novo sistema informático;
- Criação de uma biblioteca do conhecimento.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 8.

Departamento de Qualidade, Ambiente e Segurança

Foram identificados os seguintes riscos:

Q1) Contaminação dos lençóis freáticos;
Q2) Ruído ambiental para o exterior;
Q3) Utilização de água imprópria para consumo;
Q4) Derrame de produtos químicos;
Q5) Incêndio nos teares;
Q6) Incêndio na gaseadeira;
Q7) Emissão de poluentes atmosféricos;
Q8) Exposição dos colaboradores.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

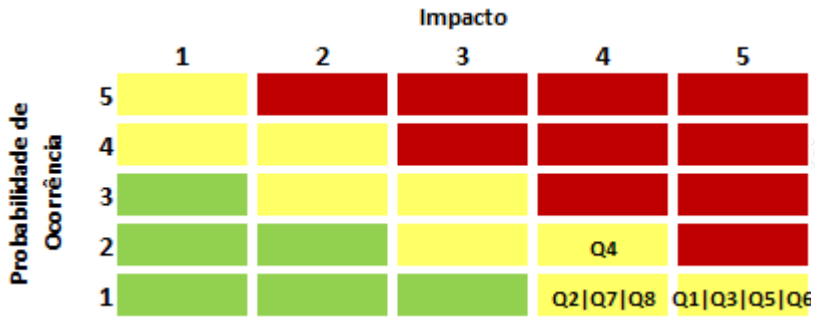

Figura 36 - Mapa de risco - departamento de Qualidade, Ambiente e Segurança

Figura 35 - Riscos e controlos existentes - departamento de Qualidade, Ambiente e Segurança

Destacam-se ainda as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Aumentar periodicidade das verificações/avaliações;
- Reforçar sensibilização dos colaboradores para regras de segurança;
- Instalação de barras protetoras na zona dos produtos químicos.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 9.

Departamento de Produção

Foram identificados os seguintes riscos:

A1) Restrição de fornecedores;
A2) Restrições na capacidade de produção devido ao equipamento;
A3) Restrições na capacidade de produção devido aos recursos humanos;
A4) *Outsourcing* da produção;
A5) Cumprimento dos requisitos legais;
A6) Cumprimento do *lead-time* de produção.

Após a sua identificação, os riscos foram avaliados quanto à sua probabilidade de ocorrência e quanto ao seu possível impacto na organização, o que resultou na construção de um mapa de risco. Recorrendo à avaliação realizada aos controlos existentes, foi também possível construir o gráfico *spider web* do departamento que põe em destaque as eventuais lacunas existentes entre riscos e controlos.

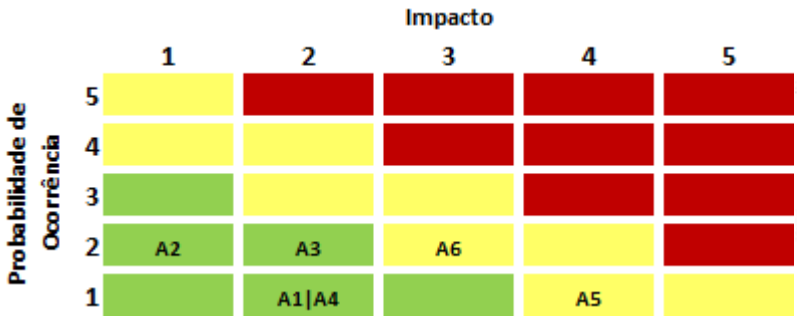

Figura 38 - Mapa de risco - departamento de Produção

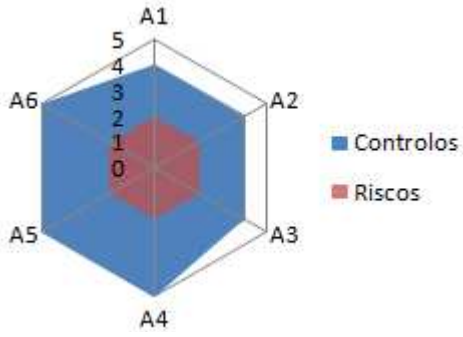

Figura 37 - Riscos e controlos existentes - departamento de Produção

Destacam-se ainda as seguintes propostas de controlos a implementar tendo em vista melhorar o controlo de alguns dos riscos identificados:

- Implementar sistema de automatização de gestão de stocks de matérias-primas;
- Adequar planos de formação.

A informação recolhida relativa a este departamento encontra-se sistematizada no anexo 10.

Após terem sido identificados os riscos de cada departamento e classificados quanto ao impacto e à sua probabilidade de ocorrência, é importante construir um mapa de risco global, de forma a perceber a posição da empresa relativamente ao risco. Desta forma, os riscos que surjam com maior impacto e maior probabilidade de ocorrência serão aqueles que, em princípio, deverão requerer uma maior atenção por parte da organização.

Apresenta-se de seguida na figura 39, o mapa de risco global da empresa:

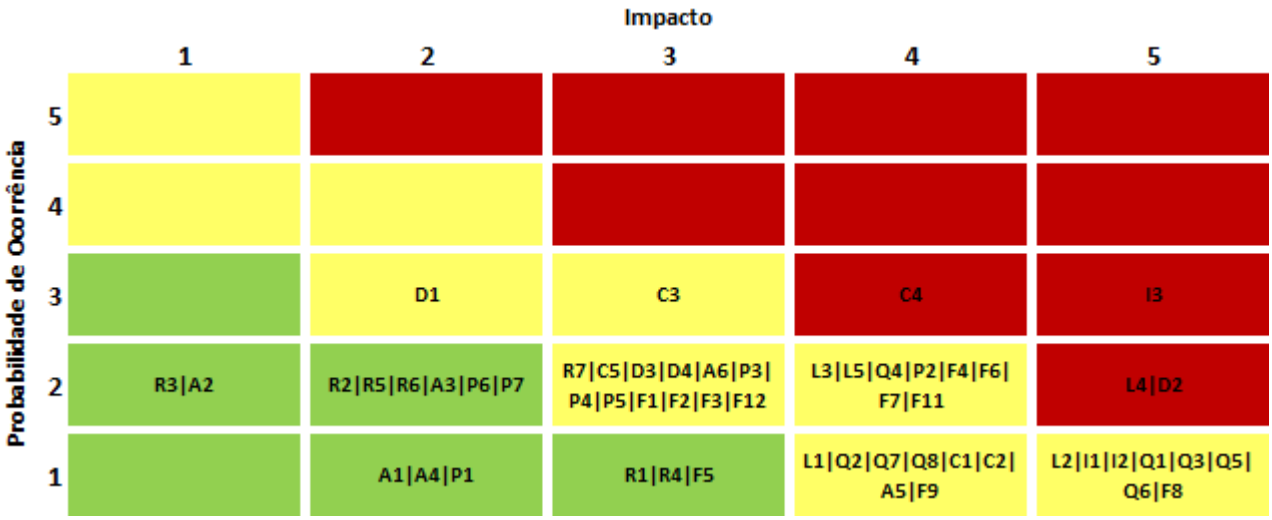

Figura 39 - Mapa de risco global da empresa

Através da análise do mapa de risco global da empresa e das lacunas existentes entre riscos e controlos identificáveis nos gráficos *spider web* construídos ao nível departamental é possível estabelecer um conjunto de prioridades de ação ao qual a organização deve atender, com o objetivo de realizar uma efetiva gestão de risco.

Deste modo, através do cálculo das diferenças entre a classificação final do risco e a classificação atribuída pelo risk owner ao controlo existentes, foi possível identificar as maiores necessidades de melhoria nos controlos dos seguintes riscos:

Figura 40 - Riscos e nível das lacunas identificadas

Riscos nos quais foram identificadas lacunas nos controlos existentes	
1. Presença *online* limitada (C3)	4
2. Incumprimento do prazo de entrega (L5)	3
3. Produtos sem sucesso comercial (D1)	3
4. Falha do sistema informático (D2)	2
5. Criação de Monos (L3)	2

Logo, importa referir as maiores lacunas identificadas anteriormente e explicitar o interesse de tratar esses riscos.

O risco que apresenta uma maior necessidade de intervenção é o risco (C3) - "Presença *online* limitada", o qual reflete a falta de novos conteúdos na página da internet da organização e um maior acompanhamento da mesma. Apesar de, recentemente, a empresa ter melhorado e refrescado o seu sítio da internet e de estar presente nas redes sociais, não existe um acompanhamento adequado destas plataformas digitais. A organização deve encetar esforços de melhoria nesta área de modo a potenciar a sua imagem e a imagem que transmite aos seus *stakeholders*.

Outro dos pontos que requer a atenção por parte da gestão da organização é o risco (L5) - "Incumprimento do prazo de entrega". Um dos objetivos expressos pela gestão de organização é o de "Melhorar os prazos de entrega das encomendas", o que revela a importância que o departamento de Logística atribui a este risco. Uma vez que não existe um acompanhamento do transporte/localização da mercadoria apenas é possível informar o cliente quanto ao dia de expedição. Deste modo, é de todo o interesse implementar um controlo para aferir o cumprimento dos tempos de entrega acordados com os transportadores e integrar o acompanhamento das mercadorias no sistema informático da organização.

Relativamente ao risco (D1) - "Produtos sem sucesso comercial", este aborda o risco de dispêndio de recursos pelo departamento de Desenvolvimento cujo retorno é limitado, devido ao desenvolvimento de produtos cuja aceitação pelo mercado é residual. Deste modo, a gestão da organização deve desenvolver esforços no sentido de atuar na fonte, isto é, desenvolver a função de Marketing de forma a adequar a investigação com o interesse dos clientes ou tendência de mercado.

Ainda ao nível do departamento de Desenvolvimento foi identificado outro risco ("Falha do sistema informático" - (D2)) que necessita de intervenção no sentido de o mitigar. Dado que grande parte do trabalho realizado pelo departamento baseia-se num sistema específico de produção de amostras, quando, por algum motivo, o programa colapsa, parte da informação sobre a qual os colaboradores estavam a trabalhar perde-se e o trabalho que estavam a desenvolver fica suspenso até à resolução do problema. Assim, importa substituir este programa por um novo sistema informático com maior capacidade e novas funcionalidades.

Outros dos riscos identificados neste estudo que é passível de ser mitigado é o risco de "Criação de Monos" (L3). Este evento tem impacto nas operações do Departamento de Logística na medida em que a sua ocorrência significa redução do

espaço disponível no armazém e um dispêndio de recursos na sua fabricação, armazenagem e abate dos monos. Deste modo, e dado que no setor da moda é inevitável gerar monos, deverá ser implementada uma política de venda e abate de monos, de forma a reduzir o seu impacto nas operações logísticas.

iv. Monitorização e Revisão

Relativamente à fase da monitorização e revisão dos controlos e dos riscos identificados, esta deve ser contínua de modo a manter o modelo atualizado. Caso não haja capacidade para esta monitorização e revisão contínua, poderá ser realizada periodicamente ou sempre que se entender que existe uma desadequação do modelo ou uma alteração das circunstâncias.

Se se verificar que existe um desalinhamento entre os resultados obtidos e alguma das fases anteriores, poderá fazer sentido "reiniciar" o modelo através de uma nova análise da envolvente interna e externa e prosseguir com as seguintes fases.

Uma vez que o intento deste modelo é o de propor um modelo de gestão de risco, não foi possível por em prática a fase da monitorização e da revisão. No entanto, se forem implementados planos de ação com o objetivo de aplicar alguns dos controlos propostos fará sentido rever a classificação atribuída aos controlos.

Esta fase poderá ser aplicada quando efetivamente a gestão de topo decidir avançar com a aplicação o modelo proposto ou outra qualquer metodologia de gestão de risco.

v. Informação e Formalização

Através da fase "Informação e Formalização", o centro do modelo, foi possível recolher informação e identificar os riscos, controlos existentes e controlos a implementar.

Posteriormente, procedeu-se também à formalização e entrega desta informação, em suporte digital, para estudo por parte da gestão da organização. Este estudo representou um passo importante na definição de uma política de gestão de risco na organização, na medida em que contribuiu para uma consolidação e análise das principais dificuldades existentes e identificação de oportunidades de melhoria.

5.4. Monitorização e Revisão do Framework e a Melhoria Continua do Framework

Segundo a ISO31000, os dois últimos componentes que devem constituir um modelo de gestão de risco são a “Monitorização e Revisão do Framework” e a “Melhoria Contínua do Framework”. Estas duas fases asseguram, por um lado, que a gestão de risco é efetiva e continua a suportar a performance organizacional, e, por outro lado, a tomar decisões que permitam melhorar o modelo adotado e a cultura de risco existente na organização.

Contudo, não foi possível observar na prática estas duas fases em funcionamento, uma vez que, tal como referido anteriormente, este estudo trata-se apenas de uma proposta de implementação de um modelo de gestão de risco, cuja aplicação e posterior monitorização e revisão, será implementada posteriormente pela gestão da organização.

VI. Conclusões

A aplicação de novas metodologias de gestão de risco nas organizações revela-se sempre um novo desafio. No que se refere a este estudo em concreto, apesar das dificuldades enfrentadas, foi compensador poder dar um contributo para a organização onde desenvolvia funções e, acima de tudo, conseguir desenvolver conhecimentos numa área tão interessante e atual como é a área da gestão de risco.

Relativamente aos objetivos deste estudo, foi possível concretizar todos eles ao nível da recolha dos dados necessários para elaborar uma proposta do que poderá ser, no futuro, o modelo de gestão de risco da organização. Conseguiu-se obter informação relativamente aos riscos a que a empresa se encontra sujeita e, também, dos controlos implementados para mitigar o efeito desses riscos na atividade da organização. Foi possível ainda, identificar melhorias passíveis de serem aplicadas aos controlos existentes e a implementação de novos controlos. Esta informação gerada foi agregada e formalizada em tabelas (anexos 2 a 10) o que permitiu à organização dispor de um ficheiro integrado sobre os seus riscos e os controlos e das respetivas avaliações, cuja consulta e revisão pode ser efetuada de forma rápida e eficaz.

No que se refere aos contratempos encontrados neste estudo, um deles prendeu-se com a dificuldade que alguns dos interlocutores demonstraram na identificação de eventos/riscos. Esta dificuldade patente poderá estar intrinsecamente ligada à definição de risco apresentada pela ISO31000 que define risco como "o efeito da incerteza nos objetivos", isto é, perante uma definição demasiado larga, torna-se difícil, para o entrevistado, conseguir perceber o objetivo do entrevistador. Esta dificuldade é ainda maior quando a questão é levantada a *risk owners* que não lidam habitualmente com os conceitos de risco. Ou seja, as entrevistas realizadas com os *risk owners* dos Departamento Financeiros e do Departamento de Qualidade, Ambiente e Segurança foram realizadas com relativa facilidade e rapidez, ao passo que algumas das entrevistas realizadas noutros departamentos dependeram muito sensibilidade e da "tentativa e erro" por parte do entrevistador na identificação dos potenciais riscos. Deste modo, e uma vez que a fase da "Informação e Formalização" é transversal a todas as outras etapas do modelo, poderia ter sido realizada uma breve formação e exposição em conjunto aos *risk owners* acerca da temática do risco e da gestão de risco, para que, posteriormente na fase da "Determinação dos Riscos", os eventos/riscos fossem

identificados com maior facilidade e com menor dispêndio de recursos. Esta preparação vai ao encontro da figura 6, referida anteriormente aquando da exposição da ISO31000, a qual pressupõe uma fase contínua de "*Communication and Consultation*" nos processos de gestão de risco, de modo a mitigar possíveis equívocos. Uma das vantagens da realização desta reunião geral dos *risk owners*, seria a promoção de uma discussão e adoção de uma linguagem de risco comum, proporcionando ao mesmo tempo, os primeiros passos para a criação de uma cultura de risco e para o desenvolvimento da comunicação inter-departamental nos processos de gestão de risco.

Apesar de não terem sido identificados claramente pelos *risk owners* riscos transversais aos departamentos, conseguiu-se percecionar a existência de riscos que são transversais a toda a organização como é exemplo a dependência do sistema SAP, a possibilidade de saída de elementos centrais dos departamentos ou a ameaça de saída de informação considerada confidencial. No entanto, em termos formais, ainda existe uma visão muito departamentalizada na empresa, no sentido de se considerarem estes riscos como responsabilidade do departamento a que dizem respeito. Certos riscos identificados, como o não cumprimento do tempo de entrega ao cliente da sua encomenda ou a existência de atrasos na sua produção, já estão incutidos ao longo de todo o processo (ver riscos C2, P2, L5 e A6). Deste modo, cabe à gestão de topo da organização e ao modelo de gestão de risco em particular, atingir o mesmo nível de sensibilidade e de tratamento interdepartamental para lidar com riscos organizacionais como o da fuga de informação considerada confidencial.

Outra das questões levantadas por este estudo prende-se com a verificação do alinhamento existente entre o perfil de risco dos *risk owners* e o perfil de risco da gestão de topo da organização. A entrevista final com um dos administradores da organização, no sentido de se ajustar a classificação dos riscos e dos controlos identificados, permitiu perceber que parte da classificação atribuída aos riscos pelos *risk owners* estava sobrevalorizada. Este desajustamento poderá resultar de uma visão muito mais departamentalizada destes na classificação dos riscos, em contraponto com um maior conhecimento do negócio e uma perspetiva global da organização e dos riscos a que esta está sujeita por parte da gestão de topo, o que levou a uma nivelação "por baixo" do nível de impacto ou probabilidade de ocorrência de alguns riscos. Outra análise que poderá ser efetuada a partir desta revisão de classificações dos riscos, poderá estar relacionada com um maior apetite pelo risco por parte da gestão de topo, ao passo que, a

responsabilização direta dos *risk owners* pelos riscos, tenderá a criar uma maior aversão ao risco por parte destes.

VII. Limitações e Questões de Investigação Futura

7.1. Limitações do Estudo

Ao nível das limitações encontradas, a inexistência de um departamento de auditoria interna não permitiu tirar qualquer tipo de conclusão quanto ao possível papel a desempenhar pelo auditor interno, no processo de implementação de um modelo de gestão de risco e quanto à conservação (ou não) dos valores da independência e da objetividade.

Uma das limitações que também se poderá apontar a este estudo decorre do facto de a elaboração do mesmo e da proposta de modelo de gestão de risco na organização ter sido somente realizada com base nas orientações da ISO31000 e nas recomendações referidas pelos outros modelos de gestão de risco abordados na revisão de literatura, não tendo havido lugar à intervenção de um agente com experiência na implementação deste tipo de metodologias.

Apesar de este estudo se ter limitado a propor um modelo de gestão de risco para a organização e não ter implementado uma metodologia integrada de gestão de risco, a avaliação realizada permitiu verificar a existência de controlos e de uma preocupação por parte dos *risk owners* e da gestão de topo em lidar com os riscos que afetam a organização.

Deste modo, as conclusões retiradas neste estudo devem ser entendidas à luz das limitações anteriormente citadas e de acordo com a especificidade do caso de estudo abordado, não se podendo, deste modo, fazer qualquer tipo de generalização por exemplo, ao nível do setor ou da dimensão da organização.

7.1. Questões de Investigação Futura

Ao longo da elaboração deste estudo levantaram-se questões que poderão fazer sentido num estudo mais aprofundado.

Poderia ser interessante desenvolver uma abordagem quantitativa na avaliação dos riscos identificados numa organização através da elaboração de estimativas de probabilidade de ocorrência e do cálculo de intervalos de impacto financeiro derivados da ocorrência de eventos geradores de risco. Durante a pesquisa de informação para a preparação da revisão de literatura, não foi possível encontrar estudos que utilizassem uma metodologia quantitativa na avaliação dos riscos de uma organização.

Uma outra sugestão útil para uma potencial investigação futura passaria pelo estudo dos eventuais ganhos conseguidos e das melhorias verificadas nos controlos e no desempenho da organização, ou por outro lado, do surgimento de eventuais problemas e custos não esperados com a aplicação de modelos de gestão de risco, num cenário de pós-implementação de uma gestão de risco integrada no modelo de negócio.

VIII. Bibliografia

- Anand, Sanjay (2007), Essentials of Sarbanes-Oxley, Editor John Wiley & Sons, Ltd, Cap.3, ISBN 978-0-470-05668-4;
- Amador, João; Opromolla, Luca (2009), "*Textiles and Clothing Exporting Sectors In Portugal - Recent Trends*", Boletim Económico, Banco de Portugal;
- Associação Têxtil e Vestuário de Portugal (2013), Boletim da Indústria Têxtil e Vestuário (2013);
- Berkowitz, Sandra (2001), "*Enterprise Risk Management and The Healthcare Risk Manager*", Journal of Healthcare Risk Management, Vol.21, disponível em http://onlinelibrary.wiley.com/doi/10.1002/jhrm.5600210106/pdf;
- Bernstein, Peter. (1996), Against the Gods: The Remarkable Story of Risk, New York: Jonh Wiley and Sons, Inc.;
- Centro de Inteligência Têxtil (CENIT, 2009), Análise da Indústria Têxtil e Vestuário no Norte de Portugal e Galiza: Consolidação da Complementaridade do "Cluster" Transfronteiriço na Euroregião, disponível em http://www.euroclustex.eu/fotos/editor2/analise_da_industria_textil_e_vesturario_de_portugal_e_galiza.pdf;
- Cenker, William J. e Nagy, Albert L. (2004),"*Section 404 implementation: Chief audit executives navigate uncharted waters*", Managerial Auditing Journal, Vol. 19 Iss: 9 pp. 1140 - 1147;
- Comissão do Mercado de Valores Mobiliários (CMVM, 2005), Recomendações da CMVM sobre o Governo das Sociedades Cotadas, disponível em www.cmvm.pt/CMVM/Recomendacao/Recomendacoes/Soccot/Soccot_Nov2005/Documents/43d104c4a8434d1ea100c3565316970erecomendacoesNov2005.pdf;
- Committee of Sponsoring Organizations (COSO, 1992), Internal Control - Integrated Framework;
- Committee of Sponsoring Organizations (COSO, 2004), Enterprise Risk Management - Integrated Framework, Executive Summary;
- Committee of Sponsoring Organizations (COSO, 2012a), Understanding and Communicating Risk Appetite;
- Committee of Sponsoring Organizations (COSO, 2012b), Risk Assessment in Pratice;

- Committee of Sponsoring Organizations (COSO, 2013), 2013 Internal Control - Integrated Framework;
- De la Rosa, Sean (2007), "*Moving Forward with ERM*", Internal Auditor, Vol.64, Iss:3, pp.50-53;
- Damodaran, Aswath (2008), "*Strategic risk taking: a framework for risk management*", New Jersey: Wharton School, Cap. 1, pp. 3-10, ISBN 978-0-13-704377-4;
- European Foundation for Quality Management (2005), EFQM Framework for Risk Management, European Foundation for Quality Management, Brussels;
- FERMA (2003), Norma de Gestão de Riscos, Federation of European Risk Management Associations;
- Ghauri, Pervez e Grønhaug, Kjell (2010), "*Data Collection*", Research Methods in Business Studies, Fourth Edition, Cap. 8, pp. 103-137;
- Grant Purdy (2010),"*ISO 31000:2009 - Setting a New Standard for Risk Management*", Risk Analysis, Vol. 30, No 6, pp 881-886;
- Hodges, Alan (2000), "*Emergency Risk Management*", Risk Management, Vol. 2, No. 4, pp. 7-18;
- ISO31000, Risk management - Principles and guidelines;
- ISO Guide 73:2009, Risk management - Vocabulary;
- Kallman, James e Maric, Romy (2004), "*A Refined Risk Management Paradigm*", Risk Management, Vol. 6, No. 3, pp. 57-68;
- Miller, Kent D. (1992), "*A Framework for Integrated Risk Management in International Business*", Journal of International Business Studies, Vol. 23, No. 2 (2nd Qtr., 1992), pp. 311-331;
- Moore, P.G. (1983), "*The Business of Risk*", Cambridge University Press, Cambridge;
- PriceWaterhouseCoopers (PWC, 2010), Managing Risk - Internal Controls for Private companies, disponível em http://www.pwc.com/en_US/us/private-company-services/assets/pcs-managing-risk.pdf;
- Roger Williams, Boudewijn Bertsch, Barrie Dale, Ton van der Wiele, Jos van Iwaarden, Mark Smith, Rolf Visser, (2006),"*Quality and risk management: what are the key issues?*", The TQM Magazine, Vol. 18 Iss: 1 pp. 67 – 86;

- Standard&Poor's (2008), "*Entreprise Risk Management: Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings*", S&P press release, 7 de maio de 2008;
- Stewart, Jenny e Subramaniam, Nava (2010); "*Internal audit independence and objectivity: emerging research opportunities*", Managerial Audit Journal, Vol.25, No.4, pp.328-360;
- Tarantino, Anthony (2006), Manager's guide to compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB A-123, ASX 10, OECD principles, Turnbull guidance: best practices and case studies, Editor John Wiley & Sons, Ltd, Cap.2, ISBN 0-471-79257-8;
- The Institute of Internal Auditors (IIA) (2009), "*IIA Position Paper: The role of internal auditing in enterprise-wide risk management*" disponível em https://na.theiia.org/standards-guidance/recommended-guidance/Pages/Position-Papers.aspx;
- The Institute of Internal Auditors (IIA) e The Risk & Insurance Management Society (RIMS) (2012), "*Risk Management and Internal Audit: Forging a Collaborative Alliance*" disponível em https://na.theiia.org/news/press-releases/Pages/Risk-Management-and-Internal-Audit-Forging-a-Collaborative-Alliance.aspx
- The Institute of Internal Auditors Research Foundation (IIARF) (2011), "*Internal Auditing's Role in Risk Management*" disponível em http://www.oracle.com/us/solutions/corporate-governance/ia-role-in-rm-345774.pdf;
- Thompson, Rose M. (2013), "*A Conceptual Framework of Potential Conflicts with the Role of the Internal Auditor in Enterprise Risk Management*", Accounting and Finance Research, Vol. 2, No. 3, disponível em http://dx.doi.org/10.5430/afr.v2n3p65;

Informação sobre entidades:

- COSO - About us: http://www.coso.org/aboutus.htm
- FERMA - What is FERMA: http://www.ferma.eu/about/mission-and-objectives/what-is-ferma
- ISO - About ISO: http://www.iso.org/iso/home/about.htm
- The Institute of Internal Auditors (IIA) - www.theiia.org

A gestão de risco nas quatro maiores cotadas portuguesas segundo a capitalização bolsista (sites acedidos no dia 03/01/13):

- Portugal Telecom: http://www.telecom.pt/InternetResource/PTSite/PT/Canais/Investidores/GovernodaSociedade/Risco/modelo/introducao.htm
- Galp: http://www.galpenergia.com/PT/investidor/GovernoCorporativo/GestaoRisco/Paginas/GestaoRisco.aspx
- Jerónimo Martins: http://www.jeronimomartins.pt/investidor/governo-da-sociedade/orgao-social/comissao-de-auditoria.aspx
- EDP: http://www.edp.pt/pt/aedp/governosocietario/gestaodorisco/Pages/RiskManagement.aspx

IX. Anexos

Anexo 1 - Principais cliente e fornecedores do setor têxtil e do vestuário

Clientes / Destino	2011	2012	Δ%	% Total (2012)
Espanha	1.248.325	1.288.907	3,3%	31,2%
França	579.131	555.443	-4,1%	13,4%
Alemanha	408.470	347.963	-14,8%	8,4%
Reino Unido	341.007	361.269	5,9%	8,7%
Itália	247.341	206.716	-16,4%	5,0%
EUA	155.245	182.873	17,8%	4,4%
Holanda	150.234	140.202	-6,7%	3,4%
Bélgica	107.543	98.048	-8,8%	2,4%
Angola	62.792	78.697	25,3%	1,9%
Suécia	84.362	73.092	-13,4%	1,8%
Outros	767.639	770.006	0,3%	18,6%
UE27 - Extra	656.319	704.023	7,3%	17,0%
UE27 - Intra	3.495.770	3.426.221	-2,0%	83,0%
Total	**4.152.089**	**4.130.244**	**-0,5%**	**100,0%**

Figura 41 - Principais clientes do setor têxtil e do vestuário
Fonte: ATP (2013)

Fornecedores / Origem	2011	2012	Δ%	% Total (2012)
Espanha	1.240.180	1.125.834	-9,2%	37,0%
Itália	449.628	427.301	-5,0%	14,0%
França	267.522	257.120	-3,9%	8,4%
Alemanha	253.128	218.033	-13,9%	7,2%
China	221.384	181.203	-18,1%	6,0%
Holanda	138.848	130.660	-5,9%	4,3%
Índia	165.538	118.450	-28,4%	3,9%
Bélgica	106.901	116.647	9,1%	3,8%
Reino Unido	70.811	65.801	-7,1%	2,2%
Irlanda	51.155	61.718	20,6%	2,0%
Outros	422.522	341.054	-19,3%	11,2%
UE27 - Extra	702.444	548.301	-21,9%	18,0%
UE27 - Intra	2.685.172	2.496.423	-7,0%	82,0%
Total	**3.387.616**	**3.044.724**	**-10,1%**	**100,0%**

Figura 42 - Principais fornecedores do setor têxtil e do vestuário
Fonte: ATP (2013)

Anexo 2 - Informação recolhida no Departamento de Recursos Humanos

Departamento: Recursos Humanos

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(R1) Contratação Inadequada	Contratação de colaboradores cujo perfil não se adequa à tarefa em questão	1	3	2	Partilhar	Processo de seleção orientado para as competências exigidas; período experimental	4	-
(R2) Saída de elementos-chave da organização	Saída de colaboradores da organização com elevado know-how e/ou conhecimento do negócio	2	2	2	Eliminar	Acompanhamento pelos supervisores dos colaboradores; Pacote salarial e de benefícios acima da média do mercado	5	Realizar inquéritos de satisfação aos colaboradores
(R3) Acidentes de trabalho	Ocorrência de acidentes que limitem as capacidades dos colaboradores, mesmo que temporariamente	2	1	2	Reduzir	Regras de segurança e de utilização dos equipamentos de segurança individuais e coletivos; Formação de Integração - módulos de Saúde, Higiene e Segurança no Trabalho	4	Melhoria contínua dos Equipamentos de Proteção Individuais e Coletivos; Criação de uma cultura de segurança
(R4) Formação inadequada	Necessidade de dotar os colaboradores de formação específica e de gerir expectativas decorrentes da formação oferecida	1	3	2	Reduzir	Formações na qual o formando classifica a formação e o supervisor avalia o impacto da mesma; diagnóstico de necessidades (formação taylor made)	4	-
(R5) Comunicação deficitária com colaboradores	Percepção incorrecta pelos colaboradores dos objectivos da organização e da importância das tarefas a desempenhar	2	2	2	Eliminar	Publicações internas; Questionário de satisfação sobre a comunicação interna	3	Definição pela gestão de topo de uma plano de comunicação interno
(R6) Subcontratação de pessoal	Dificuldades na integração e alinhamento dos colaboradores com os valores da organização	2	2	2	Reduzir	Formação de integração de todos os colaboradores da organização; Divulgação dos valores da empresa	4	-
(R7) Absentismo	Faltas e/ou atrasos dos colaboradores ao horário de trabalho previsto	2	3	3	Reduzir	Relógio de ponto	5	Implementar sistema de incentivo/ penalização

Departamento: Comercial e de Marketing

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(C1) Erros de transmissão de informação	Ocorrência de erros no registo de encomendas (preços, cores ou quatidades) e erros por parte dos agentes na transmissão de encomendas de clientes	1	4	3	Reduzir	Confirmação das encomendas com o cliente	3	Melhorar processo de controlo do SI; Adopção de um formulário padrão de encomenda
(C2) Incumprimento de prazos	Incumprimento do prazo de entrega de mercadorias acordado com o cliente	1	4	3	Reduzir	Controlo informático/ automático de datas previstas de produção	5	Implementação de APO (Advanced Planning Optimizer), ferramentas avançadas de controlo de operações
(C3) Presença online limitada	Falta de manutenção e actualização de conteúdos na internet e nas redes sociais	3	3	3	Aceitar	Verificação esporádica da plataforma/páginas online	2	Implementação de um sistema de alerta de desatualização/ inactividade das plataformas digitais
(C4) Perda de informação sobre mercados	A documentação e o acompanhamento do mercado está centrada nos gestores de mercado	3	4	4	Aceitar	Não existe	-	Desenvolver a função de Marketing (criação de um sistema de registo de informações sobre o mercado)
(C5) Desadequação de proposta feitas a clientes	Risco de apresentar uma proposta de valor desadequada às expectativas do cliente	2	3	3	Reduzir	Supervisão do processo pelo responsável da área	2	Criação de um guia de procedimento formalizado de contacto com clientes

Anexo 4 - Informação recolhida no Departamento de Planeamento e Compras

Departamento: Planeamento e Compras

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação final		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(P1) Quebra de encomenda	Quebra do contrato de uma encomenda confirmada	1	2	2	Reduzir	Documento Venda / Contrato; Registo informático	5	Melhorar a proximidade na relação cliente-empresa para antever a ocorrência deste
(P2) Incumprimento de prazos de entrega	Problemas na entrega do tecidos nos prazos acordados devido a problemas de qualidade final ou avarias	2	4	3	Reduzir	Indicadores de desempenho (nível de execução de encomendas ao nível da produção); Planos de Ação	3	Melhorias contínuas no processo de produção
(P3) Aprovisionamento incorreto de Matérias-Primas e Stocks	Risco associado à falta de matérias-primas necessárias ao processo de produção devido ao incorrecto planeamento/ consumo inesperado; Riscos associados à existência de stock elevado ou stock insuficiente devido à ineficiencia do processo de planeamento	2	3	3	Reduzir	Plano de Compras; Pedido de previsões; Gestão de stocks	4	Obtenção de Previsões de vendas por parte de agentes/comerciais
(P4) Lançamento de Telas e/ou Tecidos Acabados	Risco de produção de telas e tecidos acabados cuja venda não está assegurada ou não é imediata	2	3	3	Reduzir	Planos de Lançamentos com base em previsões	4	Obtenção de previsões de vendas por parte de agentes/comerciais
(P5) Não qualidade de fornecedores	Não entrega atempada ou nas quantidades necessárias por parte dos fornecedores ou a ocorrência de problemas com a subcontratação da produção	2	3	3	Partilhar	Controlo SAP das entregas dos fornecedores; Penalizações acordadas nos contratos celebrados com fornecedores	4	Aumento de informação regular por parte dos fornecedores
(P6 e P7) Falha de Informação	Risco de falta de precisão dos valores constantes nas listas técnicas do produto relativamente a níveis de defeituoso e contração de tela/ tecido	2	2	2	Reduzir	Controlo mensal ao defeituoso e contração do tecido	4	Atualização das fichas técnicas; Reforçar validação dos parâmetros no momento da criação dos materiais
	Mapas de posição de encomendas do cliente com informação incorrecta	2	2	2	Reduzir	Mapa de controlo de encomendas de produção e modelagens	4	Melhorar o reporting por parte da produção

Anexo 5 - Informação recolhida no Departamento Financeiro

Departamento: Financeiro

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação Final		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(F1) Redução das linhas de financiamento	Redução do crédito / não renovação de linhas de crédito atuais da empresa	2	3	3	Aceitar	Reuniões e contactos periódicos com a banca	3	Diversificar as fontes de financiamento
(F2) Volatilidade do preço das matérias primas	Risco de Preço devido à escassez de Materias-Primas	2	3	3	Reduzir	Contratos de Continuidade; Acompanhamento dos mercados de commodities; Consultoria externa especializada	2	Centralização de áreas de compras. Planeamento integrado (desenvolvimento-comercial-produção-planeamento-compras)
(F3) Risco de Crédito ao cliente	Risco de incumprimentos ou recebimento tardio por parte dos clientes	2	3	3	Partilhar	Seguro e Consultoria de Crédito; Controlo de Crédito; Mapas de Antiguidade de Saldos; SAP (Controlos de Limites de Crédito); Informação de crédito de provider externo	5	Auditar o processo de concessão descontos financeiros
(F4) Não fiabilidade da Demonstrações Financeiras	Risco de produção de informação financeira não fiável devido a erros ou a produção tardia e/ou incompleta da informação financeira	2	4	3	Reduzir	Análise por parte dos responsáveis da Área (TOC e CFO); Análise do Controlo de Gestão; Análise por parte do ROC; Controlo Automático via SAP	5	Aumentar a automatização da produção das demonstações financeiras a partir do SAP
(F5) Não cumprimento das obrigações fiscais	Risco associado ao cumprimento dos prazos legalmente exigidos bem como risco de falta de informação sobre as alterações fiscais	1	3	2	Partilhar	Informação prestada pelo ROC; Análise por parte do responsável da Área (TOC)	4	Recurso a Consultoria Fiscal
(F6) Não fiabilidade dos Indicadores de Gestão	Risco associado à incorrecta definição e cálculo dos indicadores do controlo de gestão e eventuais problemas de interpretação dos mesmos	2	4	3	Reduzir	Validação do resultado dos indicadores por parte do responsável da àrea e por parte das àreas afectas pelos mesmos	5	Automatização da produção dos indicadores atraves do sistema SAP

Departamento: Financeiro

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação Final		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(F7) Fuga de Informação Sensível	Risco de fuga de informação atraves do colaboradores da área dada a fácil acessibilidade a toda a informação financeira	2	4	3	Reduzir	Sensibilização dos colaboradores quanto ao dever de confidencialidade; Exigência de colaboradores com a característica de discrição nos processos de recrutamento da àrea	4	Estabelecer Código de Ética; Reduzir a escrito o dever de confidencialidade dos colaboradores
(F8) Utilização de plataformas online de gestão bancária/tesouraria	Risco de apropriação de informação e dados bancários por parte de piratas informáticos	1	5	3	Reduzir	Reconciliações Bancárias; Controlo pela contabilidade das contas de Terceiros; Necessidade de assinaturas autorizadas para movimentação de fundos; *Software de internet security*	5	Realização de auditoria periódicas
(F9 e F10) Processamento de pagamentos	Risco proveniente do tratamento manual de pagamentos a fornecedores (erros)	1	4	3	Reduzir	Supervisão superior do processo de pagamentos. Acompanhamento de contas correntes pela Tesouraria e pela Contabilidade	4	Automatização parcial do processo de pagamentos
	Risco de incumprimentos de prazos de pagamento a fornecedores	2	4	3	Reduzir			Aumento do controlo sobre os pedidos de compra e de faturas em conferência
(F11) Assunção de plafonds internos de crédito aos clientes	Risco associado à realização de negócios com cliente não cobertos pelo seguro de crédito	2	4	3	Aceitar	Monitorização da concessão de plafons por parte da área financeira; Informação de provider externo	5	Definição de uma política formal de crédito
(F12) Risco cambial e risco de taxa de juro	Risco associado à variação das taxas de câmbio e de juro dos mercados onde a empresa opera	2	3	3	Reduzir	Monitorização do nível de exposição ao risco; Consultoria externa especializada	3	Estabelecimento de um plano de compras em divisas não euro

Anexo 6 - Informação recolhida no Departamento de Sistemas de Informação

Departamento: Sistemas de Informação

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(I1) Incêndio	Incêndio com destruição de equipamentos críticos para o negócio	1	5	3	Reduzir	Testes periódicos aos equipamento de combate a fogo	3	Sistemas Anti-Fogo
(I2) Perda de Dados	Perda de dados críticos para o negócio	1	5	3	Reduzir	Backups calendarizados; Testes de recuperação	3	Sistema de Backups
(I3) Furto de Informação	Acesso não autorizado a informação confidencial ou crítica de negócio	3	5	4	Reduzir	Auditorias de acesso	5	Estabelecer níveis de autorizações

Departamento: Logística

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(L1) Contaminação de produtos	Contaminação de matérias primas e de prdutos em curso de fabrico no transporte dos mesmos entre as diferentes fases de produção	1	4	3	Reduzir	Verificação pelos motoristas; Salas de controlo de Poeiras	3	-
(L2) Furto de mercadorias	Risco de furto de mercadorias dos armazéns de produtos acabados	1	5	3	Partilhar	Utilização do sistema de inventário permanente; Inventário anual; Controlo no momento da carga	2	Implementação de um sistema de video vigilância no local de carga/ descarga e armazéns; Verificaçao da saída de cargas pela portaria
(L3) Criação de Monos	Ocupação do armazem com a stockagem de produtos cuja venda é de dificil concretização	2	4	3	Reduzir	Inventário anual	1	Implementar política comercial de vendas/abate de monos
(L4) Aumento de Custos de Transporte	Risco da utilização de um meio de entrega incorreto	2	5	4	Reduzir	Conhecimento das modalidades de envio; Controlo das operações	5	Carregamento em SAP da informação sobre transitários e custos de envio
(L5) Incumprimento do prazo de entrega	Entrega das mercadorias para além do prazo acordado	2	4	3	Reduzir	Não existem	-	Criação de um indicador sobre a pontualidade da entrega de encomendas; Acompanhamento online das encomendas para informar o cliente

Anexo 8 - Informação recolhida no Departamento de Desenvolvimento

Departamento: Desenvolvimento

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(D1) Produtos sem sucesso comercial	Dispêndio de recursos no desenvolvimento de produtos sem sucesso no mercado	3	2	3	Aceitar	Não existem	-	Desenvolvimento da função de marketing
(D2) Falha do sistema informático	A actividade desenvolvida por este departamento baseia-se num programa específico de produção de amostras	2	5	4	Reduzir	Back-up da informação existente	2	Substituição do software por um sistema mais recente e com maior capacidade
(D3) Disparidade no custeio teórico/real	Risco do custeio teórico de um produto diferir do custeio real, inviabilizando a sua produção	2	3	3	Aceitar	Simulação do custeio	3	Refinar o sistema de custeio
(D4) Incoerência dos processos desenvolvimento /produção	Dificuldade em extrapolar os resultados obtidos na fase de desenvolvimento ao nível da validação do produto	2	3	3	Aceitar	Reuniões de validação de produto	3	Criação de uma biblioteca de conhecimento que permita prever e antecipar eventuais problemas no desenvolvimento

Departamento: Qualidade, Ambiente e Segurança

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(Q1) Contaminação dos lençóis freáticos	Risco de infiltração do efluente no rio	1	5	3	Reduzir	Manutenção preventiva atraves da verificação do estado das estruturas do tanque de homogeneização	4	Verificar com maior periodicidade o estado do tanque de homogeneização; Reforçar estrutura das paredes
(Q2) Ruido Ambiental para o exterior	Poluição sonora libertada para o meio envolvente	1	4	3	Reduzir	Aplicação de atenuadores de ruido no parque de maquinas; Isolamento do tanque de efluente de agua quente	5	Avaliação de Ruido Ambiental
(Q3) Utilização de água imprópria para consumo	Recurso a água proveniente de captações de água impropria para consumo	1	5	3	Reduzir	Sistema de tratamento de àgua (controlador com cloro)	2	Ligação das àguas para consumo humano à rede pública
(Q4) Derrame de produtos químicos	Libertação/ vazamento de produtos químicos para o meio envolvente	2	4	3	Reduzir	Formação e Segurança; Bacias retenção; Piso impremeável; Produtos absorventes	5	Reforçar formação/ sensibilização dos colaboradores na condução de empilhadores; Instalação de barras protectoras na zona dos contentores de Produtos Químicos que impeçam o choque dos empilhadores com os contentores
(Q5 e Q6) Incêndio	Ocorrência de um incêndio na àrea da Tecelagem (teares)	1	5	3	Reduzir	Limpeza assídua das centrais de ar condicionado. Meios/equipas de intervenção para atuar em situações de emergência.	3	Alteração do *lay-out* do parque de máquinas da tecelagem Instalação de sistemas de deteção/extinção de incêndio.
	Ocorrência de um incêndio na Gaseadeira	1	5	3		Sistema de deteção insuficiente, próximo da saída da máquina.	2	Detetor precoce da fratura da costura na gaseadeira
(Q7) Emissão de poluentes atmosféricos	Emissões decorrentes da combustão de gases	1	4	3	Reduzir	Monitorização dos efluentes gasosos	4	Monitorização dos efluentes gasosos
(Q8) Exposição dos colaboradores	Inalação pelo colaborador de poeiras, gases e vapores; Ruido Ocupacional	1	4	3	Reduzir	Utilização dos Equipamentos de Protecção Individual (máscara, protectores auriculares)	5	Reforçar a sensibilização para o uso dos Equipamentos de Proteção Individual

Anexo 10 - Informação recolhida no Departamento de Produção

Departamento: Produção

Identificação de Eventos		Avaliação do Risco			Resposta ao Risco	Atividades de Controlo		
Evento	Descrição	Probabilidade de Ocorrência	Impacto	Classificação		Controlos Existentes	Classificação do Controlo	Descrição do Controlo a Implementar
(A1) Restrições de fornecedores	Risco associado às restrições ao nível da capacidade de resposta dos fornecedores de produtos químicos	1	2	2	Reduzir	Conhecimento de previsões de clientes	4	Consignação de matérias-primas; Implementar em SAP um sistema de ordens de compra mediante a necessidade de Materias-Primas
(A2 e A3) Restrições de capacidade de produção	Restrições da capacidade de produção ao nível do equipamento produtivo	2	1	2	Aceitar	Recurso à subcontratação de produção	4	-
	Restrições da capacidade de produção ao nível do disponibilidade de Recursos Humanos (preparação de equipas / formação)	2	2	2	Reduzir	Recurso a trabalho temporário	4	Adequação dos planos de formação
(A4) *Outsourcing* da produção	Problemas de qualidade do produto final devido à subcontratação da produção	1	2	2	Aceitar	Acompanhamento da produção subcontratada; Elaboração de testes preliminares; Transferência do Know-How de	5	-
(A5) Cumprimento dos requisitos legais	Requisitos legalmente exigidos ao nível das práticas ambientais e laborais	1	4	2	Aceitar	Certificação pelo Instituto Português da Qualidade (ISO 9000 e ISO 14000); Recurso a fornecedores certificados	5	-
(A6) Cumprimento do *lead time* da produção	Riscos associados ao problema da sobreprodução (encomendas solicitadas superiores à capacidade de produção)	2	3	2	Aceitar	Monitorização do processo de produção; Indicadores de desempenho dos níveis de execução	5	-