Os Auditores Internos Portugueses e o Risco de Interrupção do Negócio

Fátima Susana Ferreira Vale

Dissertação de Mestrado

Mestrado em Auditoria

Porto – 2017

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

Os Auditores Internos Portugueses e o Risco de Interrupção do Negócio

Fátima Susana Ferreira Vale

Dissertação de Mestrado

apresentada ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação do Mestre Carlos Mendes

Esta versão contém as críticas e sugestões dos elementos do júri

Porto – 2017

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

Resumo

O risco faz parte do dia a dia das organizações e, atualmente, mais do que nunca deve ser gerido de uma forma consciente. Afinal o Risco de Interrupção do Negócio é real, consiste no risco de o volume de negócios ser afetado negativamente devido a um risco a "montante".

Face à evolução e ao papel relevante que o controlo interno e a gestão de risco têm adotado como ferramentas de gestão, é cada vez mais necessário que as organizações detenham adequados sistemas de gestão de risco e de controlo interno, alinhados entre si, integrando-os na sua cadeia de valor e nos seus processos de negócio.

A auditoria interna com pensamento baseado no risco, estimula os auditores internos a desenvolverem maior atenção nesta área preponderante para os dias de hoje.

Daí que, com este estudo, tivéssemos pretendido responder à questão "*Como os Auditores Internos Portugueses vêm o Risco de Interrupção do Negócio*", com o objetivo de analisar o processo de gestão do risco de interrupção do negócio, analisar a sensibilidade do auditor interno perante o risco de interrupção do negócio e o impacto daquele risco. O estudo foi realizado aos auditores internos das empresas inscritas no IPAI. Como principais resultados apurados, salienta-se a debilidade do processo de gestão de risco de interrupção do negócio embora exista o reconhecimento do risco.

Palavras chave: Risco, Risco de Interrupção do Negócio, Gestão de Risco, Auditoria Interna

Abstract

Risk is a part of the day-to-day in organizations, and today, more than ever, it must be managed in a conscious manner. After all, the business interruption risk is real, it consists of the risk that the turnover will be negatively affected due to a sum of risks.

In view of the evolution and relevant role that internal control and risk management have adopted as a management tool, it is increasingly beneficial for organizations to have appropriate risk management and internal control systems, aligned with each other and integrating them into their chain of value and in their business processes.

Internal auditing with a risk-based thinking, encourages internal auditors to develop more attention in this preponderant area on the present day.

Hence, with this study, we intended to answer the question "How do Portuguese Internal Auditors perceive the Business Interruption Risk", with the purpose of analysing the risk management process of business interruption, analysing the internal auditor's sensitivity to the risk of business disruption and the impact of that risk.

The study was conducted on internal auditors of the companies registered in IPAI. As the main results found, the weakness of the risk management process of business interruption is highlighted, although there is risk recognition.

Key words: Risk, Business Interruption Risk, Risk Management, Internal Audit.

Agradecimentos

Ao Professor Mestre Carlos Mendes, meu orientador, o meu agradecimento, pelas suas palavras de incentivo, pela sua sabedoria, e disponibilidade, que demostrou ao longo da realização desta dissertação.

Ao Dr. Soares da Cruz, pela disponibilidade e partilha de conhecimentos imprescindíveis.

À coordenadora Professora Doutora Alcina Dias, partilhando os seus conhecimentos e ferramentas para o mundo do trabalho.

À minha mãe e ao Ivo, pelo apoio incondicional que demonstraram ao longo deste percurso.

A todos, um profundo e sincero agradecimento.

Lista de Abreviaturas

AGCS - *Allianz Global Corporate and Specialty*

AI - Auditoria Interna

BCM - *Business Continuity Management*

CI - Controlo Interno

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

ERM - *Enterprise Risk Management*

FERMA - *Federation of European Risk Management Association*

IFAC - *Internal Control from a Risk-Based Perspective*

IIA - *The Institute of Internal Auditors*

INTOSAI - *International Organization of Supreme Audit Institutions*

IPAI - Instituto Português de Auditoria Interna

ISO - *International Organization for Standardization*

RIN - Risco de Interrupção do Negócio

Índice Geral

Índice de Figuras

Índice de gráficos

Índice de tabelas

Introdução

A presente dissertação insere-se no âmbito do Mestrado em Auditoria sendo dedicada ao tema "Os Auditores Internos Portugueses e o Risco de Interrupção do Negócio". Este delimita o enquadramento e o objeto de estudo, o objetivo da investigação, a organização estrutural e a metodologia seguida.

Vivemos num período de volatilidade sem precedentes. Tendências económicas, demográficas, geopolíticas e tecnológicas convergem para criar novas realidades globais desafiadoras para as organizações. As novidades acarretam novos riscos ou riscos mais sofisticados, quer de natureza positiva quer negativa.

O Risco Interrupção do Negócio não é uma novidade, sempre foi real, carecendo de monitorização e de gestão, liderando o ranking internacional dos riscos que mais inquietam as organizações.

Nesse sentido o nosso objetivo foi o de perceber como os Auditores Internos Portugueses vêm o Risco de Interrupção do Negócio.

O trabalho foi estruturado da seguinte forma:

Os primeiros três capítulos foram dedicados à revisão da literatura. O primeiro capítulo aborda o Risco, em especial o Risco de Interrupção do Negócio, sua caracterização, sendo complementado pelo tema da Gestão de Risco Empresarial.

O segundo capítulo aborda o Controlo Interno e a sua relação com a Gestão do Risco Empresarial.

No terceiro capítulo é apresentada a Auditoria Interna, a sua evolução e a sua relação com a Gestão do Risco Empresarial.

A metodologia aplicada no nosso estudo empírico consistiu na elaboração de um questionário aos auditores internos das empresas inscritas como membros coletivos do Instituto Português de Auditoria Interna.

No Capítulo das Conclusões damos conta dos resultados obtidos, das limitações encontradas e apontamos sugestões de futuras investigações sobre o tema.

Capítulo I – Risco

1.1.Risco

São diversas as considerações em redor da palavra risco e do significado que esta tem em termos práticos no quotidiano de qualquer organização. A própria definição de risco tem sofrido mutações ao longo dos tempos, o que comporta uma adaptação à crescente volatilidade, complexidade e ambiguidade.

Risco, no dicionário de língua portuguesa é definido por "*perigo; inconveniente*", o que evidencia um entendimento negativo quanto ao risco. No entanto, vários autores defendem que o risco também pode ser visto como uma oportunidade, ou seja, pode ter um efeito positivo.

Em termos literários existem diversas definições de risco.

Segundo Pinho et al. (2011) "*a origem da palavra risco deriva do termo italiano risicare, desafiar. Logo, e nesta aceção, o termo risco pode ser entendido mais como uma escolha do que uma fatalidade"*.

Já o *The Institute of Internal Auditors* (IIA) (2009a) estabelece que o risco é "*A possibilidade da ocorrência de um evento que possa ter impacto sobre a consecução de objetivos. O risco é medido em termos de impacto e probabilidade de ocorrência"*.

A *Federation of European Risk Management Associations* (FERMA) (2003) considera que "*o risco pode ser definido como a combinação de um acontecimento e as suas consequências*".

1.2.Risco de Interrupção do Negócio

A maioria das organizações, sejam elas do sector primário, secundário ou terciário, têm como objetivo comum a obtenção de lucro, no entanto, este objetivo pode ser contrariado com a paralisação da produção, em consequência de diversos fatores que levam ao risco de interrupção de negócio (RIN). Afinal, todas as organizações padecem deste risco.

Mesmo que o objetivo de uma organização seja a prestação de um serviço social à comunidade (como por exemplo escolas ou hospitais) sem fins lucrativos, o risco de interrupção do negócio/atividade é real e deve ser monitorizado e gerido.

Já em 1910 o RIN era tratado na Alemanha, com a utilização de uma estratégia de transferência deste risco, tendo na época aparecido uma apólice de seguro relativa à interrupção do negócio devido a avaria de máquinas.

Com as mudanças entretanto ocorridas na economia mundial e o aumento da interdependência entre os diversos agentes económicos, o impacto de certos riscos, especialmente os não seguráveis, têm vindo a tornar-se de difícil mitigação e prevenção.

Segundo Suarez (1976), o RIN pode provocar durante um determinado período de tempo, que poderá ser curto ou longo, a interrupção da atividade produtiva (interrupção total) ou afetar parcialmente a atividade (interrupção parcial).

Assim, a noção de interrupção do negócio é diametralmente oposta à destruição total da mesma, entendida como uma cessação completa, definitiva e irreversível.

Por outras palavras, a gestão do risco de interrupção de negócio tem subjacente a continuidade da empresa.

Também segundo Suarez (1976), a interrupção do negócio implica o desaparecimento do volume de negócios gerado pelas receitas da venda de produtos ou serviços, ou apenas a sua diminuição, se apesar da interrupção, existirem stocks armazenados, ocorrendo a um ritmo diferente.

Segundo Azevedo (2016), a interrupção de negócio implica a suspensão do lucro líquido apesar da continuação dos custos fixos do negócio. Assim, o risco de interrupção de negócio consiste no risco do volume de negócios, isto é, na paralisação total ou parcial do negócio, com perda de lucro e continuação dos custos fixos uma vez que os custos variáveis, esses diminuem.

A interrupção do negócio deve ser avaliada em função do setor de atividade da empresa e deve ter em conta as seguintes especificidades:

- Atividade desenvolvida,
- Dimensão da empresa,
- Nível tecnológico,
- Processos de fabrico,
- Estrutura interna,

- Qualidade das instalações,
- Conjuntura do mercado potencial e efetivo,
- Relações de dependência económica com outras empresas,
- Pontos de estrangulamento, e
- Duração de reconstrução de edifícios e aquisição de equipamentos.

No entanto, sejam quais forem as causas que originam a paralisação da empresa, existem inúmeros fatores que potenciam esse acontecimento. A paralisação parcial ou total implica a rutura da harmonia no funcionamento de uma qualquer organização.

Apesar dos custos variáveis que, por definição variam ao ritmo da produção, possam deixar de ocorrer, os custos fixos, como a sua própria designação indica, não são suscetíveis de suspensão. Impostos, salários, rendas, custos financeiros, seguros, permanecem, apesar das operações da empresa estarem parcialmente ou totalmente inativas, permitindo assim continuar a operar durante e após os efeitos adversos resultantes do incidente ter terminado.

De salientar que a tempestividade da ocorrência pode ser crucial. Dados indicam que geralmente uma interrupção por um curto período de tempo dificilmente prejudica o resultado geral da atividade comercial. No entanto, uma longa interrupção pode causar danos irreversíveis, como por exemplo a perda de clientes. Assim, haverá que considerar sempre a tempestividade da ocorrência.

O estudo barómetro de risco "Top Riscos Negócios 2017", publicado pela *Allianz Global Corporate and Specialty* (AGCS, 2017), seguradora especializada em diversos riscos, após ter entrevistado mais de 1200 profissionais de risco, em 50 países, posiciona o RIN como líder do ranking como o principal risco para as empresas em 2017, mantendo-se nesse ranking há 5 anos consecutivos. Profissionais de países como Espanha, França, Itália, Canadá e Estados Unidos são exemplos de países que o elegeram como número um.

No estudo citado, os inquiridos consideram como principais fatores que, a montante, podem originar a interrupção do negócio:

- Fogo/ Explosão;

- Catástrofes Naturais;
- Cadeia de abastecimento;
- Ataques cibernéticos; e
- Avaria de máquinas

A consultora Marsh (2016), conforme o estudo *"Continental European Cyber Risk Survey:* 2016*"*, inquiriu 700 empresas europeias, das quais 60 portuguesas, sobre o risco de ataques cibernéticos. Quando questionadas sobre qual a maior ameaça, no caso de uma perda cibernética, 60% das empresas em Portugal destacam a interrupção do negócio.

Dados internacionais revelam que após um grande sinistro, que afete mais de 75% da capacidade produtiva, nas organizações:

- 43 % não recomeçam a atividade após o sinistro;
- 28 % não sobrevivem ao fim de 3 anos; e
- 29 % continuam a operar ao fim de 3 anos.

De destacar que, segundo Suarez (1976), os efeitos da ocorrência do RIN raramente se circunscreve ao contexto de uma única empresa, uma vez que esse fenómeno vai afetar fornecedores, clientes, o seio familiar dos seus funcionários, e indiretamente o tecido económico de uma região/país. Uma empresa também tem cariz social, acabando por se tornar num problema para todos. A transferência do impacto deste risco revela-se como uma resposta possível.

1.2.1. O Seguro "Risco de Interrupção do Negócio"

Segundo Suarez (1976), a resposta a essa necessidade económica é um meio *adhoc*, criado pelo próprio sistema económico, para cobrir as necessidades que superam a área patrimonial da pessoa: o seguro. Assim, temos o facto de que o seguro cria segurança contra a homogeneização de riscos diferentes e únicos, dando desta forma proteção ao segurado contra a possível perda ou efetivação do risco.

Também Suarez (1976), refere que quando uma empresa sofre uma avaria ou um acidente numa máquina ou até numa das suas infraestruturas, a reparação deste dano normalmente pode ser assegurada através da cobertura de um seguro de danos materiais. Falamos de

coberturas como incêndio, avaria de máquinas, multirriscos empresa. Na prática esta cobertura garante os danos materiais diretos.

Porém, nesta cobertura, não estão previstos os danos indiretos que as máquinas causaram ao deixar de trabalhar, durante um determinado período de tempo. Portanto, se estivermos perante uma situação catastrófica na qual uma empresa sofre um grave incêndio que a paralise durante vários meses, e se esta tem a cobertura multirriscos empresa, por exemplo, podemos considerar que, em regra, a indemnização correspondente irá permitir reconstruir os edifícios e repor as máquinas afetadas. Na prática, não são considerados os gastos fixos, que independentemente da laboração ou não da empresa continuam a existir.

Para fazer face a este tipo de situações, surgiu o seguro de lucros cessantes/perdas de exploração/interrupção de negócio.

Para Azevedo (2016), a cobertura do risco da interrupção do negócio destina-se a proteger o lucro líquido e os custos fixos do negócio, sendo o objetivo de assegurar que a empresa não será encerrada como resultado do incidente, permitindo continuar a operar após os efeitos adversos resultantes do incidente ter terminado.

A empresa pretende assim salvaguardar a obtenção do lucro que se vê frustrado pela paralisação inesperada do processo produtivo, garantindo a função vital de continuidade da empresa.

Em Portugal, inserido no ramo não vida, o seguro de perdas pecuniárias diversas, rege-se pelo DL n.º 72/2008, de 16 de abril e pelo que contratualmente as partes acordarem, e abrange o risco, nomeadamente de: perdas de lucros; persistência de despesas gerais; perda de rendas ou de rendimentos; perdas pecuniárias não comerciais; despesas comercias imprevisíveis – artigo. 123.º, n.º 16 do DL n.º 94.º-B/98, de 17 de abril.

Não existe divulgação de dados por parte das seguradoras, do número de sinistros e coberturas em Portugal, em consequência da ocorrência do risco de interrupção de negócio, apesar de todas as seguradoras portuguesas oferecerem este seguro. No entanto, segundo dados recolhidos no Segurdata (2017) intitulado "indicadores de gestão multirrisco", numa amostra total 87,2% de multirriscos a junho de 2017, existiam 3.590.729 apólices de seguros, tendo ocorrido 136.294 sinistros. Será que nestes sinistros houve interrupção de negócio. Não é possível aferir, devido a indisponibilidade de dados.

O processo de contratação de um seguro de interrupção de negócios pode incluir a revisão pelas seguradoras de um plano de contingência e de recuperação de desastres, o relatório de avaliação de riscos dos danos materiais e um plano de continuidade.

1.2.2. Planos de contingência

A necessidade de planos de contingência e de recuperação de desastres foram sendo sentidas com as catástrofes naturais e os fenómenos de terrorismo durante os anos 1980. Foi sendo reconhecido um cada vez maior do impacto no negócio a que as interrupções que as organizações estão sujeitas no caso de um evento desta natureza. Tornou-se, assim, conhecida a disciplina de *Business Continuity Management* (BCM) (Gasiorowski-Denis, 2012).

A BCM tem como objetivo a adoção das medidas que visem manter a capacidade de recuperação de serviços de acordo com as necessidades, requisitos e prazos acordados do negócio. Inclui uma série de atividades para assegurar que os planos de continuidade e recuperação desenvolvidos bem como estratégias de políticas de continuidade estão alinhados com a cultura da entidade.

O Plano de Continuidade de Negócios é um processo de Gestão cujo objetivo é permitir repor os processos de negócio após uma disrupção grave dos mesmos, incluindo a gestão de todos os recursos necessários para a produção, nomeadamente pessoas e bens.

Surgiu a necessidade de estabelecer um único padrão internacional de segurança, desenvolvido em 2012, o ISO 22301 - *International Organization for Standardization - Business continuity management systems*. Este novo *standard* foi o resultado de uma iniciativa global de interesse, cooperação e recolha de inputs sobre a necessidade de continuidade, contingência e recuperação das organizações na era da Globalização. É o único referencial no âmbito da gestão de continuidade de negócio internacionalmente reconhecido. Descreve uma *framework* que tem como objetivo melhorar a identificação de potenciais ameaças, avaliar o seu impacto e desenvolver as capacidades para gerir estas ocorrências.

Segundo Silva (2016), em 2014, Portugal, tinha apenas 3 certificações da ISO 22301 das 593 existentes na Europa.

1.3.Gestão de Risco Empresarial

A gestão de risco iniciou-se pelas seguradoras com a oferta de apólices para cobertura da atividade marítima. No decorrer dos anos, o setor financeiro dedicou-se ao aperfeiçoamento das ferramentas de controlo de risco, entusiasmado pela possibilidade de "prever" o futuro e evitar as perdas previsíveis.

Em consequência de vários escândalos financeiros, da manipulação de resultados, o caso de organizações como a "*Enron"*, "*WorldCom"*, entre muitas outras, afetou de forma significativa a confiança dos *stakeholders*, originando a necessidade do desenvolvimento e implementação de modelos de Gestão de Risco Empresarial. Os principais objetivos foram os de criar princípios, conceitos chave e uma linguagem comum, que constituíssem um guia para a Gestão de Riscos de Negócio nas organizações.

Assim, o *Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM)* (2007) definiu o conceito de Gestão de Risco Empresarial, como sendo:

> *"um processo efetuado pelos quadros de direção, gestão e outro pessoal da empresa, aplicado numa estratégia e transversal a toda a empresa, desenhado para identificar potenciais eventos que possam afetar a empresa e gerir os riscos de acordo com o seu apetite de risco, proporcionando uma segurança razoável com vista ao cumprimento dos seus objetivos."*

Já para a FERMA (2003) "*a gestão de risco deve ser um processo contínuo e em constante desenvolvimento, aplicado à estratégia da organização e à implementação dessa mesma estratégia. Deve analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e, em especial, futuras de uma organização*".

Para Beja (2004) a gestão de risco significa *"tomar ações corretivas para mudar a probabilidade de ocorrência dos riscos de forma a aumentar a probabilidade de ocorrência de resultados positivos e diminuir a de resultados negativos"*.

Atualmente, com o relatório mais recente emitido pelo COSO (2017), o principal objetivo da gestão do risco será o de maximizar o valor para os acionistas, conseguido através da melhoria do apoio no processo de tomada de decisões, identificando quais as áreas de

risco, e as formas de reforçar a confiança dos investidores, através da definição de um processo estratégico que tenha em conta as incertezas.

Benefícios da Gestão de Risco Empresarial

Segundo o relatório do COSO (2017), as organizações que integram a gestão de risco em toda a sua estrutura podem obter vários benefícios, incluindo, mas não estando limitados a:

- Aumentar o leque de oportunidades;
- Identificar e gerir os riscos em toda a organização;
- Aumentar os resultados positivos e vantagens, diminuindo surpresas negativas;
- Reduzir a instabilidade do desempenho;
- Melhorar a utilização dos recursos;
- Reforçar a resiliência dos recursos.

Estes benefícios destacam o facto de que o risco não deve ser visto apenas como um constrangimento ou potencial desafio para a definição e realização de uma estratégia. Em vez disso, a mudança que está por trás do risco e as respostas organizacionais a adotar, podem dar origem a oportunidades estratégicas e ao aumento das capacidades de diferenciação.

1.3.1. Modelos de Gestão de Risco Empresarial

Existem vários modelos de gestão de risco empresarial, tais como:

- Gestão de Risco Empresarial: COSO ERM - *Integrating with Strategy and Performance*, emitido pelo COSO em junho de 2017.
- ISO 31000 da *International Organization for Standardization* emitida em 2009.
- ERM – *Enterprise Risk Management Framework*, emitido pelo COSO em 2004;
- Norma de Gestão de Riscos Australiana AS/NZS 4360 - *Risk Management Guidelines* em 2004; e
- Norma de Gestão de Riscos da FERMA: Risk Management Standard emitida pela *Federation of European Risk Management Associations* em 2002.

Contudo, vamo-nos focar no mais atual, o COSO ERM, de 2004 a 2017.

1.3.1.1. Relatório COSO II - Enterprise Risk Management

Em 2004, o COSO publicou o COSO II -*Enterprise Risk Management* (ERM), com a colaboração da *Price Water House Coopers* com vista ao desenvolvimento de um modelo que permitisse ajudar os gestores na avaliação e melhoria da gestão de risco das suas organizações.

O ERM vai para além do sistema de controlo interno (CI), promovendo uma focalização mais forte e abrangente na Gestão de Risco Empresarial, aumentando assim a segurança e a credibilidade do mercado. Contudo, não substitui o modelo de CI desenvolvido pelo COSO I, mas incorpora-o, proporcionando que as organizações utilizem este modelo com vista a satisfazerem as necessidades do seu sistema de CI, progredindo para um processo com a integração da gestão de risco no controlo interno.

No quotidiano, as organizações enfrentam uma multiplicidade de riscos, desafios e incertezas, sendo o grande desafio da Gestão determinar qual o nível de risco que a empresa está disposta a aceitar (risco aceitável). Nem todos os riscos têm o mesmo nível de importância/criticidade. A ERM permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos cujo impacto seja maior (positivo ou negativo), com o objetivo de criar valor para os *stakeholders*.

Há uma interligação direta entre os objetivos, que uma organização está disposta a alcançar, e os componentes da ERM, que representam aquilo que é indispensável para a sua consecução. Esta interligação é apresentada através de uma matriz tridimensional em forma de cubo, podendo ser ilustrada na forma de um cubo, como apresenta a Figura 1.

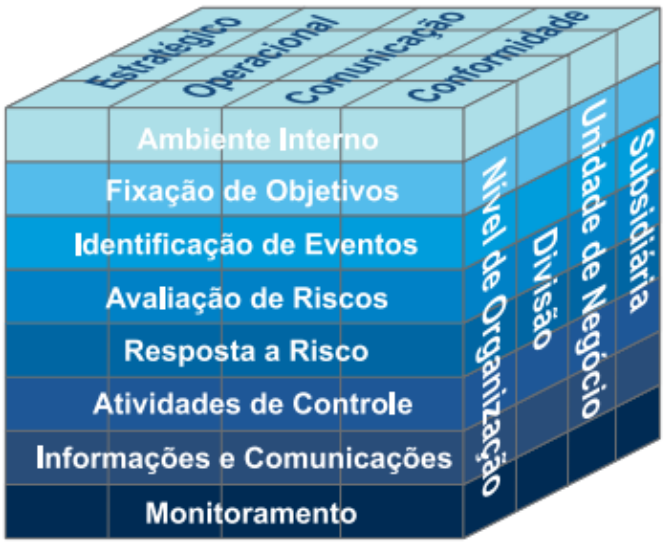

Figura 1 Modelo de Gestão de Riscos COSO 2004
Fonte: COSO, 2007.

As quatro categorias de objetivos empresariais (estratégicos, operacionais, de comunicação e conformidade) estão exibidas no topo do cubo. Os oito componentes são apresentados nas linhas horizontais (mais 3 componentes, que o COSO I, sendo estas: Definição de objetivos; Identificação de eventos e Resposta ao risco) e a estrutura organizacional na terceira dimensão. Essa representação ilustra a capacidade de manter o enfoque na totalidade da ERM de uma organização, ou na categoria de objetivos, componentes, estrutura organizacional ou qualquer um dos subconjuntos (COSO, 2007).

De acordo com este modelo, os componentes de gestão caracterizam-se por:

Ambiente Interno

Contexto ou ambiente em que as organizações funcionam, com objetivos a atingir e meios a serem utilizados para esse fim. Abrange a filosofia de gestão de risco, o apetite pelo risco, a integridade e os valores éticos.

Definição de Objetivos

Os objetivos devem existir antes que a administração possa identificar os eventos negativos ou positivos. É uma pré-condição para a identificação dos riscos, para a sua avaliação e formulação das respostas possíveis de serem implementadas.

Identificação de Eventos

Consiste na identificação dos fatores internos e externos, com capacidade para afetar a estratégia e os seus objetivos e serem identificados como oportunidades ou riscos.

Avaliação de Riscos

Os riscos são avaliados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser tratados. A gestão avalia a situação como risco inerente ou risco residual.

> **Risco Inerente:** aquele em que a organização incorre na ausência de medidas preventivas ou de correção, e que varia de acordo com a natureza das operações.
> **Risco Residual:** nível do risco remanescente, após as ações empreendidas pela

gestão com o intuito de minimizar o impacto e a probabilidade de uma ocorrência adversa, incluindo as atividades de controlo para face ao risco (IIA,2009).

Os riscos são considerados mediante a probabilidade de ocorrência de acontecimentos e as suas consequências ou impactos.

Na análise dos riscos, é possível utilizar uma análise quantitativa ou uma análise qualitativa.

Análise Qualitativa: ordenação dos riscos através da avaliação e combinação da probabilidade de ocorrência e impacto.
Análise Quantitativa: observação numérica dos efeitos dos riscos identificados nos objetivos gerais.

Resposta aos Riscos

A resposta deve ser dada considerando a probabilidade de ocorrência, e o efeito/impacto do risco, assim como os respetivos custos e benefícios. A resposta pode ser:

Evitar: descontinuar as atividades que geram riscos, podendo envolver o abandono de linhas de produção ou segmentos de mercado;
Reduzir: adotar medidas para reduzir a probabilidade ou o impacto dos riscos;
Transferir: redução da probabilidade ou do impacto dos riscos pela transferência ou partilha de uma fração do risco, através, por exemplo, de seguros, operações de cobertura, *outsourcing*; e
Aceitar: nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos.

Aceitar indica que nenhuma opção de resposta foi encontrada para minimizar o impacto e a probabilidade a um nível aceitável. Reduzir e partilhar diminuem o risco residual a um nível compatível com as tolerâncias desejadas de risco, por sua vez, evitar aponta para que o risco inerente já esteja dentro da tolerância ao risco.

Controlo das atividades

Constituída pelas políticas (o que deve ser feito) e procedimentos (a forma como deve ser feito) estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia.

Informação e comunicação

As informações pertinentes deverão ser identificadas e comunicadas, no devido prazo.

Monitorização

A monitorização é realizada através de atividades de gestão contínuas ou avaliações independentes ou de ambas as formas.

Criticas ao COSO ERM 2004

Santos (2013) refere o congresso sobre gestão de risco organizado pelo IIA em agosto de 2010, em que Arnold Schanfield, membro do Conselho Consultivo do IIA, apontou algumas críticas à ERM, nomeadamente:

- Não há a mínima atenção às partes interessadas externas e às suas necessidades e/ou expectativas; o COSO ERM parece estar voltado principalmente para o público interno, mas as partes interessadas externas são fundamentais;
- O COSO ERM confunde processo de gestão de risco com a estrutura de gestão de risco, facto que explica a difícil compreensão e aplicação da norma;
- A norma refere os riscos cuja evolução é rápida e discrimina os riscos considerados em evolução mais lenta, como por exemplo as mudanças demográficas da população;
- O risco é associado a um aspeto negativo cuja ocorrência trará desvantagens não sendo dada grande relevância aos riscos que poderão ser positivos, nomeadamente em oportunidades de negócios inexploradas ou em ascensão.

1.3.1.2. COSO ERM - *Integrating with Strategy and Performance*

Em junho de 2017 é apresentada uma nova versão, o relatório COSO ERM - *Integrating with Strategy and Performance*, em que se destaca a importância de considerar os riscos,

tanto no processo de definição da estratégia, quanto na condução no desempenho da sua execução pela organização. Esta nova publicação advém da evolução do risco para atender às demandas de um ambiente de negócios em evolução. As organizações necessitam de se adaptar à constante volatilidade e complexa ambiguidade global.

Na definição de um processo estratégico, quanto maior é a dimensão da organização mais difícil se torna em delinear a sua aplicabilidade, pois este é um processo complexo. Dado que as organizações com maiores oportunidades de crescimento enfrentam maior incerteza, é requerida uma gestão do risco mais cuidada para controlar os riscos com que se deparam, mas também para orientar o seu crescimento na direção apropriada, com base no impacto das várias oportunidades associadas ao risco.

Na decomposição dos objetivos estratégicos em objetivos operacionais, é necessário atribuir responsabilidades, mas também recorrer a uma entidade independente, para avaliar e garantir que esses objetivos definidos estão de acordo e vão ao encontro da estratégia definida.

O relatório COSO (2017) esclarece que a ERM não é uma função ou departamento. É constituído pela cultura, capacidades e práticas que a organização integra com a definição de estratégia e aplicam-se quando são desenvolvidas nessa estratégia, com objetivo de a gestão de risco criar, preservar e realizar valor.

Figura 2: COSO ERM - *Integrating with Strategy and Performance* **Fonte:** COSO, 2017

A figura 2, reflete o conjunto de princípios organizados em cinco componentes inter-relacionados:

Governação e Cultura

A cultura incide sobre os valores éticos, comportamentos desejados e compreensão do risco na entidade. A organização estabelece a importância de instituir responsabilidades de supervisão para a gestão de risco.

Estratégia e definição de objetivos

Gestão de risco, estratégia e definição de objetivos de trabalho em conjunto no processo de planeamento estratégico. O apetite pelo risco estabelecido é alinhado com a estratégia de negócio.

Desempenho

Riscos que podem afetar a realização da estratégia e negócio. Os riscos são ordenados por gravidade no contexto do apetite pelo risco. A organização seleciona as respostas a dar ao risco.

Análise e Revisão

Ao analisar o desempenho da organização, uma organização pode considerar os componentes de gestão de risco, ao longo do tempo e à luz de mudanças substanciais, em que são necessárias revisões.

Informação, Comunicação e Relatórios

A gestão de risco é um processo contínuo de obtenção e partilha de informações necessárias, tanto de fontes internas como externas, por toda a organização.

As cinco componentes do quadro foram complementadas por um conjunto de 20 princípios, que descrevem práticas que podem ser aplicadas de maneiras diferentes, para os diferentes tipos de organização, independentemente do seu tamanho, tipo ou sector.

Assim, a aplicação do novo modelo COSO-ERM, traz um potencial significativo para as organizações, nomeadamente como uma alternativa na delineação da estratégica empresarial. Deste modo, as organizações poderão definir a implementação da estratégia com maior potencial, já que o modelo procura combinar os fatores de risco com a filosofia estratégica de gestão da empresa e deste modo permitir antecipar ocorrências futuras, para

que na elaboração do plano estratégico, haja a oportunidade de uma redução significativa dos riscos e da probabilidade de que os resultados sejam desfavoráveis.

O processo de tomada de decisões será mais fiável se elas forem tomadas tendo em conta informações relacionadas com as incertezas relacionadas com o futuro. Pelo que, através da harmonização entre a vertente de gestão de risco e a vertente de análise estratégica, nos leva a olhar para o controlo dos riscos num contexto mais alargado. Deste modo a empresa terá melhores condições de obter sucesso uma vez que terá respostas mais concretas na definição estratégica.

1.3.2. Limitações da Gestão de Risco

Os modelos de gestão de risco não garantem que os objetivos de uma organização sejam atingidos, apenas dá uma segurança razoável de que tais objetivos possam ser alcançados.

Afinal os riscos pertencem ao futuro, logo representam acontecimentos que não são possíveis de prever com segurança e exatidão, em que alguns casos não dependem da própria organização, são externos à organização, o que os torna mais difíceis de prever.

Também a gestão de riscos é feita por pessoas, logo existe a hipótese de ocorrer erro humano, como por exemplo, uma informação menos clara que pode dar início a uma decisão ou a um juízo de valor menos correto, podendo afetar a concretização de determinado objetivo.

Para o relatório COSO (2017), o conceito de segurança razoável, não significa que a gestão de riscos deva fracassar frequentemente. Porém, pode ocorrer um erro, um evento incontrolável ou uma informação falsa. A segurança razoável não é sinónimo de segurança absoluta.

Capítulo II – Controlo Interno

2.1. O Controlo Interno

Controlo é um processo que pretende obter uma garantia de que a consecução dos objetivos estabelecidos é conseguida.

Martins & Morais (2007) mencionam que o *American Institute of Certified Publics Accounts* (AICPA) foi o primeiro organismo a definir o controlo interno (CI): *"o controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas adaptadas num negócio a fim de garantir a salvaguarda de ativos, verificar a adequação e confiabilidade dos dados contabilísticos, promover a eficiência operacional e encorajar a adesão às políticas estabelecidas pela gestão."*

Em 1992, o organismo COSO, publica o Relatório *Internal Control - Integrated Framework*, uniformizando o conceito de CI, em que o classifica como *"um processo, da responsabilidade do Conselho de Administração, da Gestão Executiva e restante pessoal da entidade, estabelecido com vista a proporcionar uma garantia razoável da consecução dos seguintes objetivos da organização:*

- *Eficiência e eficácia das operações;*
- *Fiabilidade do reporte financeiro;*
- *Conformidade com as normas e regulamentos aplicáveis".*

Logo, é um processo traçado para alcançar os objetivos da organização, que começa no topo desta, com os quadros de direção e de gestão a criar e reforçar a estrutura e harmonia dos controlos, envolvendo toda as pessoas da organização, indo além dos controlos internos relativos ao relato financeiro.

Contudo a crescente globalização de mercados e transações e a consequente complexidade que os negócios assumem, levaram à revisão do Relatório *Internal Control - Integrated Framework.* Estas mudanças, deram origem, em 2013, à publicação de um novo Relatório, o COSO ERM *Framework.* Assim, *"Controlo interno é um processo conduzido pela estrutura de governação, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à*

realização dos objetivos relacionados com as operações, divulgação de informação e conformidade com Leis e Regulamentos." (COSO, 2013).

Existe uma relação direta entre os objetivos da organização, os componentes que representam, interligados entre si, para atingir os objetivos, e a estrutura organizacional, podendo ser ilustrada na forma de um cubo, como apresenta a Figura 3.

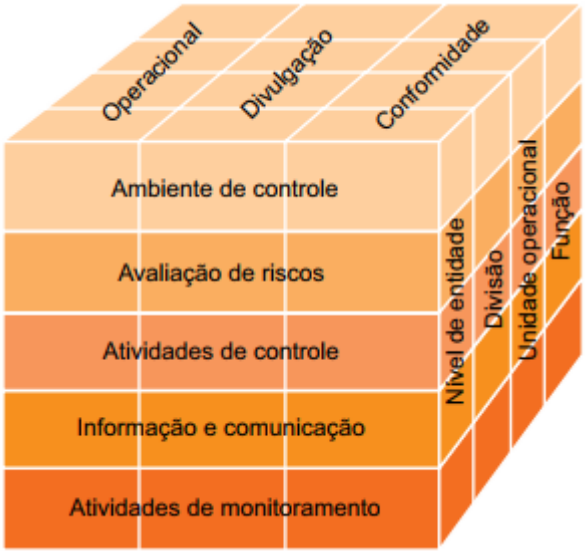

Figura 3: COSO - Controlo Interno
Fonte: COSO 2013

O Cubo COSO compreende cinco componentes: Ambiente de controlo; Avaliação de riscos; Atividades de controlo; Informação e comunicação; e Atividades de supervisão/monitoramento. Estas devem operar interligadas, um único processo, no cumprimento dos objetivos. Estes estão relacionados com o modo como a Gestão conduz o negócio e fazem parte integrante do processo de gestão. A estrutura organizacional da entidade é representada pela terceira dimensão. As três categorias de objetivos: operacional, divulgação e conformidade, são representadas pelas colunas.

Os princípios enunciados pelo COSO, que representam os conceitos fundamentais associados a cada componente, são os seguintes (COSO, 2013):

Ambiente de Controlo

1. A organização demonstra um compromisso para com os valores éticos e de integridade;
2. O conselho de administração demonstra independência da gestão e exerce supervisão sobre o desenvolvimento e desempenho do CI;
3. A Gestão estabelece, com a supervisão da administração, estruturas, linhas de relato e autorizações e responsabilidades apropriadas na prossecução dos objetos;
4. A organização demonstra um compromisso de atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos;

5. A organização mantém medidas que conduzam à responsabilização dos indivíduos pelo desempenho e CI.

Avaliação do Risco

6. A organização especifica os objetivos com clareza suficiente para permitir a identificação e avaliação dos riscos associados aos objetivos;
7. A organização identifica os riscos para alcançar os objetivos através da entidade e analisa riscos como base para determinar como devem ser geridos;
8. A organização considera a possibilidade de existência de fraude na avaliação dos riscos para a concretização dos objetivos;
9. A organização identifica e avalia as mudanças que poderiam afetar significativamente o sistema de CI.

Atividades de Controlo

10. A organização seleciona e desenvolve atividades de controlo que contribuem para a mitigação de riscos na execução dos seus objetivos para níveis aceitáveis;
11. A organização seleciona e desenvolve atividades de controlo geral sobre as tecnologias que suportem o alcance dos objetivos;
12. A organização implementa atividades de controlo através de políticas que estabelecem as suas expectativas e definem procedimentos que coloquem essas políticas em prática.

Informação e Comunicação

13. A organização obtém ou gere e usa informação de qualidade relevante, para apoiar o funcionamento do CI;
14. A organização comunica internamente informação, que inclui objetivos e responsabilidades de CI, necessárias para o seu funcionamento;
15. A organização comunica com públicos externos sobre a matérias que afeta o funcionamento do CI.

Atividades de Monitorização

16. A organização seleciona, desenvolve e executa avaliações contínuas ou separadamente, para verificar se todos os componentes do CI estão presentes e em funcionamento;
17. A organização avalia e comunica as deficiências do controlo interno, em tempo útil aos responsáveis por tomar as medidas corretivas, incluindo aos gestores executivos e quadros de direção.

Assim, relativamente à estrutura da organização, o novo *Framework* alinha-se com o *Framework* do COSO ERM de 2004, o qual considera toda a organização e todos os níveis funcionais. Este atualizado agora em 2017.

2.2. Os Controlos Internos

O grau de confiança nos controlos internos, é o princípio fundamental para o trabalho desenvolvido pelo auditor interno.

Ao longo do processo de implementação de um sistema de controlo interno, há um aspeto de elevada reflexão pelas organizações – a relação custo/benefício, uma vez que uma grande parte das empresas está condicionada com a limitação de recursos.

Assim, e uma vez que a implementação de um controlo significa, inevitavelmente, um custo. O auditor interno deve avaliar, com precisão, os benefícios resultantes do mesmo. A *International Organization of Supreme Audit Institutions* (INTOSAI) (2008) afirma que "*os controlos dependem de uma vantajosa relação de benefícios e custos, sendo que estes devem ser inferiores às perdas decorrentes da consumação do risco não controlado.*"

Conforme ilustrado na figura 4, por vezes pode acontecer a implementação de um controlo cujo custo seja maior que o benefício; no entanto, se controlos não forem aplicados, a organização pode ficar demasiada exposta aos riscos, vivendo uma situação de ausência de controlos, logo numa situação vulnerável.

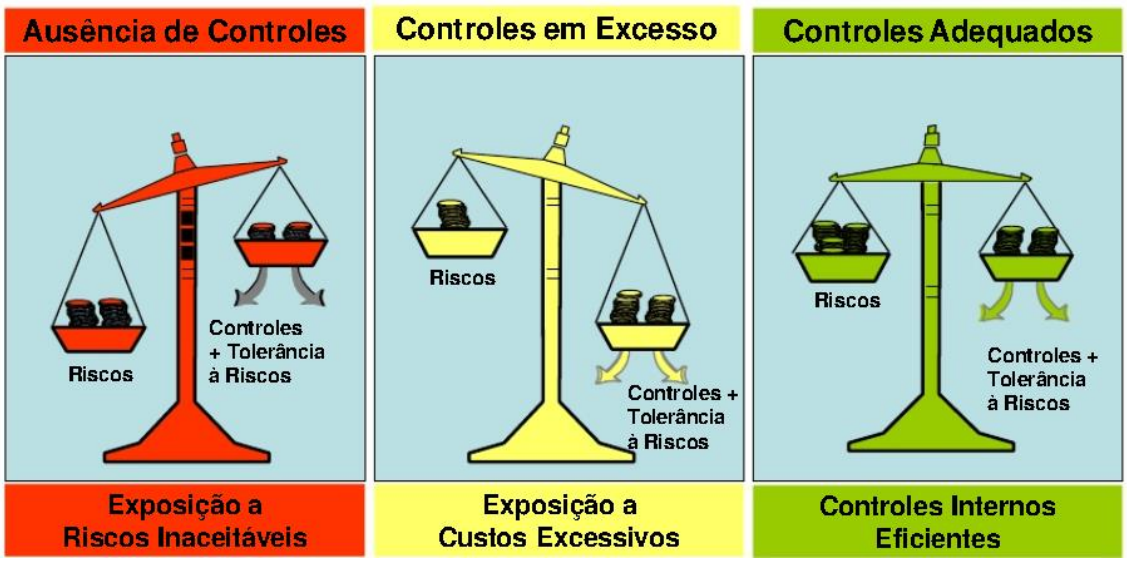

Figura 4: O Peso dos Controlos **Fonte**: Santos 2009

De salientar que, por vezes, é melhor aceitar determinados riscos não implementando determinados controlos internos, quando estes representam um custo superior aos benefícios que podem trazer.

2.2.1. Tipos de controlos internos

Os controlos internos são constituídos por procedimentos, políticas e práticas desenvolvidas com a finalidade de mitigar os riscos previamente identificados e que afetam, de alguma forma, a consecução dos objetivos estabelecidos pela organização. Existem vários tipos de controlos, tais como:

Controlos preventivos: servem para impedir a ocorrência de factos não desejados. São considerados controlos *apriori*, que entram imediatamente em funcionamento, devendo atuar antes que os factos ocorram;
Controlos detetivos: servem para detetar factos não desejados que já tenham ocorrido;
Controlos diretivos: servem para encorajar ou provocar a ocorrência de factos pretendidos (por exemplo: definição de políticas e procedimentos);
Controlos corretivos: servem para corrigir factos ocorridos e indesejados; e
Controlos compensatórios: servem para aplicar/colmatar eventuais falhas de outros controlos.

2.3. O controlo interno e a gestão de risco

O CI permite a identificação de insuficiências mitigando-as ou, se possível, eliminando-as contribuindo para uma melhoria dos comportamentos que consequentemente terão reflexo nos resultados da organização.

Os costumes, a cultura e o sistema de governo da sociedade podem inibir irregularidades a cometer pela gestão, mas não se tornam impedimentos absolutos.
O relatório COSO (2017) define a Gestão de Risco como parte integrante do CI agregando uma visão global dos riscos a partir do topo. Também refere que gestão de risco é constituída pela cultura da organização. Assim, o CI deve ser parte integrante da gestão de risco, só assim é possível conseguir um processo de gestão de risco eficaz e eficiente.

Num estudo realizado pelo IFAC em 2007, *Internal Control from a Risk-Based Perspective*, John Fraser, auditor interno e diretor de gestão de risco da empresa canadiana *Hydro One Inc*., salienta que o " *controlo interno é apenas um meio de obter uma gestão de risco empresarial. O controlo interno é um subconjunto do governo e da gestão de riscos empresariais e (…) é a chave de uma boa gestão*"

Assim, é necessário que cada vez mais as organizações detenham apropriados sistemas de gestão do risco e controlo interno, interligados e integrados com os objetivos estratégicos da entidade.

Capitulo III – Auditoria Interna

3.1. A Auditoria Interna e a sua evolução

De forma genérica, considerando o objeto e objetivos de auditoria, esta consiste num:

> *"Processo de acumulação e avaliação de prova sobre certa matéria para determinar e relatar sobre o grau de correspondência entre essa matéria e os critérios estabelecidos para a mesma. Essa matéria pode, entre outras, revestir a forma de informação financeira ou não financeira, procedimentos, conduta das operações, resultados das operações, ou o cumprimento das leis, regulamentos e ordens."* (Alves, 2015)

Segundo Morais & Martins (2007), *"nos anos 40/50, impôs-se, nos Estados Unidos, a ênfase na revisão do controlo interno empresarial."*

Assim, em 1941, surge nos Estados Unidos, *The Institute of Internal Auditors* (IIA) que foi determinante para o desenvolvimento da atividade dos auditores internos a nível global. Este organismo permite, por um lado, a divulgação das melhores práticas de Auditoria Interna, e por outro, a homogeneização da profissão pelos padrões mais elevados. Em Portugal, foi criado em 1992, o Instituto Português de Auditores Internos (IPAI), membro do IIA.

Na conferência internacional do IIA em 1978, foram aprovados os *Standard for the Professional Practice of Internal Auditing* definindo *"Auditoria Interna como uma função de apreciação independente, estabelecida dentro da organização, como um serviço para a mesma, para examinar e avaliar as suas atividades."* (Costa, 2007)

Castanheira (2007) adapta da seguinte forma esquematizada a tabela 1 o trabalho preconizado por McNamee e Selim (1998), que traduz a mudança da Auditoria Interna do enfoque sobre o "Controlo Interno" para a "Gestão do Risco".

Características	Velho paradigma	Novo Paradigma
Foco AI	Controlo Interno	Risco do Negócio
Resposta da AI	Reativa após os factos, descontinua, observadora das iniciativas de planeamento estratégico	Pró-ativa, tempo real, monitorização continua, participativa nos planos estratégicos
Avaliação de Risco	Fatores de risco	Planeamento de cenários
Testes de AI	Controlos importantes	Gestão dos Riscos importantes
Métodos de AI	Ênfase em testes de controlo detalhados e completos	Ênfase na importância e abrangência dos riscos de negócio cobertos
Recomendações AI	Controlo Interno: •Reforço •Custo-benefício •Eficácia/Eficiência	Gestão de Risco: •Evitar/diversificar o risco •Partilhar/transferir o risco •Controlar/Aceitar
Relatórios de AI	Dirigidos aos controlos funcionais	Dirigidos aos riscos dos processos
Papel de AI na Organização	Função de avaliação independente	Atividade que integra a Gestão de Risco e a Governação da Organização

Tabela 1: Auditoria Interna: Velho paradigma e o Novo Paradigma **Fonte:** Castanheira (2007)

A auditoria interna deixou de ser vista como uma mera função de controlo, passando a preocupar-se com a identificação dos riscos, das atividades de controlo e a avaliação da eficácia das mesmas na mitigação dos riscos, bem como, propor recomendações com o objetivo de implementarem medidas de correção e melhoria para mitigação do risco, de modo a que os objetivos da organização sejam atingidos.

Esta alteração mostra também a mudança que veio a acontecer ao longo dos anos na atividade de AI, em que estamos a convergir de um trabalho fundamentalmente focado em factos passados, para um trabalho que se foca no presente e no futuro, acrescentando deste modo maior valor à organização.

Assim, a grande diferença entre o anterior e o atual paradigma da auditoria interna, reside na análise estratégica e na avaliação dos processos de negócio como passo prévio aos trabalhos que são levados a cabo pelos departamentos de auditoria (Lorenzo, 2001; Gronli e Xystos, 1999; citados por Castanheira, 2007).

O IIA adaptou o conceito de AI aos tempos atuais e acontecimentos ocorridos:

> "*Auditoria Interna é uma atividade independente, de garantia e consultoria, destinada a acrescentar valor e melhorar as operações de uma organização. Ajuda a organização a alcançar os seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação e melhoria da eficácia dos processos de gestão de risco, controlo e de governação."* (IIA, 2009a).

A AI é vista como uma atividade que acrescenta valor, permite à organização melhorar as suas operações, reduzir riscos e alcançar os objetivos, através da identificação de melhorias e respetivas recomendações.

> *"A necessidade criou a Auditoria Interna e está a tornar-se parte integrante do negócio moderno. Nenhuma grande empresa pode escapar dela. Se elas não têm isso agora, terão de tê-lo mais cedo ou mais tarde, e, se continuarem a desenvolver-se eventos como o fazem no presente, elas terão que ter isso mais cedo."* (Martins, 2015).

3.2. A Auditoria Interna - Terceira Linha de Defesa

Verifica-se assim, que a auditoria interna vem ganhando nos últimos anos um espaço cada vez mais relevante nas organizações, assumindo o papel de agente principal numa estrutura sólida de governação.

Observar, indagar, questionar e avaliar, estas são algumas das atividades da auditoria interna, que trabalha com o objetivo de agregar valor à organização. A auditoria interna consegue alcançar esse objetivo quando analisa de forma inteligente os riscos, controlos e processos, e como resultado dessas análises, contribui de maneira relevante e direta para a eficácia e eficiência dos processos de governação, gestão de risco e controlos internos. Quando se analisa o modelo das três linhas de defesa, podemos observar que, numa estrutura de governação eficaz, de gestão dos riscos e controlos internos, a auditoria

interna aparece na Terceira Linha de Defesa, ficando ao cargo desta (detendo alto nível de independências, diferente da 1ª e da 2ª linha de defesa), fornecer ao órgão de governação e à gestão de topo, avaliações abrangentes, conforme figura 5.

Figura 5: Modelo de Três linhas de defesa **Fonte:** IIA (2013)

Segundo (IIA, 2013) essas avaliações, cobrem normalmente:

- Uma grande variedade de objetivos, incluindo a eficiência e a eficácia das operações; a salvaguarda de ativos; a confiabilidade e a integridade dos processos de reporte; e a conformidade com leis, regulamentos, políticas, procedimentos e contratos.
- Todos os elementos integrantes da estrutura de gestão de riscos e de controlo interno, que incluem: o ambiente de controlo interno; todos os elementos da estrutura de gestão de riscos da organização (isto é, identificação de riscos, avaliação de riscos e resposta); informação e comunicação; e supervisão. (componentes COSO)
- A entidade como um todo, as suas divisões, subsidiárias, unidades operacionais e funções - incluindo os processos de negócio, tais como vendas, produção, marketing, segurança, funções voltadas para o cliente e operações - assim como as funções de suporte.

No entanto, muito embora a área de auditoria interna esteja posicionada como a terceira linha de defesa, é percetível notar a mudança de entendimento sobre a auditoria interna e do seu papel dentro das organizações.

Anteriormente, a auditoria interna era vista como uma área segregada, pouco amigável e que trabalhava com o único foco de encontrar problemas e "apontar o dedo", sendo que atualmente é imprescindível que tenha uma atuação como parceiro do negócio, que ao mesmo tempo age como sendo os olhos da administração, agrega valor com propostas importantes e relevantes, ajudando as demais áreas e contribuindo com a estratégia da companhia.

Uma empresa que possui uma boa estrutura de governação, com uma área de auditoria interna presente, consegue antecipar-se aos problemas, aperfeiçoar-se em termos de gestão de riscos, além de evoluir de forma contínua nos seus controlos internos.

3.3. A Auditoria Interna e a Gestão de Risco

No início, os auditores internos não despendiam muitas preocupações com a gestão do risco empresarial (velho paradigma). Hoje, com os contributos dados pelo COSO, existe uma abordagem mais formal e exigente para o pensamento baseado no risco, o que estimula os auditores internos a possuírem maior atenção nesta área quando planeiam e desempenham muitas das suas atividades.

No seguimento do ERM emitido pelo COSO, o IIA veio esclarecer a posição da Auditoria Interna, considerando que:

> *"O principal papel da Auditoria Interna no processo de gestão de risco é fornecer segurança objetiva acerca da eficácia das atividades de gestão de risco das organizações, para ajudar a assegurar que os principais riscos do negócio estão a ser geridos de forma apropriada e que o sistema de controlo interno está a funcionar eficazmente" (IIA, 2009).*

De acordo com Ferreira (2010) citando McNamee (1997), a Auditoria Interna baseada em riscos, melhora o modelo de avaliação de riscos e altera o "foco" da Auditoria Interna, que em vez de olhar para os processos de negócio como fazendo parte de um sistema de controlo, analisa-os numa perspetiva de risco.

Uma auditoria baseada no risco acrescenta mais valor a uma organização do que uma auditoria assente nos controlos, uma vez que os controlos por si só não garantem o sucesso.

Castanheira e Rodrigues (2009) citando Maynard (1999), partilham da opinião de que um adequado processo de avaliação de risco é a chave para a auditoria interna desenvolver uma adequada abordagem baseada no risco.

O IIA contribuiu para esta melhoria, emanando normas onde refere a responsabilidade profissional para considerar o risco. As normas onde enumera esta função (risco) são: planeamento (2010), natureza do trabalho (2100) e as de gestão do risco (2120).

Em concordância com a norma interpretativa 2120 do IIA o auditor interno está em condições de averiguar se o processo de gestão do risco é eficaz, se

> *"os objetivos da organização sustentam e estão alinhados com a missão da entidade; os riscos significativos são identificados e avaliados; são selecionadas as respostas adequadas que alinham os riscos com a apetência ao risco da organização; e a informação relevante sobre o risco, é identificada e comunicada em tempo oportuno transversalmente pela empresa, permitindo que o pessoal, os gestores e o Conselho de Administração cumpram com as suas responsabilidades"*.

Os principais fatores a considerar na determinação do papel da auditoria interna são: se a atividade tem riscos quanto à independência e objetividade da atividade da auditoria interna; e se aperfeiçoa os processos de gestão de riscos, controlo e governação da organização, conforme tabela 2.

Papel fundamental da AI em Relação Gestão de Risco	Dar garantia dos processos de gestão Risco; Dar garantia que os riscos são corretamente avaliados; Avaliar os processos de gestão de risco; Avaliar o processo de reporte dos riscos; Rever a gestão dos riscos.
Papel legítimo da AI com salvaguardas	Facilitar a identificação e avaliação dos riscos; Orientar a administração na resposta ao risco; Coordenar as atividades de Gestão de Risco; Reporte consolidado sobre os riscos; Manter e desenvolver a estrutura da Gestão de Risco; Defender a implementação da Gestão de Risco.
Papel que a AI não pode assumir	Estabelecer o apetite pelo risco; Responsabilizar-se pela gestão de risco; Implementar respostas aos riscos em nome da administração; Tomar decisões sobre a resposta a dar ao risco; Impor processos de gestão de risco;

Tabela 2: O papel AI na Gestão Risco **Fonte:** Adaptado IIA 2009b

3.4. O papel da auditoria interna no processo de controlo interno e de gestão de risco

Para as organizações terem sistemas de gestão do risco e controlo interno, interligados e integrados com os objetivos estratégicos da entidade, é impossível desagregar tal realidade do papel da auditoria interna.

Segundo Castanheira e Rodrigues (2009), no estudo *dos "fatores associados à adoção de abordagens baseadas no risco no processo de auditoria interna"*, promovido pelo IPAI, refere que a auditoria interna tem algum tipo de envolvimento no processo de gestão de risco, para além de uma eventual intervenção na implementação do mesmo.

Castanheira e Rodrigues (2009), citam estudos sobre AI envolvendo gestão de risco e controlo interno, realizados por:

- Walker et al. (2003), num estudo executado a cinco organizações de topo (FirstEnergy Corp., General Motors Corp., WalMart Stores Inc., Unocal Corp. e Canadá Post Corp.), acerca do papel da auditoria interna no processo de gestão de risco, concluíram que a função de auditoria interna estava diretamente relacionada com o processo de gestão de risco, depois da implementação dos devidos processos.
- Merkley & Miccolis (2002) referem um estudo, que revelou um profundo interesse em ERM. O estudo concluiu que os responsáveis por liderar o processo de ERM, regra geral, são provenientes da área de auditoria interna.
- Beasley et al. (2005), estudaram a relação entre várias características organizacionais e o impacto da Gestão de Risco na função de auditoria interna, tendo concluído que o ERM tem um maior impacto nas atividades de auditoria interna quando é maior a maturidade do processo de Gestão de Risco, quando a Gestão e a Comissão de Auditoria apelam a uma maior atividade de auditoria interna relacionada com ERM, quando o responsável de auditoria tem uma maior influência.

Capitulo IV – Metodologia

4.1. Enquadramento teórico

Sousa e Baptista (2011) definem as metodologias de investigação como "*um processo de seleção da estratégia de investigação, que condiciona, por si só, a escolha das técnicas de recolha de dados, que devem ser adequadas aos objetivos que se pretendem atingir*".

Assim, segundo Moreira (2016) *"após, uma revisão de literatura e através do levantamento das objeções e hesitações desencadeadas ao longo da revisão, deve-se obter prova através de uma abordagem metodológica que nos permita aplicar/defender uma teoria científica."*

Popper (1972) salientou o facto de a ciência se basear em conjeturas e refutações. A ciência não é verdadeira, mas conjeturável. Uma teoria só é científica se puder ser contestada.

Em sentido amplo, existem dois tipos de abordagens metodológicas de investigação: quantitativa e qualitativa (ou mista, conjunto das duas).

Prodanov e Freitas (2013) defendem que os métodos de investigação estão interligados.

Segundo Sousa e Baptista (2011) os métodos qualitativos relevam para positivismo lógico e têm como objetivos:

- Identificação e apresentação de dados, indicadores e tendências observáveis. Através de medidas numéricas para testar hipóteses, mediante uma rigorosa recolha de dados, ou procura de padrões numéricos, permitindo uma generalização dos resultados obtidos.

Os mesmos autores, no que diz respeito aos métodos qualitativos defendem a fenomenologia e compreensão, que tem como objetivos:

- Analisar comportamentos, atitudes ou os valores. Não generalizando os dados, sendo de caracter holística e indutiva.

4.2. Opção metodológica

O método de investigação a seguir neste estudo é o método qualitativa, com a técnica de recolha de dados através de um inquérito por questionário de resposta mista, visando "*quantificar uma multiplicidade de dados e proceder, por conseguinte, numerosas análises de corelação*" (Quivy &, Campenhout 2005).
A opção justifica-se pela menor dificuldade de comunicação com o universo da amostra populacional, e celeridade na obtenção de respostas do inquérito, sendo a principal génese de recolha da informação para este estudo.

4.3. Questão de Investigação

A questão de investigação que permitirá dar prosseguimento ao nosso estudo e deste modo constituir a nossa metodologia de investigação. A questão levantada é:

Como os Auditores Internos Portugueses vêm o Risco de Interrupção do Negócio

Objetivos:

1. Analisar a sensibilidade relativamente à existência do RIN;
2. Analisar o processo de Gestão do RIN; e
3. Analisar a ocorrência/impacto do RIN.

4.4. Recolha de dados

As organizações portuguesas, de uma forma genérica, não são inquiridas em estudos de risco de interrupção do negócio, nesse sentido consideramos o auditor interno de cada uma das empresas inscritas como membros coletivos do IPAI, depreendendo que dispõem de maior sensibilidade para a área de risco e controlo interno.

Solicitamos a colaboração do IPAI, para a partilha do nosso inquérito perante as entidades selecionadas, que prontamente responderam ao nosso pedido.

Este mesmo organismo enviou os inquéritos, a oito de setembro de dois mil e dezassete, via correio eletrónico, com carta de apresentação e o respetivo *link* do inquérito realizado *online* na plataforma *Google Forms* (anexo 1). O inquérito foi dividido em duas partes: 1.ª parte caracterização da amostra, existência do risco de interrupção do negócio e se o

mesmo foi avaliado; e 2.ª parte avaliação do processo de gestão de risco, se ocorreu o risco de interrupção do negócio e qual o seu impacto.

Foram enviados 65 e-mails, representativos da nossa população, para 65 auditores internos (65 empresas), só foi possível uma resposta por empresa.

Capítulo V – Análise de Dados

5.1. Caraterização da Amostra

Da nossa população de 65 auditores, obtivemos 28 respostas válidas, representativas da nossa amostra em 43%. De salientar que estamos perante uma amostra bastante estratificada.

Analisando as empresas que os auditores internos exercem funções, na nossa amostra verificamos que 36% (n=10) das empresas tem como ramo de atividade o sector financeiro e seguros, 18% (n=5) indústria, construção e saúde 11% (n=6), os restantes 35% (n=7) correspondem ao setor de aviação e espaço, comunicações, automóvel e concessão rodoviária.

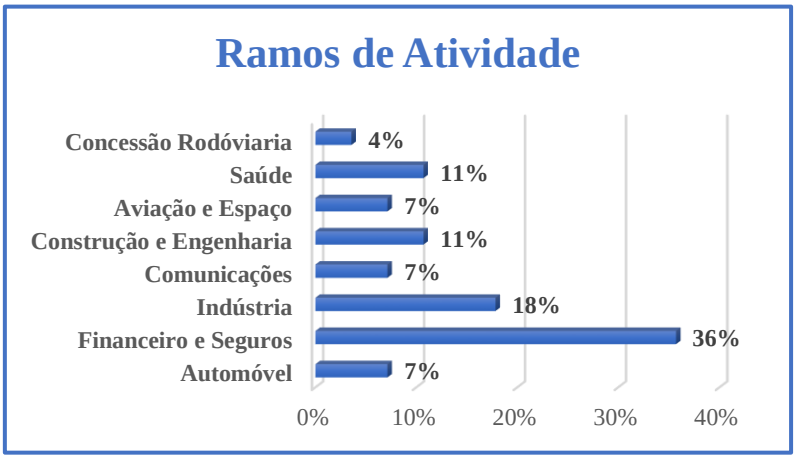

Gráfico 1: Ramos de Atividade

Da nossa amostra, relativamente ao volume de negócios, 82% (n=23) correspondem a um volume de negócios maior que 40.000.000 euros, 11% (n=3) maior que 700.000 euros e 8.000.000 euros, os restantes 8% (n=2) menos que 700.000 euros e entre 8.000.000 euros e 40.000.000 euros.

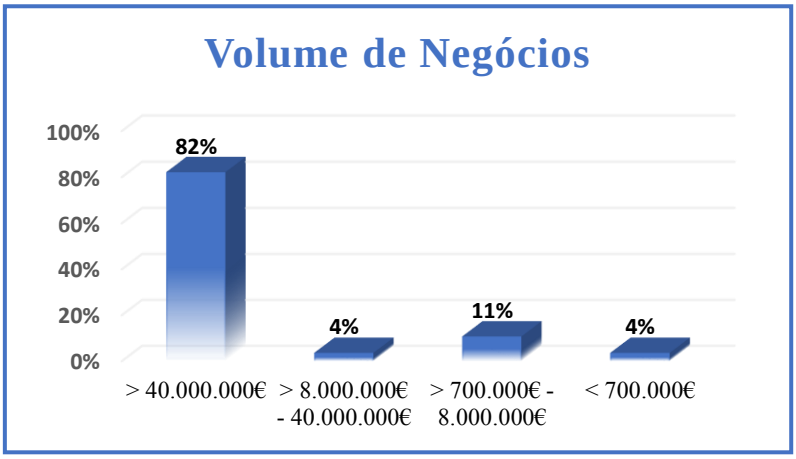

Gráfico 2: Volume de Negócios

Por função desempenhada, 86% (n=24) correspondem a auditores internos, 11% (n=3) correspondem a gestores de risco e 4% (n=1) correspondem a coordenador de auditoria interna.

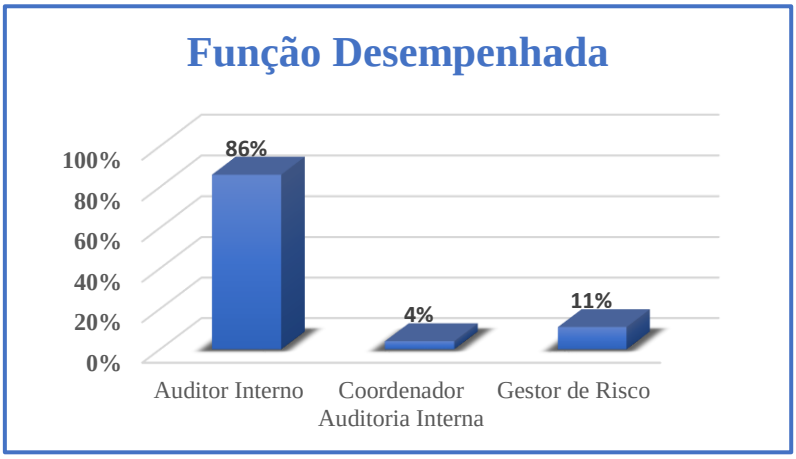

Gráfico 3: Função Desempenhada

5.2. Risco de Interrupção do Negócio

À questão sobre a existência do RIN, 82% (n=23) responderam haver risco, e 18% (n=5) disseram não existir esse risco. A estes 18%, questionados se houve processo de avaliação do RIN, 100% dizem não haver avaliação. Destes, 40% correspondem ao setor da saúde e 60% em igual proporção aos sectores de construção e engenharia, indústria, e financeiro e seguros. Uma das funções de auditoria interna consiste na avaliação de risco, o que nos permitiu concluir por um contrassenso relativamente à perceção da função de auditor interno.

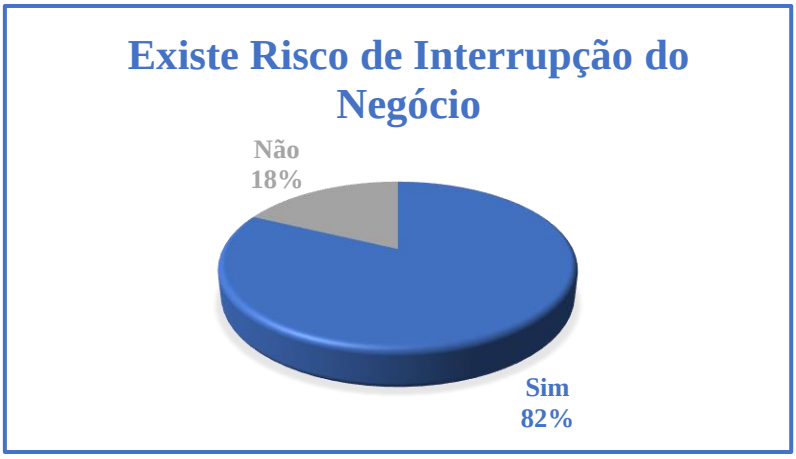

Gráfico 4: Existe RIN

Após a resposta às questões sobre se existe risco de interrupção e se o mesmo tinha sido avaliado, a nossa amostra ficou reduzida a 23 respostas, representativa de 35% da população. À questão sobre se já ocorreu o RIN, 74% (n=17) responderam não ter ocorrido, 17% (n=4) dizem já ter ocorrido e 9% (n=2) desconhecem se o mesmo ocorreu.

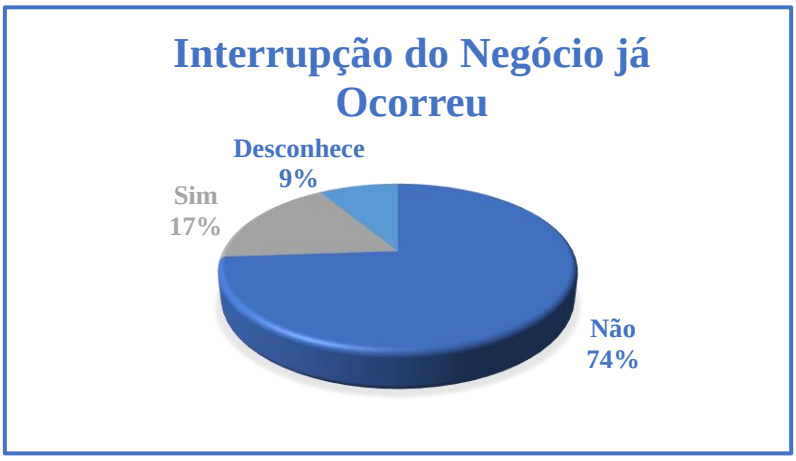

Gráfico 5: Ocorrência de RIN

Dos inquiridos que responderam já ter ocorrido RIN, foi inquirido qual o seu impacto, quais as medidas tomadas e se consideravam que a empresa estava preparada, as respostas foram as seguintes:

Questão / Sector de Atividade	Qual impacto?	Quais as medidas tomadas?	Preparada?
Construção e Engenharia	Custos para a empresa	Reposição das condições de funcionamento	Sim
Construção e Engenharia	Perda do capital investido	Contenção do contágio a outras entidades do grupo	Não
Concessão Rodoviária	Variável	Corretivas para resolver a situação	Sim
Indústria	Paragem da produção	Implementação da gestão de riscos	Não

Tabela 3: Impacto, Medidas, Preparação

De referir que 50% dos negócios que sofreram interrupção de negócio não estavam preparados, tendo o impacto sofrido sido essencialmente perdas financeiras, o que nos leva a equacionar que talvez o seguro de interrupção de negócio teria sido uma mais valia, assegurando o volume de negócio não realizado e os custos fixos.

5.3. Processo de Gestão de Risco de Interrupção do Negócio

À questão sobre quem identifica o RIN, 48 % (n=11) afirmaram ser a gestão de topo; 35% (n=8) identificaram ser a gestão de risco e 17% (n=4) ser a gestão operacional. O COSO ERM menciona que uma visão global dos riscos advém da gestão de topo, ao contrário de muitas organizações que procedem à gestão do risco ao nível da gestão operacional. Efetivamente dos 3 dos inquiridos que incorreram no RIN aferiram ser a gestão operacional a identificar o mesmo.

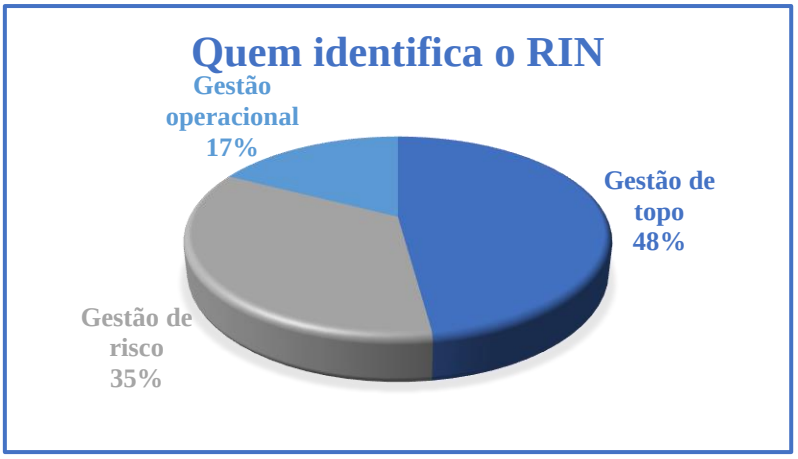

Gráfico 6: Identificação do RIN

Na questão relativa a quais os fatores que provocam a ocorrência do RIN era permitido selecionar mais do que uma hipótese. Foram obtidas 93 respostas. O fator catástrofes naturais predominou com 18% das respostas (n=17), ciberataques 16% (n=15), falhas técnicas 15% (n=14) e guerra/ terrorismo e fogo/explosão 12% (n=24).

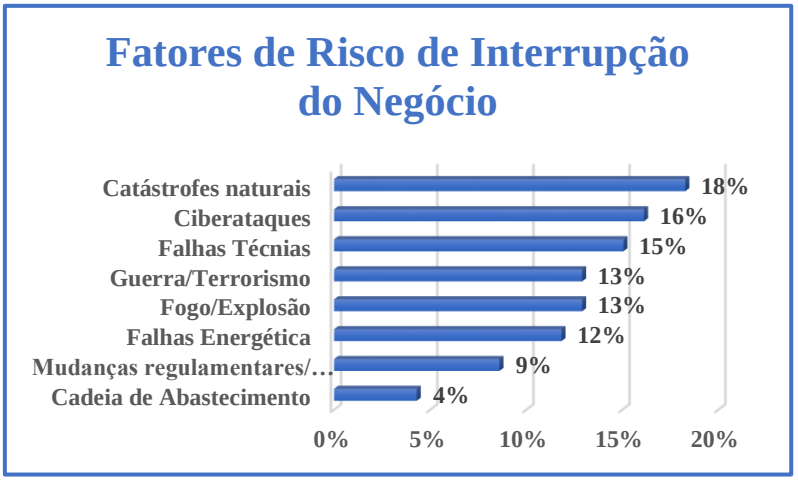

Gráfico 7: Fatores de RIN

Apesar de Portugal não ter sido inquirido no estudo elaborado pela AGCS, os fatores de risco mencionados vão de encontro às respostas obtidas naquele estudo. Estes fatores ou outros são identificados como os que, a montante, podem originar a interrupção do negócio.

Relativamente à questão colocada sobre se o RIN é considerado como inerente ou residual, 57% (n=13) mencionaram ser inerente, sendo um risco diretamente relacionado com a atividade, independentemente dos controlos aplicados; no entanto 43% (n=10) referiram ser residual, isto é, o risco remanescente, após aplicados os controlos.

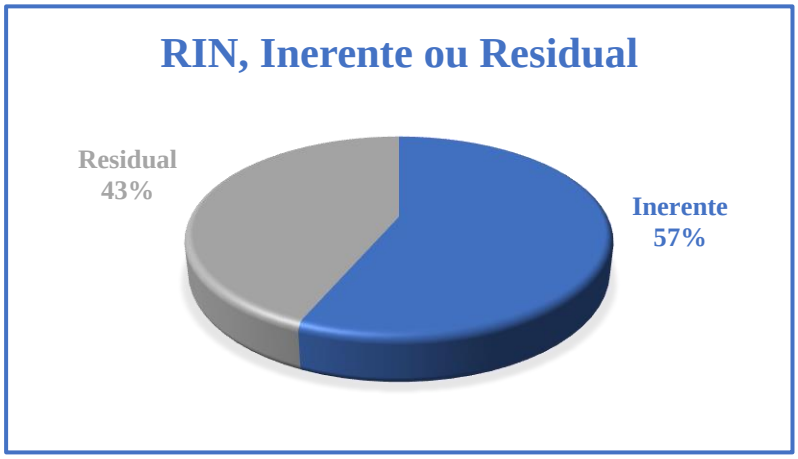

Gráfico 8: RIN Inerente ou Residual

Na questão sobre os métodos utilizados para avaliação do RIN, 91% (n=21) responderam uma avaliação qualitativa e 9% (n=2) uma avaliação quantitativa. Aos que responderam avaliação quantitativa questionou-se qual critério/indicador utilizado, sendo as respostas obtidas o critério RTO (*Recovery time objective*/tempo de recuperação) e o critério RPO (*Recovery point objective*/ponto de recuperação), sendo que o RPO significa o tempo máximo durante o qual os dados não foram salvaguardados, antes do desastre e o RTO significa o tempo máximo para colocar os sistemas novamente *Online*, após desastre ou interrupção dos serviços. De salientar que foi o setor financeiro e seguros que referiu o uso do método de avaliação quantitativa.

Relativamente à questão relativa aos tipos de controlos aplicados, sendo possível a múltipla escolha, foram obtidas 53 respostas. 40% (n=21) responderam controlos preventivos, 24% (n=13) responderam controlos detetivos e 21% (n=11) indicaram controlos corretivos. Concluímos assim pela predominância de controlos para impedir e detetar factos indesejados.

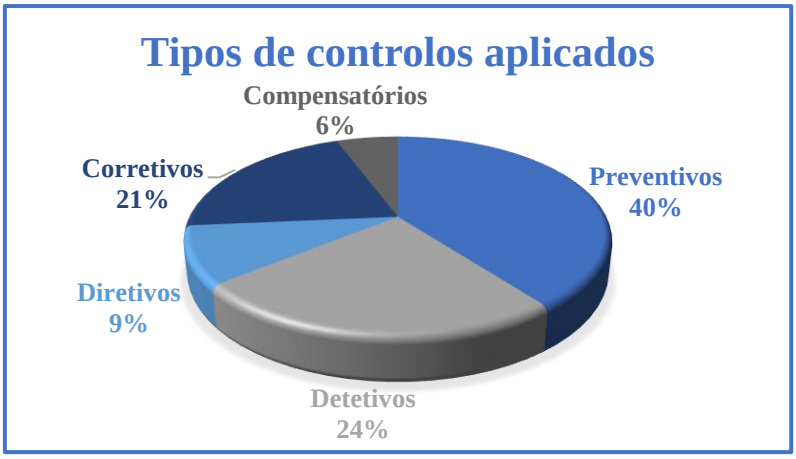

Gráfico 9: Tipos de controlos aplicados

Relativamente à questão sobre o tipo de resposta utilizada quanto à gestão do RIN, 78% (n=18) dos auditores internos responderam mitigar, 9% (n=4) aceitar e evitar e 4% (n=1) transferir. No entanto os que incorreram no RIN optaram pelas respostas "mitigar, aceitar e evitar".

De salientar, que cada vez mais a transferência deste risco é de enorme importância devido à volatilidade de fatores. A interrupção pode ser uma consequência secundária, que pode colocar em causa a função vital da organização, sendo que uma interrupção total ou parcial é sempre prejudicial para a entidade. Só um inquirido, do sector da indústria, optou pela hipótese "transferir o risco".

Gráfico 10: Resposta ao RIN

Relativamente à questão sobre quem decide sobre o RIN, 87% (n=20) identificaram ser a gestão de topo; no entanto, 9% (n=2) responderam ser a gestão operacional e 4% (n=1) a gestão de risco.

Gráfico 11: Decisão sobre RIN

Na pergunta quanto à periocidade de avaliação do risco, 39% (n=9) afirmaram ser a avaliação anual, 22% (n=9) trimestral, 17% (n=4) bianual, 13 %(n=3) semestral e 9% (n=2) indicaram que não é realizada qualquer avaliação periódica.

De salientar que 70% dos inquiridos indicaram fazer avaliações em pelo menos 360 dias. Destacamos que os inquiridos do sector da construção e engenharia que responderam já ter ocorrido o RIN responderam não efetuar avaliações periódicas. Já os outros inquiridos do setor indústria e concessão rodoviária, dizem efetuar avaliação semestral e anual respetivamente.

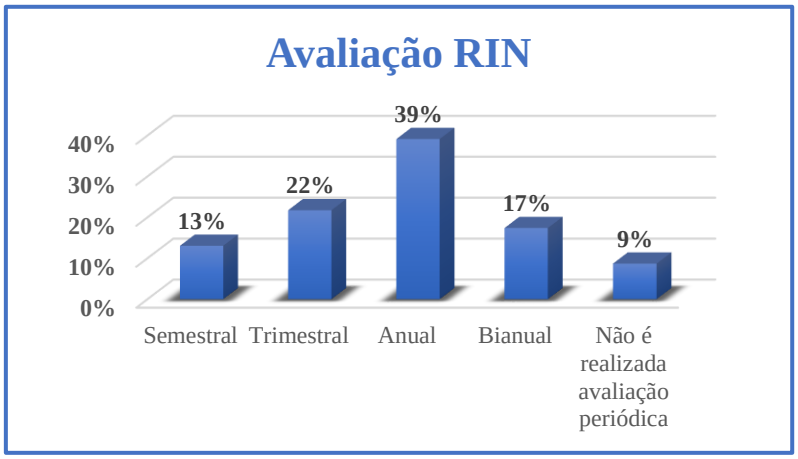

Gráfico 12: Avaliação RIN

Perante a análise de dados recolhidos, foi possível retirar as seguintes conclusões:

- Ao selecionarmos empresas com auditores internos membros do IPAI, destaca-se o facto de estas já deterem sensibilidade para a auditoria interna. No entanto, verificou-se que 18% dos auditores internos das empresas inquiridas terem respondido não existir um processo de avaliação de risco e automaticamente respondem não existir risco de interrupção do negócio.

Sendo uma das funções do auditor interno efetuar o processo de avaliação de risco, podemos determinar, com base nas respostas de 18% dos auditores internos, que estamos perante um contrassenso com a função do auditor interno.

Falamos de sectores tais como o da saúde, da construção e engenharia, do financeiro e seguros e da indústria, com volume de negócios superiores a 40.000.000€. O que nos leva a pensar que estes auditores não estão sensibilizados para o conceito de risco de interrupção do negócio.

- 82% dos auditores internos das empresas dizem existir RIN. Porém no processo de gestão de risco, existem lacunas na sua execução. Uma vez que 17% dos auditores internos menciona que é a gestão operacional quem identifica o RIN. E 9% afirma que é a gestão operacional quem toma a decisão do RIN. Contrariamente o que define a gestão de risco empresarial.

- 57% dos auditores internos afirmam que o RIN na empresa em que exercem funções é avaliado como risco inerente, isto é, diretamente relacionado com atividade. Sendo que estes, maioritariamente, estes afirmam como resposta ao risco, a mitigação. No entanto, existe um infindável número de fatores de risco, podendo aferir que neste risco dificilmente depois de aplicados todos os controlos é um risco residual.

- 40% dos auditores internos aplicam controlos preventivos, no sentido de detetar incidentes.

- Dos 4 Auditores que afirmaram ter ocorrido interrupção do negócio, e salientam-se outros 2 auditores que desconhecem a ocorrência do mesmo. Estes últimos mencionam existir avaliação anual, o que é um contrassenso desconhecerem uma interrupção do negócio.

Relativamente às empresas que ocorreram na interrupção do negócio, retiramos como conclusões:

- 50% das empresas que ocorreram no RIN, responderam não estarem preparadas para interrupção do negócio, sendo que pelo menos uma, implementou de gestão de risco, o que nos leva a concluir que não existia gestão de risco previamente. No entanto, esta atualmente descreve corretamente o processo de gestão de risco e o mesmo é avaliado semestralmente, de referir que é uma empresa com um volume de negócios inferior a 700.000 euros.

- Dos 3 dos acidentados afirmam ser a gestão operacional a identificar o RIN, dois desses afirmam não existir avaliação periódica, pertencendo estes ao sector da construção e engenharia. O que nos leva a concluir que este é o sector mais exposto ao risco, porque não existe um sistema de gestão de risco a funcionar corretamente. Uma vez que, apesar dos acontecimentos, aparentemente, as medidas de gestão de risco não foram revistas ou implementadas.

Capítulo VI – Conclusões

A gestão de risco é parte integrante do controlo interno, agregando uma visão global dos riscos a partir do topo. A nova framework do COSO, vem salientar que a gestão de risco é constituída pela cultura da organização. Evidenciando que o risco está sempre presente no nosso dia a dia.

É necessário que cada vez mais as organizações detenham sistemas apropriados de gestão do risco e controlo interno, interligados e integrados com os objetivos estratégicos da entidade e que os auditores internos acompanhem a evolução.

A nossa amostra tem como público alvo auditores internos de empresas inscritas no IPAI, com sensibilidade para auditoria interna, gestão de risco e controlos internos. Apesar de reduzida, na nossa amostra recolhida reflete 43% da população. De salientar que 82% apresenta um volume de negócios superior a 40.000.000€, de forma genérica, grandes empresas.

Para concluir, à questão "Como Auditores Internos Portugueses vêm o Risco de Interrupção do Negócio", podemos aferir que maioritariamente os auditores internos, tem sensibilidade para o RIN, no entanto o processo de gestão de risco é bastante débil, de salientar a nível essencialmente da sua identificação e do processo de tomada de decisão.

As empresas que incorreram na interrupção do negócio tiveram essencialmente perdas financeiras, no entanto não optaram pela transferência do risco. As mesmas empresas não tinham e algumas continuam a não ter um adequado ou quase inexistente processo de gestão de risco.

Os auditores internos quando planeiam o seu trabalho devem ter em consideração os riscos de forma genérica, o risco de interrupção de negócio, a montante, pode ser um fator de risco, de outro risco. Logo este está sempre em constante avaliação através dos seus fatores, isto é, se forem realizadas respetivas avaliações e deteções pela gestão de topo.

De salientar que o RIN ocupa o primeiro lugar no ranking mundial, tem uma multiplicidade de fatores de risco o que se torna de difícil mitigação e prevenção, sendo a mitigação opção de resposta em 78% pelos auditores internos questionados. Este é um risco verídico que necessita de gestão e monitorização. As vantagens da implementação de um sistema gestão de risco e controlo interno são inerentes para toda a cultura estratégica da organização.

Limitações Estudo

No desenvolver da presente dissertação, fomo-nos debatendo com algumas limitações, nomeadamente quanto à recolha de informação sobre o risco de interrupção do negócio. Uma vez que as empresas seguradoras não divulgam dados, Portugal não realiza estudos nesta vertente e também não fazemos parte de estudos internacionais.

Outra dificuldade foi a obtenção de respostas por parte dos auditores internos, embora tendo sido enviados questionários às 65 empresas destinadas apenas a um auditor interno, apenas obtivemos 28 respostas válidas, uma vez que obtivemos respostas com profissões diferentes das de auditor interno ou relacionadas.

Embora a realização de amostragem nos permita tentar chegar a uma probabilidade bastante próxima da realidade, relativamente a empresas com sensibilidade para a auditoria interna não podemos concluir que a amostra seja representativa de um sector de atividade.

Porém, consideramos que o número de respostas obtidas nos permitiram efetuar uma análise fiável e conclusiva face às questões abordadas.

Orientações para futuras investigações

Para investigação futura sugerimos a realização de estudos na vertente da gestão de topo, sobre qual a perceção do RIN. Assim como perceber porque as organizações não transferem o risco.

Poder-se-ia também propor um estudo mais pormenorizado de um sector de atividade, caracterizando os principais fatores de risco, incidentes e procedimentos da gestão de risco numa vertente de auditoria interna e gestão do topo.

Referências bibliográficas

Autores

Alves, J. (2015). Princípios e Práticas de Auditoria e Revisão de Contas (1ª Edição). Lisboa: Edições Sílabo. (p. 33 – 35)

Azevedo, C. (2016). *Walmsley on Business Interruption Insurance* (2ª Edição). *Witherby Insurance*. (p. 1 – 15)

Beja, R., (2004). *Risk Management* – Gestão, Relato e Auditoria dos Riscos do Negócio; Lisboa: Áreas Editora, S.A.

Castanheira, N. & Rodrigues, L. (2009) Fatores Associados à Adoção de Abordagens Baseadas no Risco no Processo de Auditoria Interna. IPAI.

Castanheira, N. (2007). Auditoria Interna Baseada no Risco – Estudo do Caso Português. Dissertação de Mestrado em Contabilidade e Auditoria, Universidade do Minho, Braga.

Costa, C. (2014). Auditoria Financeira – Teoria & Prática (10ª Edição). Lisboa: Letras e Conceitos. (p. 80 – 90)

Ferreira. A. (2010). A Gestão de Risco Aplicada à Auditoria Interna. Dissertação de Mestrado em Contabilidade e Auditoria, Universidade de Aveiro.

Martins, D. (2015). A implementação da Auditoria Interna numa Câmara Municipal do Minho. Relatório de Estágio de Mestrado em Auditoria. ISCAP.

Morais, G. & Martins, I. (2007). Auditoria Interna – Função e Processo (3ªEdição). Lisboa: Áreas Editora. (p. 28 – 89)

Moreira, L. (2016). Avaliação do Risco de Fraude nas Autarquias Locais. Dissertação de Mestrado em Auditoria. ISCAP.

Pinho, P., Valente, R., Madaleno, M. & Vieira, E. (2011). Risco Financeiro – Medida e Gestão (1ª Edição). Lisboa: Edições Sílabo. (p 14 – 16)

Popper, Karl Raimund, (1972). Karl Popper A Lógica da pesquisa científica, Universidade São Paulo.

Prodanov, C. e Freitas E. (2013). Metodologia do Trabalho Cientifico: Métodos e Técnicas de Pesquisa e do Trabalho Académico (2ª Edição). Brasil: Feevale.

Quivy, R. e Campenhoudt, L. (2005). Manual de investigação em ciências sociais, (4ª Edição). Lisboa: Gradiva.

Santos, M. (2013). O Controlo Interno e a Gestão de Riscos nas Empresas da Área Metropolitana do Porto. Dissertação de Mestrado em Auditoria. ISCAP.

Silva, P. (2016). Diretrizes para a elaboração de um Plano de Continuidade de Negócios – Estudo de Caso. Dissertação em Sistemas de Informação Organizacionais. IPS.

Sousa, M. e Baptista, C. (2011). Como fazer investigação, dissertações, teses e relatórios – segundo Bolonha (1ª Edição). Lisboa: Pactor.

Suárez, T. (1976). *El Seguro de pérdidas de beneficios por interrupción de la empresa, Jerez de la Frontera*. (p. 31 – 45)

Webgrafia

AGCS (2017). *Allianz Risk Barometer – Top BusinessRisks 2017*. Disponível em: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdfAcesso: fevereiro 2017.

COSO (2007) - *Committee of Sponsoring Organizations of the Treadway Commission*. Gerenciamento de Riscos Corporativos - Estrutura Integrada. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf.Acesso: setembro 2017.

COSO (2013) - *Committee of Sponsoring Organizations of the Treadway Commission*. *Internal Control - Integrated Framework*. Disponível em: https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf. Acesso: maio 2017.

COSO (2017) - *Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Managemente - Integrating with Strategy and Performance*. Disponível em: http://www.coso.org/-erm.htm. Acesso: setembro 2017.

Ferma (2003). *Federation of European Risk Management Associations* - Norma de Gestão de Riscos. Disponível em: http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdfA: setembro 2017.

Gasiorowski-Denis, E. (2012). *Business continuity - ISO 22301 when things go seriously wrong.* Disponivel: https://www.iso.org/news/2012/06/Ref1602.html Acesso: agosto 2017.

IFAC (2007). *Internal Control from a Risk-Based Perspective.* Disponível em: http://www.ifac.org/sites/default/files/publications/files/internal-control-from-a-ris.pdf.Acesso: maio 2017.

IIA (2009, a). *The Institute of Internal Auditors* – Enquadramento internacional de práticas profissionais de Auditoria Interna. Disponível em: http://www.ipai.pt/fotos/gca/ippf_2009_port_normas_0809_1252171596.pdf.Acesso: maio 2017.

IIA (2009, b) *The Institute of Internal Auditor*s – O papel da Auditoria Interna no gerenciamento de riscos corporativos. Disponível em: http://www.iiabrasil.org.br/new/IPPF_declaracao_posicionamento.html.Acesso: junho 2017.

IIA (2013) *The Institute of Internal Auditors* - As Três Linhas De Defesa no gerenciamento eficaz de riscos e controles. Disponível em: https://na.theiia.org/standards-guidance/Public.pdf Acesso: setembro 2017.

INTOSAI (2008) – *International Organization of Supreme Audit Institutions.* Disponível em: http://www.issai.org/media/13329/intosai_gov_9100_e.pdf.Acesso: maio 2017.

ISO 22301 (2012). *Societal security - Business continuity management - Requirements. Societal security - Business continuity management systems - Requirements. ISO.* Disponível: www.iso.org. Acesso: setembro 2017.

Marsh (2016). *Continental European Cyber Risk Survey: 2016.* Disponível: https://www.marsh.com/content/dam/marsh/Documents/PDF/eu/en/Continental%20European%20Cyber%20Risk%20Survey%202016%20Report.pdfAcesso: setembro 2017.

Santos, R. F. (2009). Gestão de Risco e Controle Interno. Disponível em: http://pt.scribd.com/doc/35413699/Gestao-de-Risco-e-Controle-Interno-com-COSO. Acesso: setembro 2017.

Segurdata (2017). Indicadores de Gestão Multirriscos. Disponível em: https://segurdata.apseguradores.pt/apex/f?p=100:0:14903930707347:APPLICATION_PROCESS%3DDOWNLOAD_FILE:NO::APP_FILE_ID,APP_FILE_ID_CHECK:30576,616Acesso: outubro 2017.

Legislação e Normas

Decreto Lei nº72/2008, de 16 de abril - Estabelece o regime jurídico do contrato de seguro.

Decreto Lei nº94-B/98 de 17 de abril - Regula as condições de acesso e de exercício da atividade seguradora e resseguradora no território da Comunidade Europeia, incluindo a exercida no âmbito institucional das zonas francas.

IIA - Norma de desempenho 2010 - Planeamento

IIA - Norma de desempenho 2100 - Natureza do Trabalho

IIA - Norma de desempenho 2120 - Gestão do Risco

Anexo

Os Auditores Internos Portugueses e o Risco de Interrupção do Negócio

Este inquérito/questionário insere-se no âmbito da dissertação do Mestrado em Auditoria, do Instituto Superior de Contabilidade e Administração do Porto, que tem como objectivo avaliar "Os Auditores Internos Portugueses e o Risco de Interrupção do Negócio".
Este, destina-se a um auditor interno de cada uma das empresas inscritas como membros colectivos do Instituto Português de Auditoria Interna.
Toda a informação recolhida é anónima e confidencial, destinando-se exclusivamente para análise estatística de âmbito académico.
Agradeço desde já a sua participação, a qual será muito relevante para as conclusões deste estudo.
Obrigada!

*Obrigatório

1. **1. Qual o sector de atividade em que opera?** *
   Marcar apenas uma oval.

   - ◯ Automóvel
   - ◯ Construção e Engenharia
   - ◯ Power utilites
   - ◯ Agricultura e Pesca
   - ◯ Aviação e Espaço
   - ◯ Distribuição e Consumo
   - ◯ Energia
   - ◯ Hotelaria e Lazer
   - ◯ Saúde
   - ◯ Transportes
   - ◯ Financeira e Seguros
   - ◯ Indústria
   - ◯ Outra: _____

2. **2. Qual o volume de negócios?** *
   Marcar apenas uma oval.

   - ◯ < 700.000€
   - ◯ > 700.000€ - 8.000.000€
   - ◯ > 8.000.000€ - 40.000.000€
   - ◯ > 40.000.000€

3. **3. Qual a função que exerce?** *
   Marcar apenas uma oval.

   - ◯ Auditor interno
   - ◯ Gestor de risco
   - ◯ Controller
   - ◯ Outra: _____

4. **4. Na Entidade em que exerce funções, existe Risco de Interrupção de Negócio (RIN)?** *
   Marcar apenas uma oval.

   - ◯ Sim *Após a última pergunta desta secção, passe para a pergunta 6.*
   - ◯ Não

5. **4.1. Se respondeu não na questão anterior, existiu processo de avaliação?**
   Se respondeu sim na questão anterior, avance para o II parte do inquérito.
   Marcar apenas uma oval.

   - ◯ Sim *Pare de preencher este formulário.*
   - ◯ Não *Pare de preencher este formulário.*

II Parte

6. **5. Quem identifica o RIN?** *
   Marcar apenas uma oval.

   - ◯ Gestão de topo
   - ◯ Gestão operacional
   - ◯ Auditoria interna
   - ◯ Gestão de risco
   - ◯ Outra: _____

7. **6. Quais os factores de risco, que implicam o RIN?** *
   Marcar tudo o que for aplicável.

   - ☐ Catástrofes naturais
   - ☐ Ciberataques
   - ☐ Fogo/Explosão
   - ☐ Falhas técnias
   - ☐ Falhas de energéticas
   - ☐ Guerra/Terrorismo
   - ☐ Cadeia de abastecimento
   - ☐ Mudanças regulamentares/ legislativas
   - ☐ Outra: _____

8. **7. Tendo em conta os conceitos de risco inerente e residual, como classifica o RIN, de acordo com a sua entidade?** *
   Marcar apenas uma oval.

   ◯ Inerente (É o risco diretamente relacionado com a atividade, independentemente dos controlos aplicados)
   ◯ Residual (É o risco remanescente após aplicados os controlos)

9. **8. Quais os métodos utilizados para avaliar o RIN?** *
   Marcar apenas uma oval.

   ◯ Avaliação qualitativa
   ◯ Avaliação quantitativa
   ◯ Outra: _____

10. **8.1. Se respondeu avaliação quantitativa, qual o critério/indicador utilizado?**

    _____

11. **9. Quais os tipos de controlos que são aplicados?** *
    Marcar tudo o que for aplicável.

    ☐ Preventivos
    ☐ Detetivos
    ☐ Diretivos
    ☐ Corretivos
    ☐ Compensatórios
    ☐ Não aplicável
    ☐ Outra: _____

12. **10. Qual o tratamento efetuado ao RIN?** *
    Marcar apenas uma oval.

    ◯ Aceitar
    ◯ Mitigar
    ◯ Transferir
    ◯ Evitar

13. **11. Por quem é tomada a decisão da gestão de risco?** *
    (Por exemplo: contratação de seguros, transferir ou partilhar com clientes/fornecedores)
    Marcar apenas uma oval.

    ◯ Gestão de topo
    ◯ Gestão operacional
    ◯ Auditoria interna
    ◯ Gestão de risco
    ◯ Outra: _____

14. **12. Qual a periodicidade com que avalia este risco, AD HOC considerando que há alterações substantivas nas condições do negócio?** *

Marcar apenas uma oval.

- ◯ Trimestral
- ◯ Semestral
- ◯ Anual
- ◯ Bianual
- ◯ Não é realizada avaliação periódica

15. **13. O RIN já ocorreu?** *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Desconheço

16. **13.1. Se respondeu sim na questão anterior , qual impacto?**

_____

17. **13.2. Quais as medidas tomadas?**

_____

_____

_____

_____

_____

18. **13.3. A entidade estava preparada para RIN?**

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não