ISCAC |

2019

Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Pedro Miguel Domingos dos Reis

A importância da Auditoria Interna e da Gestão de Risco nas empresas do distrito de Leiria

Coimbra, 10 de março de 2019

Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Pedro Miguel Domingos dos Reis

A importância da Auditoria Interna e da Gestão de Risco nas empresas do distrito de Leiria

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria Empresarial e Pública, realizada sob a orientação do Professor Nuno Castanheira.

Coimbra, 10 de Março de 2019

TERMO DE RESPONSABILIDADE

Declaro ser o autor desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

AGRADECIMENTOS

Expresso o meu sincero agradecimento a todos aqueles que contribuíram para que este trabalho fosse possível.

Ao meu orientador, Doutor Nuno Castanheira, expresso a minha especial gratidão pela disponibilidade, apoio demonstrado e crítica construtiva durante a realização desta dissertação.

Ao meu cunhado, pela disponibilidade e ajuda no tratamento estatístico.

Aos meus pais por durante todo este tempo acreditarem e insistirem para que eu concluísse o trabalho.

E por último a minha esposa e principalmente a minha filha por toda a compreensão pelo tempo que todo este processo me privou da sua companhia da forma que desejava.

RESUMO

No actual contexto de globalização, em que as organizações estão sobre uma pressão económica significativa, os gestores de topo procuram formas alternativas de reduzir custos, identificar oportunidades de maximização de proveitos e de melhorar a performance e eficiência da gestão da organização, potenciando a criação de valor para os seus stakeholders.

A gestão de risco empresarial tem vindo assim, a assumir um papel cada vez mais importante na agenda estratégica das empresas, constituindo um elemento fundamental de suporte à gestão num contexto macroeconómico instável e complexo.

Através do profundo conhecimento que tem do sistema de controlo interno, a auditoria interna fornece, deste modo, um contributo necessário e fundamental para a gestão de riscos.

Nesta dissertação pretende-se analisar qual o grau de maturidade da Auditoria Interna nas empresas do distrito de Leiria e de que modo a Gestão de Risco é uma das preocupações dos órgãos de gestão/administração e qual a sua importância estratégica.

Este tema vai ser estudado numa primeira parte, através da revisão de literatura, revendo vários conceitos, que permitirão efetuar um adequado enquadramento do mesmo, e seguidamente procede-se a análise das respostas a um questionário enviado às 250 maiores empresas, em volume de negócios, do distrito de Leiria em 2016.

Através das respostas obtidas o objetivo geral apresentado pode ser comprovado pela conclusão de que a gestão de riscos e a auditoria interna ainda não são uma das prioridades dos órgãos de gestão/administração das empresas de Leiria. No entanto, apesar dos resultados obtidos, a reduzida dimensão da amostra não permite a sua generalização, consistindo esta uma limitação do estudo.

Palavras-chave: Auditoria Interna, Gestão de Risco, Riscos

ABSTRACT

In today's context of globalization, where organizations are under significant economic pressure, top managers look for alternative ways to reduce costs, identify profit maximization opportunities, and improve organizational performance and management efficiency, value for its stakeholders.

Corporate risk management has thus taken on an increasingly important role in the strategic business agenda, constituting a fundamental element of support for management in an unstable and complex macroeconomic context.

Through its in-depth knowledge of the internal control system, internal audit provides a necessary and fundamental contribution to risk management.

This dissertation intends to analyze the degree of maturity of the Internal Audit in the companies of the district of Leiria and how Risk Management is one of the concerns of the management / administration bodies and what their strategic importance is.

This subject will be studied in a first part, through the literature review, reviewing several concepts, which will allow an adequate framework of the same, and then the analysis of the responses to a questionnaire sent to the 250 largest companies in terms of turnover , of the district of Leiria in 2016.

Through the answers obtained the general objective presented can be proven by the conclusion that risk management and internal audit are not yet one of the priorities of the management / administration bodies of Leiria companies. However, despite the results obtained, the small sample size does not allow its generalization, which is a limitation of the study.

Keywords: Internal Audit, Risk Management, Risk

ÍNDICE GERAL

ÍNDICE DE FIGURAS, GRÁFICOS E QUADROS

Lista de abreviaturas, acrónimos

AI – Auditoria Interna

AIBR – Auditoria Interna baseada no risco

AICPA – American Institute of Certified Public Accountants

CI – Controlo Interno

COSO – Comitee of Sponsoring Organizations of the Tradeway Comission

ERM – Enterprise Risk Management

IIA – Institute of Internal Auditors

SCI – Sistema de Controlo Interno

SEC – Securities and Exchange Commission

SOX – Sarbanes Oxley Act

SPSS – Statistical Package for the Social Sciences

INTRODUÇÃO

A velocidade de mudança, a complexidade crescente da economia associada à crise económica mundial que estamos a atravessar, as expectativas cada vez maiores dos consumidores, a agressividade da concorrência, as consequências dramáticas que podem advir das falhas de controlo, a rápida evolução da tecnologia, entre outros fatores, estão a afetar as organizações, expondo-as a uma grande variedade de riscos. Os riscos empresariais podem assumir várias formas e o seu impacto nos stakeholders (acionistas, clientes, fornecedores, colaboradores, entre outros) pode ser inesperado, rápido e atingir grandes proporções. Deste modo, as organizações devem conhecer os riscos que ameaçam o seu negócio, de modo a implementar medidas adequadas que mitiguem estes mesmos riscos e que evitem colocar em causa a concretização dos objetivos e até mesmo a continuidade do negócio.

Risco é um tema muitas vezes evitado pelos executivos das organizações, o que é compreensível, porque muitos pensam nele como uma ameaça ou uma série de eventos negativos que impactam o negócio. Cada vez mais, porém, tem se discutido o outro lado do risco, aquele relacionado à criação de valor, ou seja, o de correr riscos considerando o retorno esperado.

Portanto, deve-se considerar a adoção de uma definição mais abrangente de risco, ponderando igualmente a gestão dos riscos relacionados ao crescimento e á rentabilidade.

A visão moderna diz-nos que as empresas que melhor responderão às mutações que rapidamente estão a acontecer no mercado global, são aquelas que compreendem desde já, de uma forma mais esclarecida, os seus riscos e que alinham essa assumpção de riscos com aquilo que melhor sabem fazer.

Uma das formas encontradas para praticar uma eficiente mitigação dos riscos, passa pela implementação de controlos que poderão auxiliar, na deteção dos mesmos, assim como possibilitar que estes tenham um impacto menos significativo numa organização.

Um importante coadjuvante na implementação desses mesmos mecanismos de controlo é a Auditoria Interna.

É neste enquadramento que se entende ser relevante conhecer a forma como a Auditoria Interna pode articular-se com a Gestão de Risco com vista á criação de valor.

Pretende-se com este trabalho, perceber até que ponto a gestão de risco é uma preocupação das empresas portuguesas, nomeadamente no distrito de Leiria, e se estas estão atentas às rápidas mudanças nos mercados de modo a se poderem posicionar no mercado, de forma a aproveitarem as oportunidades que surgem e a reduzir os riscos.

O objetivo, mais propriamente, é perceber qual o grau de maturidade da Auditoria Interna nas empresas do distrito de Leiria e de que modo a gestão de risco é uma das preocupações dos órgãos de gestão e qual a importância estratégica para as empresa de Leiria.

Nesse sentido, o trabalho realizado divide-se em duas partes, sendo a primeira constituída por três capítulos, onde se efetua uma revisão de literatura, abordando conceitos e processos relativos a auditoria interna, gestão de riscos e a relação existente entre um processo de auditoria interna e a sua focalização na gestão de riscos.

Na segunda parte do trabalho efetua-se uma descrição sobre o modo como a investigação será realizada, descrevendo os procedimentos adotados e as variáveis utilizadas. Seguidamente, serão expostos e analisados os resultados obtidos.

Por fim, procede-se à apresentação das conclusões, tendo em vista os objetivos previamente definidos.

Serão evidenciadas ainda quais as limitações/dificuldades sentidas durante a realização do estudo em questão, bem como serão propostos alguns temas para futuros trabalhos.

1 AUDITORIA INTERNA

Epistemologicamente a palavra Auditoria teve a sua origem no verbo latino *"audire"* que significa ouvir, o que levou a que se formasse a palavra auditor, que deriva igualmente do Latim *"Auditore"*, aquele que ouve, o responsável por ouvir, dado que inicialmente os então auditores baseavam as suas análises e posteriores conclusões apenas na matéria que ouviam, não havendo nenhum outro tipo de evidência a não ser aquela.

A crescente globalização de mercados, exige aos responsáveis das organizações uma maior eficácia na realização dos objetivos e eficiência na utilização dos recursos, constituindo, deste modo, a informação uma poderosa ferramenta para a tomada de decisão.

A auditoria interna permite aos decisores obter de forma sistemática informação sobre a atuação da organização, e conforme define (Marques:1997) o objetivo principal da auditoria tende a ser o de, progressivamente e através das suas análises, avaliações, sugestões e recomendações, auxiliar os membros da própria unidade económica ao bom desempenho das suas atribuições e responsabilidades.

A atividade da Auditoria Interna é desenvolvida ao longo de todo o ano. A sua principal responsabilidade é dotar a Direção de uma ferramenta de controlo, mediante a identificação dos pontos fracos da entidade, emitindo um relatório de diagnóstico. (Morais:2013)

À medida que o fator humano vai emergindo como fator determinante do sucesso das organizações, também a auditoria interna se vai assumindo como uma ferramenta e um contributo indispensável a esse sucesso, fomentando a qualidade e o rigor nas decisões tomadas e nos métodos adotados. (Morais:2013)

1.1 Evolução da Auditoria Interna – Mudança de Paradigma

Como consequência da Revolução Industrial, no princípio do séc. XIX, e consequente desenvolvimento das sociedades anónimas, surge a figura do Auditor, mais próxima da atual. A atividade da Auditoria limitava-se a um trabalho de mera vigilância ou de "polícia". O seu objetivo era detetar erros, irregularidades e fraudes, através de uma análise detalhada das transações. (Morais:2013)

Durante muitas décadas a auditoria interna foi entendida como uma atividade que visava essencialmente a avaliação da fiabilidade dos controlos internos, frequentemente, designada de "o controlo dos controlos", ou seja, tinha como principal função salvaguardar os ativos da empresa, verificar se os procedimentos instituídos na organização estavam a ser cumpridos e ainda verificar a veracidade da informação financeira.

Um dos principais objetivos desta função centrava-se na deteção de fraudes ocorridas dentro da empresa cometidas pelos próprios colaboradores. Dado o seu cariz de fiscalização – forma como era encarada por estes - tratava-se de uma função não muito apreciada pela generalidade dos colaboradores da organização, daí existir ainda hoje o estigma relativamente a Auditoria Interna.

Em Junho de 1999, a noção de Auditoria Interna foi redefinida pelo Institute of Internal Auditors (IIA), passando a incorporar as mudanças ocorridas na profissão e a orientar os auditores internos para uma atividade mais abrangente, em que se dá maior relevo à questão do valor acrescentado que é dado pela Auditoria Interna à organização. A Auditoria Interna passou a ser definida como "uma atividade independente de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste a organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controlo e governação".

Esta nova focalização da auditoria interna veio dar lugar ao que se designa, frequentemente, Auditoria Interna Baseada no Risco.

A diferença entre o velho e o novo paradigma da Auditoria Interna, reside essencialmente na transferência da focalização do controlo para os riscos. A auditoria, deixou de ser vista como uma mera função de controlo financeiro/contabilístico, passando a preocupar-se com a identificação dos riscos inerentes ao negócio, na identificação das atividades de controlo e 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. Deste modo, a Auditoria Interna tem como principal objetivo apoiar a gestão de topo a alcançar os objetivos definidos para a organização.

No seguimento do Enterprise Risk Managment (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, 2004).

De referir que a auditoria interna baseada no risco, permite ao auditor verificar não só se os controlos existentes são suficientes e eficazes na mitigação dos riscos, mas também verificar se existem controlos excessivos, podendo recomendar a existência de menos controlos caso se venha a confirmar que os mesmos são ineficazes ou que os custos são demasiado elevados face ao risco.

Neste sentido, espera-se que a Auditoria Interna seja, principalmente, uma ferramenta de apoio à gestão e que ajude a alcançar os seus objetivos.

1.2 Fases do trabalho de Auditoria Interna

Todo o trabalho de auditoria interna, deverá ter como ponto de partida um detalhado e exaustivo planeamento de todas as tarefas a efetuar, pois, é a partir daqui que se consegue delinear a estratégia a seguir para a consecução dos objetivos estabelecidos. Nesta fase deverá ser delineado um plano de ações de forma a cobrir com transversalidade todas as áreas da empresa onde exista risco associado, pois não fará sentido alocar recursos a um sector onde o risco seja materialmente irrelevante.

Para que sejam tomadas decisões que poderão fazer a diferença entre manter uma posição sólida no mercado ou mesmo perdê-la, o trabalho de auditoria deve ser tempestivamente reportado, permitindo que ocorram assim melhorias significativas no controlo interno e consequentemente nas várias áreas da empresa, incrementando valor na empresa

Num processo de auditoria interna, identifica-se três fases essenciais:

- Planeamento
- Execução do trabalho de campo

- Avaliação e elaboração do relatório (recomendações)

Planeamento

O planeamento reveste-se de uma importância capital, pois é por esta parte que começa a delinear-se todo o trabalho a realizar. É aqui que se verificam quais os principais fatores de risco associados à empresa e ao sector de atividade em que esta opera, permitindo assim adaptar melhor o trabalho a efetuar e testar as áreas mais susceptiveis, tendo sempre em conta os objetivos da atividade alvo do trabalho de auditoria.

Antes de se dar inicio a um trabalho de auditoria interna é necessário ter em conta vários fatores que poderão influenciar o resultado do mesmo, será neste caso fundamental adquirir um profundo conhecimento dos processos internos da empresa, da estrutura orgânica e funcional, assim como de todo o SCI.

Segundo Baptista da Costa (2010), "o auditor deve planear o trabalho de campo e estabelecer, a natureza, extensão, profundidade e oportunidade dos procedimentos a adotar, com vista a atingir um nível de segurança que deve proporcionar e tendo em conta a sua determinação do risco de auditoria e a sua definição dos limites de materialidade".

Execução do trabalho de campo

A execução do trabalho de campo constitui o *core* de Auditoria Interna dado que é nesta fase que, entre outras ações, se efetuam todos os tipos de teste aos procedimentos de controlo interno, para assim se poderem retirar informações suficientes que permitam retirar elações sobre o funcionamento global do SCI da entidade ou de uma determinada área específica. É também nesta parte que se detectam alguns tipos de risco, ao ser feita a análise dos controlos existentes e de quais as consequências da sua não aplicação ou das falhas do mesmo.

Avaliação e elaboração do relatório (recomendações)

Esta é a parte que precede a execução dos testes anteriormente descritos, pois serão aqui delineadas as possíveis alterações ou correções a efetuar, resultantes da deteção de situações passiveis de serem melhoradas. Nesta fase, o auditor deve apresentar explicações sobre todas as questões suscitadas pelo trabalho anterior e apreciar os seus eventuais efeitos sobre as conclusões gerais, com vista á determinação das matérias que serão objeto de relatório e que, como tal, determinarão, em parte, a respectiva estrutura.

Estas recomendações deverão ser veiculadas por intermédio de um relatório, constituindo este o produto final de todo o trabalho de auditoria interna. Trata-se de um documento formal onde o auditor interno relata o trabalho efetuado, qual a metodologia utilizada na realização dos testes, os métodos e procedimentos utilizados e ainda qual a apreciação do auditor relativamente ao SCI. Todas as recomendações contidas no referido relatório, deverão ser discutidas com os auditados antes da sua aplicação, para assim surgirem oportunidades de melhorar e envolver os mesmos na busca de soluções para a mitigação dos riscos incorridos, tendo sempre em consideração os objetivos estratégicos da entidade.

É também de primordial importância fazer uma análise da relação "custo-benefício" no âmbito da resolução do problema detectado.

Muito importante será também o tempo despendido na aplicação de uma recomendação, pois nos dias que correm, considera-se a tempestividade uma variável que poderá fazer a diferença.

O trabalho de auditoria é finalizado quando as recomendações ficam implementadas e após o acompanhamento se constata que estas estão a funcionar e a mostrar-se de facto uma mais-valia para a entidade.(Follow –Up)

Comprova-se assim a visão proactiva da auditoria interna, pois não se limita a avaliação, análise e diagnóstico, mas também à implementação de soluções e medidas corretivas certificando-se que a sua aplicação incrementará na entidade um ponto passível de ser considerado valor acrescentado. (Pinheiro, 2005)

1.3 Controlo Interno

Controlo é qualquer ação empreendida pela gestão, pelo conselho e outras entidades para aperfeiçoar a gestão do risco e melhorar a possibilidade do alcance dos objetivos e metas da entidade. A gestão planeia, organiza e dirige o desempenho de ações suficientes para assegurar com razoabilidade que os objetivos e metas serão alcançados.

É comum designar por sistema de controlo interno um conjunto de regras, politicas e procedimentos (mecanismos de controlo), envolvidos na gestão de risco empresarial.

Um mecanismo de controlo ajuda a atingir o objetivo de um processo sem ser necessariamente parte do processo. Estes mecanismos são recursos que têm por objetivo, quando utilizados pelos processos, eliminar ou minimizar os riscos.

Conforme evidencia Morais:2013, o primeiro organismo a definir controlo interno foi o AICPA em 1934 e usada pela SEC, SAS nº1 que definia: "*O controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas adoptadas num negócio a fim de garantir a salvaguarda de activos, verificar a adequação e confiabilidade dos dados contabilísticos, promover a eficiência operacional e encorajar a adesão às politicas estabelecidas pela gestão"*.

Foi publicado em 1987 o primeiro documento sobre esta temática, o denominado *Treadway Report,* identificando a necessidade da adoção de um referencial comum sobre este tema, apelando a que os responsáveis da gestão reportassem sobre a efetividade do funcionamento do sistema de controlo interno e enfatizando os elementos chave de um sistema de controlo interno, nomeadamente a existência de um código de conduta e de uma comissão de auditoria que integrasse profissionais competentes que possuíssem um adequado conhecimento da atividade desenvolvida e, uma gestão competente. (Gonçalves:2008)

Na sequência deste relatório, o COSO, em 1992 no seu relatório com o titulo "*Internal Control – Integrated Framework"*, define controlo interno, como um processo (um meio para atingir um fim) levado a cabo pelo Conselho de Administração, Direção e outros membros da entidade (pessoas, não é apenas um manual de politicas e documentos) com o objetivo de proporcionar um grau de confiança razoável (não consegue eliminar a totalidade dos riscos, apenas os minimiza) na concretização dos seguintes objetivos: eficácia e eficiência dos recursos, fiabilidade da informação e cumprimento das leis e normas estabelecidas.

O controlo interno está presente em qualquer entidade, mais definido numas e menos noutras, mas todas as entidades possuem mecanismos de controlos para a optimização da gestão das mesmas.

Embora com tendência a ser mais sofisticado nas entidades de maior dimensão, nenhuma entidade, por mais pequena que seja, pode exercer a sua atividade sem ter instituído um sistema de controlo interno, ainda que menos formal ou sistematizado. (Gomes:2014)

O controlo interno é uma preocupação constante em muitas autoridades e organismos reguladores, impulsionada sobretudo a partir de 2002 com o surgimento da Lei de *Sarbanes-Oxley Act* (conhecida como Lei SOX ou simplesmente SOX). (Morais:2013)

Fundada pelos senadores Paul Sarbanes (democrata de Maryland) e Michael Oxley (republicano de Ohio).

Os escândalos financeiros ocorridos em entidades globais, designadamente, a Enron, a WorldCom, a Parmalat e a Mitsubishi Motors contribuíram decisivamente para uma alteração do *status quo* da organização empresarial a nível internacional. (Gomes:2014)

A SOX foi a resposta do governo americano para reforçar a confiança dos investidores após a ocorrência de vários escândalos financeiros. É aplicável a todas as empresas com títulos cotados na bolsa de valores dos Estados Unidos da América (SEC), mesmo às estrangeiras (efeito extraterritorialidade). (Morais:2013).

O controlo interno surge como resposta às ameaças identificadas e preconiza a definição concreta de medidas para combater os riscos ou minimizá-los ao implementar politicas e processos transversais a toda a organização, que garantam o cumprimento das metas propostas. O COSO e a Lei Sarbanes-Oxley surgem nesta linha de atuação, como forma de combate à fraude e às ineficiências que abalam a confiança dos investidores nos mercados. (Oliveira:2011)

1.4 Controlo Interno e Auditoria Interna

O controlo tem uma perspetiva dinâmica na organização, valorizadora, permitindo-lhe manter o domínio enquanto que a Auditoria avalia esse grau de domínio atingido. (Morais:2013)

O auditor interno é aquele que no exercício da sua função incluiu a avaliação da adequação e eficácia do sistema de controlo interno. (Morais:2013)

O controlo interno é um conjunto de procedimentos implementados pela gestão com vista a reforçar a possibilidade de atingir os objetivos definidos, garantindo a eficiência e eficácia na utilização de recursos. Traduz-se na introdução de boas práticas de gestão e procedimentos de acompanhamento de ordem operacional.

A auditoria interna deve proceder ao exame e avaliação da adequação e eficácia do sistema de controlo interno e da qualidade do desempenho na realização do trabalho, fornecendo análises, avaliações, recomendações e comentários sobre as atividades auditadas assessorando a administração no desempenho eficiente das suas funções na procura de uma melhoria continua.

A finalidade da revisão da adequação do sistema de controlo interno é determinar se ele estabelece certeza razoável de que os objetivos da organização são cumpridos de maneira eficiente e económica. A finalidade da revisão para determinar a eficácia é assegurar que o sistema de controlo interno funciona como deve. A finalidade da revisão quanto á qualidade do desempenho é assegurar que os objetivos da organização foram atingidos.

A auditoria interna analisa o controlo interno na óptica do que ele representa para a organização, de forma a possibilitar o desenvolvimento harmonioso, seguro e adequado de todas as ações e permitir o reflexo aos setores e pessoal interessado nas informações.

A Auditoria é uma função de supervisão, isto é, um controlo *ex-post*, ao passo que o controlo interno tem carácter preventivo ou *ex-ante*. Assim, o controlo interno pertence ao primeiro nível de monitorização e a auditoria está num patamar superior. (Morais:2013).

O primeiro passo para a elaboração de um programa de auditoria, deve ser a avaliação do sistema de controlo interno existente, de modo a determinar o grau de confiança do mesmo, com o objetivo de determinar os procedimentos de atuação, o alcance e a profundidade dos testes a efetuar.

Verifica-se do exposto, que a auditoria interna sendo parte integrante da componente de monitorização do sistema de controlo interno, exerce um papel fundamental em termos do exame, fortalecimento e constante melhoria do controlo interno.

1.5 Auditoria Interna baseada no modelo COSO

O COSO ERM é uma estrutura que pretende ajudar as organizações a perceber o que é o risco, e de que modo é que ele está presente na empresa. Na perspetiva do COSO, o risco é observado sob o ponto de vista empresarial, tendo em conta as pessoas em todos os níveis da organização. (Pinheiro:2013)

O modelo ERM é um guia prático de fácil aplicação e é desenhado de modo a identificar determinados acontecimentos que podem vir a afetar a organização. Destina-se a identificar, avaliar e gerir o risco, de modo a fornecer uma segurança razoável quanto á realização dos objetivos da organização. (COSO:2004)

O papel da AI é o de assegurar a Governance, a gestão do risco e o controlo interno, e não as operações nem o desenho das mesmas. É necessária uma auditoria de alto nível, para assegurar a Governance, através do plano de negócio, da tomada de decisão, remuneração do executivo, das relações entre quadros e do papel da comissão de auditoria. (Pnheiro:2013)

A AI analisa o desenho do processo de gestão de riscos e os resultados dos testes executados, e determina se a gestão de riscos oferece uma garantia razoável referente aos objetivos definidos.

De acordo com o IIA (2004), no documento "The Role of Internal Auditing in Enterprise-wide Risk Management", onde são identificadas formas dos auditores internos manterem a objetividade e a independência de acordo com as normas do IIA, existem 3 áreas chave para a AI atuar: uma onde a AI tem um papel importante baseado no risco, no que diz respeito ao ERM (ao rever a gestão dos riscos chave, ao avaliar o reporte desses riscos, ao avaliar os seus processos), outra onde a AI tem um papel legitimo, embora com ressalvas (ao dar segurança de que os riscos foram corretamente avaliados e na gestão dos processos), e por último, onde a AI não deve ter qualquer papel, pois já são assuntos que competem apenas à gestão, que é a responsável pela gestão do risco (definição do apetite ao riscos, tomada de decisões).

A AI é de extrema importância no encorajamento do órgão de gestão na implementação de um processo de gestão de risco e sugerindo uma estrutura eficiente para esse processo, dado o seu conhecimento de toda a organização e da distribuição dos riscos existentes, ajudando assim a uma mais melhor implementação da metodologia da gestão de risco.

O conhecimento íntimo do risco existente na organização, a familiaridade com avaliações baseadas no risco, os laços estreitos com o órgão de gestão e a capacidade única de assimilar grandes quantidades de informação e produzir resultados claros e concisos, posicionam a AI como um instrumento valioso na implementação de um processo de ERM dentro da organização.

2 GESTÃO DE RISCO

Correr riscos é um facto inerente à própria existência de uma empresa, pressupondo, contudo, que esta tenha uma capacidade e vontade de inovar e gerar riqueza, aproveitando assim as oportunidades que lhe vão surgindo de todo o meio envolvente.

Segundo o COSO ERM, a gestão de risco empresarial, é "um processo, desenvolvido pelo Conselho de Administração, Órgãos de Gestão e outros elementos da organização, aplicado na definição de estratégia e que deve abranger toda a organização. Este processo tem como objetivo a identificação dos eventos que podem afetar a organização e a gestão dos riscos, alinhados como perfil de exposição definido, com vista a providenciar uma segurança aceitável com vista ao cumprimento dos objetivos definidos pela organização." (COSO:2004)

A gestão de risco é um meio para atingir um fim e, não um fim em si mesmo. É um processo educativo que nos consciencializa que de facto existem riscos, e que aos gestores cabe a responsabilidade de os gerir.

Nestes últimos anos, a gestão de riscos, de um modo geral, tem procurado aproveitar as oportunidades de ganho e minimizar os impactos negativos. A "nova" gestão de risco é parte integrante das boas práticas de gestão empresarial e é um elemento essencial de governação empresarial.

Na gestão de riscos devem ser utilizadas metodologias adequadas, senso comum, conhecimento da cultura organizacional e, ainda, sensibilidade pessoal.

"A principal diferença entre o processo de ERM e as outras formas tradicionais de gestão de risco é que o processo de ERM adota uma perspetiva que coordena a gestão de risco ao longo de toda a organização, em vez de cada área da organização gerir os seus próprios riscos" (Banham, 2004) citado por Castanheira e Rodrigues (2006)

Segundo a KPMG, o ERM "é uma proposta disciplinada e estruturada que alinha a estratégia, os processos, as pessoas, a tecnologia e o conhecimento com o objetivo de avaliar e gerir as incertezas que a empresa enfrente à medida que cria valor".

2.1 Definição

A noção de risco nem sempre é pacífica, no entanto, está sempre relacionada com os efeitos possíveis da ocorrência de um evento. Em regra, está associado ao efeito negativo dessa ocorrência.

Assim, o risco é a possibilidade de um evento ocorrer e afetar negativamente a concretização de um objetivo planeado, seja por uma pessoa ou por uma empresa.

O COSO define risco como sendo a possibilidade de um evento ocorrer e afetar negativamente a realização dos objetivos. Contudo, os eventos podem resultar de fontes internas ou externas à organização e podem causar impactos positivos e ou impactos negativos. Neste sentido, o COSO refere o seguinte:

"Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização de objetivos" (COSO:2004)

De acordo com Hussein (2008), o American Institute of Certified Public Accountants (AICPA), classificou os riscos em três grupos, a saber:

- Riscos relacionados com o ambiente empresarial – ameaças do ambiente empresarial em que a entidade opera, como riscos decorrentes da atuação da concorrência, políticos, legais ou decorrentes da ação de órgãos reguladores e fiscalizadores, financeiros e de procura;
- Riscos relacionados com o processo de negócio e dos seus ativos – ameaças ao negócio da organização pelos concorrentes e perdas de ativos, sejam físicos ou financeiros;
- Riscos relacionados com as informações – ocorrência de ameaças decorrentes de má qualidade das informações para o processo de tomada de decisão e, fornecimento de informações a terceiros.

2.2 A Gestão de Risco como criadora de valor

A gestão do risco tem vindo a assumir um papel cada vez mais importante na agenda estratégica das empresas, constituindo um elemento fundamental de suporte à gestão num contexto macroeconómico instável e complexo.

A gestão de risco é uma prática vocacionada para a criação e preservação de valor, bem como para o que pode pôr em causa esse valor. (KPMG:2013)

De forma a se fortalecerem as estruturas para minimizar ou tornar as empresas menos voláteis a estas situações, têm de ser identificados, bem como avaliada a sua probabilidade de ocorrência e o seu impacto, os grandes fatores adversos que podem pôr em causa o valor da empresa.

Para uma efetiva gestão de risco é crucial o alinhamento do apetite ao risco dentro da organização e da perceção dos riscos a que a empresa está exposta. Por esta razão, a definição do apetite ao risco da organização e a aprovação de uma politica de risco por parte da gestão de topo, constituem fatores críticos para a implementação bem sucedida do processo de gestão de risco. (KPMG:2013)

A gestão de risco deve ser assegurada a três níveis, constituindo as unidades de negócio/suporte a 1ª linha de defesa na gestão de risco. Estas áreas devem ser as primeiras responsáveis pela avaliação dos riscos e pela implementação de ações corretivas, com vista a colmatar eventuais deficiências nos processos e controlos. Por outro lado, a criação de áreas específicas de gestão do risco, tipicamente consideradas como 2ª linha de defesa, têm por missão facilitar o desenvolvimento do *framework* de gestão do risco e monitorizar se os processos estão a ser devidamente operacionalizados pela 1ª linha de defesa. (KPMG:2013)

A 3ª linha de defesa na gestão do risco é assegurada pela função de Auditoria Interna, tendo por objetivo avaliar a efetividade do modelo de governo, do *framework* de gestão do risco e dos controlos internos implementados, sendo independente da 1ª e 2ª linhas de defesa. (KPMG:2013)

No sentido de aumentar o seu desempenho, o valor e a reputação da própria marca, as empresas com a introdução de uma gestão do risco integrada, tornam-se mais proactivas na identificação e gestão dos seus riscos, aplicando a sua experiência e conhecimento no suporte às decisões estratégicas.

Cada vez mais as empresas preocupam-se com a criação de uma cultura corporativa vocacionada para a gestão do risco, transversal e em todos os níveis da organização.

A gestão de risco continuará certamente a ganhar confiança da gestão de topo e a ser considerada uma prioridade para os diferentes níveis dentro da organização. Neste contexto, o risco deixará também de ser visto como reativo e defensivo (preservação de valor), tornando-se proactivo e criativo (criação de valor), contribuindo positivamente para a competitividade das empresas. (KPMG:2013)

A gestão de risco além de apoiar na implementação de procedimentos de compliance e auditoria, visa a antecipação de eventos com uma orientação pró-ativa, considerando e estratégia e planeamento adotados. (Oliveira:2011)

Em suma, desenvolver um processo formal de gestão de risco reduz o tempo de reação das empresas, cria uma cultura de risco positiva e melhora continuamente o processo de mitigação de risco. (Castanheira:2006)

A gestão de risco empresarial, qualquer que seja o modelo que se aplique, não garante que os objetivos de uma organização sejam todos atingidos, apenas dá uma segurança razoável de que tais objetivos possam ser alcançados.

Não nos podemos esquecer que o risco pertence ao futuro, logo é um acontecimento que não é possível prever com segurança e muitos deles não dependem da própria organização, são externos à organização, o que os torna ainda mais difíceis de prever.

A gestão de riscos é feita por pessoas, logo existe a possibilidade de ocorrer um erro humano, como por exemplo uma informação mal entendida pode dar origem a uma decisão ou um juízo de valor menos correta, podendo afetar a concretização de determinado objetivo.

Por outro lado, e tendo em consideração os dias de hoje, em que os recursos são escassos, as organizações devem ter em consideração os custos/benefícios da implementação de controlos para a mitigação de riscos, ou até mesmo ponderar se é vantajoso para determinada organização implementar um modelo de gestão de risco.

De acordo com o COSO ERM, o conceito de segurança razoável, não quer dizer que a gestão de risco empresarial vá fracassar frequentemente. Contudo, pode ocorrer um erro, um evento incontrolável ou uma informação falsa. Uma segurança razoável não constitui uma segurança absoluta.

2.3 O processo da Gestão de Risco: identificar, avaliar, mitigar e monitorizar/reportar

No que respeita ao mapeamento de riscos, as empresas devem identificar riscos emergentes de forma contínua, criando processos específicos para facilitar a sua identificação e análise. A análise de riscos inclui a caracterização de causas, efeitos, ações de mitigação e correlação entre riscos, e pode ser desenvolvida através da utilização de diferentes técnicas, de acordo com as especificidades e a maturidade de cada empresa. (KPMG:2013)

O processo de gestão do risco engloba igualmente a monitorização da exposição ao risco que a empresa incorre, a identificação de eventos de risco e a emissão de alertas de potenciais riscos que possam vir a ocorrer. (KPMG:2013)

Não existe um modelo de avaliação do risco que seja standard e como tal aplicado a todas as empresas, pois cada uma tem as suas próprias especificidades, pelo que o auditor interno deve ter em consideração as características mais representativas do risco.

No entanto, o modelo do COSO ERM efetua a medição do risco através do mapeamento do risco, utilizando para o efeito a matriz de risco, conforme exemplo a seguir:

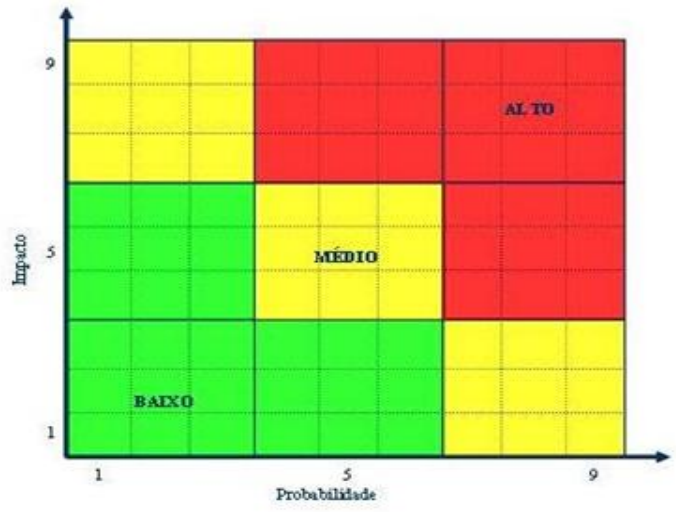


Figura 1 – Matriz de risco

Após a identificação, classificação e análise dos riscos, será necessário avaliar cada um em termos da sua ocorrência potencial, e quais os seus impactos tanto estratégicos e operacionais como financeiros.

Trata-se de uma matriz de dupla entrada, em que no eixo das abcissas se mede a probabilidade de um determinado risco vir a ocorrer, e no eixo das ordenadas avalia-se o impacto que o risco pode causar, caso se venha a verificar.

Digamos que se trata de uma avaliação em 3 dimensões, horizonte temporal, impacto e a probabilidade de um determinado risco acontecer. A avaliação do impacto e da probabilidade de ocorrência dos riscos de cada processo permite identificar os riscos que apresentam maior criticidade e que exigem uma atenção especial da gestão.

Fazendo uma análise critica a esta matriz facilmente se deduz que para qualquer entidade os riscos a serem prioritariamente tratados serão os de impacto alto e probabilidade também alta. Isto porque o impacto terá grandes consequências para a empresa, podendo mesmo pôr em causa a sua continuidade, o que acrescido ao facto de ter também uma probabilidade de ocorrência alta o torna num dos riscos mais sensíveis para uma entidade, como tal deverá ser tratado delicada e eficazmente.

O COSO ERM (2004), considera que a avaliação da probabilidade e do impacto do risco pode ser efetuada através de métodos qualitativos e quantitativos e podem ser avaliados individualmente ou por categorias, tendo por base um período temporal. Por regra são utilizados métodos qualitativos, quando os riscos são difíceis de quantificar ou não existe informação suficiente. Os métodos quantitativos são mais precisos e são normalmente utilizados em atividades mais complexas e como complemento às técnicas qualitativas. A probabilidade e o impacto de um ou mais riscos podem ser representadas graficamente através da utilização de uma matriz de riscos, conforme figura acima.

A gestão de riscos fecha o ciclo tomando as decisões de gestão que mais se adequam ao risco identificado. Existem várias estratégias que podem ser seguidas na gestão de risco das quais se destacam:

Mitigação de riscos – É a reação ao risco normalmente evocada em primeiro lugar. Esta contém todas as medidas tomadas pelas empresas contra as ameaças que determinados riscos podem representar para elas.

Aceitação de riscos – Este caso põe-se desde que o custo da eliminação de um determinado risco for substancialmente superior ao custo para a empresa associado à consequência que este produzirá na mesma. Ou desde que a sua eliminação desvie recursos da eliminação de um outro risco muito mais grave.

Transferência de riscos – Esta é também uma prática comum no que á gestão de risco diz respeito, pois em alguns casos é mais prudente transferir o risco para terceiros – seguradora – do que alocar recursos limitados a iniciativas de mitigação que provavelmente farão pouca ou nenhuma diferença.

Contenção de riscos – Haverá casos em que o custo associado à eliminação de um determinado nível de risco simplesmente não pode ser comportada pela empresa. Nesses casos é melhor evitar totalmente o risco, ou seja retirando o processo em questão, ou antes disso deixando mesmo de o instalar.

2.4 COSO ERM

Mais do que se concentrar em riscos ao acaso, a abordagem integrada procura implementar processos consistentes que considerem todos os eventos que podem afetar adversamente as empresas. É neste contexto que surgiu a Gestão de Risco Empresarial (ERM – *Enterprise Risk Management*) como um novo paradigma na gestão do risco do negócio. (Castanheira:2006)

A principal diferença entre o processo de ERM e as outras formas tradicionais de gestão de risco é que o processo de ERM adota uma perspetiva que coordena a gestão de risco ao longo de toda a organização, em vez de cada área da organização gerir os seus próprios riscos. (Banham.2004 referido por Castanheira:2006)

O Framework COSO ERM fornece as linhas de orientação para a implementação e desenho do processo de ERM em qualquer organização. (Castanheira:2006)

Em 2001, o COSO iniciou um projeto, em parceria com a PricewaterhouseCoopers com vista ao desenvolvimento de um modelo que permitisse ajudar os gestores na avaliação e melhoria da gestão de risco das suas organizações.

Nos últimos anos, os escândalos financeiros das empresas que manipularam as informações financeiras como a Enron, Tyco, Worldcom e outras, afetaram de forma significativa a confiança dos investidores, funcionários e outros stakeholders, vindo reforçar a necessidade de maior transparência e fiabilidade na realização e divulgação de informação contabilística e financeira e introdução de medidas de melhoria e reforço de competências ao nível da governação corporativa e da gestão de risco, através de novas leis e regulamentações.

O modelo de gestão de risco (publicado em Setembro de 2004), designado Gestão de Riscos Corporativos – Estrutura Integrada, emitido pelo Comitee of Sponsoring Organizations of the Tradeway Commission (COSO) com a colaboração da PricewaterhouseCoopers expande-se para além do sistema de controlo interno, promovendo uma focalização mais forte e abrangente na gestão de risco empresarial.

Não substitui o modelo de controlo interno desenvolvido pelo COSO em 1992, mas incorpora-o, permitindo que as organizações adotem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno, progredindo para um processo de gestão de risco.

O COSO ERM, além de preservar a estrutura do anterior modelo, explora o controlo interno mais extensivamente no que se refere à gestão de risco de uma organização. A premissa subjacente à gestão de risco empresarial é definida como um processo efetuado e aplicado na empresa, disposto a projetar e identificar os eventos potenciais que pudessem afetar a entidade, reduzindo o risco de forma a fornecer uma garantia razoável a respeito da realização dos objetivos da entidade.

O COSO – Gestão de Riscos Corporativos – Gestão Integrada, inclui também outra categoria de objetivos, denominados objetivos estratégicos, que operam a um nível superior dos outros objetivos que resultam da missão ou visão da entidade, com as quais deveriam estar alinhados os objetivos operacionais, de informação e de cumprimento, bem como, inclui o conceito de apetite ao risco e tolerância ao risco.

A gestão de riscos corporativos permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos cujo impacto seja maior – quer seja positivo quer seja negativo, com o objetivo de criar valor para os acionistas.

O modelo de gestão de risco proposto pelo COSO ERM está assente em 8 componentes que são afetados de acordo com os objetivos da organização. Estes objetivos podem ser classificados em : estratégicos, táticos, comunicação, regulação e conformidade legal.

Existe uma relação direta entre objetivos e componentes, uma vez que os objetivos são metas que a entidade pretende alcançar e os componentes são os meios necessários para atingir esses objetivos.

Figura 2 – Cubo do COSO ERM (Fonte: COSO:2004)

O modelo deverá ser avaliado e implementado de uma forma abrangente a toda a organização, partindo de um nível mais elevado (Entidade) até chegar ao nível mais básico (Atividades).

De acordo com este modelo, os componentes da gestão do risco estão identificados como sendo os seguintes:

Ambiente Interno, ou seja, contexto ou ambiente onde as organizações funcionam com objetivos a atingir e meios a serem utilizados para esse fim. Abrange a cultura da organização, a base como o risco é visto e dirigido por uma entidade, incluindo a gestão do risco, a consciência interna sobre o risco, a integridade, os valores éticos e o ambiente em que a empresa opera.

Definição de objetivos, é uma pré-condição para a identificação dos riscos, para a sua avaliação e formulação das respostas possíveis de serem implementadas.

Identificação de eventos/acontecimentos, trata-se de identificar os fatores internos e externos, com capacidade de influenciar a estratégia e os seus objetivos.

Avaliação dos riscos, a gestão avalia a situação potencial subdividindo o conceito de risco em risco inerente (aquele em que a organização incorre na ausência de medidas preventivas ou de correção) e risco residual (risco que permanece mesmo depois de tomadas as ações preventivas e/ou corretivas de comportamentos). Os riscos são valorizados mediante a probabilidade de ocorrência do acontecimento e das suas consequências ou impactos.

Na análise dos riscos, pode-se recorrer a análises qualitativas ou quantitativas dos mesmos. A análise qualitativa faz a priorização dos riscos através da avaliação e combinação da probabilidade de ocorrência e impacto. Já a análise quantitativa faz a análise numérica do efeito dos riscos identificados nos objetivos gerais.

Resposta aos riscos, isto é, depois de identificados e avaliados os riscos, a gestão deve preparar respostas que obedecem inevitavelmente às seguintes possibilidades: evitar o risco, reduzir o risco, partilhar o risco ou aceitar o risco.

A resposta ao risco é o processo de desenvolver e determinar ações para mitigar os riscos, reduzindo as ameaças dos objetivos da organização. A administração avalia a probabilidade e o impacto da ocorrência do risco, os custos e benefícios, a prioridade das ações a implementar e seleciona a resposta que melhor se adequar dentro dos limites de tolerância do risco aceite.

Controlo das atividades, este controlo deve ser efetuado através do vector risco. Como tal deve ser enquadrado/identificado com as politicas (o que deve ser feito) e os procedimentos (a forma como se deve fazer) que garantem a resposta aos riscos.

Informação e comunicação, torna-se particularmente importante, com vista a facilitar a criação de valor acrescentado, formalizar na organização um sistema de informação estratégico.

Monitorização, pode revestir-se de duas formas. A primeira, prende-se com o conhecimento (em tempo real) do desenvolvimento das atividades, sendo a monitorização, neste caso, parte integrante das atividades operacionais definidas numa organização. A segunda consiste em atividades de avaliação, que o departamento de auditoria interna e outras entidades desenvolvem, em função do perfil e frequência dos riscos, da dificuldade ou importância das respostas aos riscos e dos seus controlos de gestão.

Muito recentemente, mais propriamente em Setembro de 2017, o COSO publicou a atualização da sua estrutura de gestão de riscos num novo *framework*, que ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance.

Esta atualização do *Framework*, tem como base os seguintes pontos:

- Elucida o valor da gestão de riscos ao estabelecer e executar uma estratégia;
- Intensifica o alinhamento entre performance e gestão de riscos, com o objetivo de aperfeiçoar a definição de metas de performance e o entendimento do impacto do risco sobre a performance;
- Comtempla as expectativas relativas a governança e supervisão;
- Reconhece a globalização dos mercados e das operações e a necessidade de aplicar uma abordagem comum, embora adaptada, a todas as regiões geográficas;
- Apresenta novas formas de interpretar riscos ao definir e atingir objetivos no contexto de maior complexidade dos negócios;
- Amplia os aspetos de divulgação dos riscos para atender às expectativas dos *stakeholders* em relação a maior transparência;
- Comtempla tecnologias evolutivas e a proliferação de dados e análises de dados que suportam no apoio à tomada de decisões;
- Estabelece definições básicas, componentes e princípios para todos os níveis da organização envolvidos no desenho, na implementação e na execução das práticas de gestão de riscos.

Como a própria organização COSO reconhece, a gestão de riscos tem-se aperfeiçoado nos últimos anos, entretanto o aumento da volatilidade e complexidade das operações globalizadas ou não, tem desafiado as empresas a contar com uma estrutura flexível e muito mais adaptável as mudanças de forma a dar sustentabilidade e perenidade, mitigando os riscos de reputação, confiança e relevância operacional. (Pardini:2017)

A compreensão da natureza do risco, a arte e a ciência da escolha, está no cerne da economia moderna. Cada escolha que fazemos quando buscamos atingir um objetivo tem seus riscos. Das decisões operacionais do dia a dia aos *trade-offs* fundamentais na reunião do conselho, lidar com o risco dessas escolhas faz parte do processo decisório. (COSO:2017)

Cada vez mais, os *stakeholders*, avaliam as empresas pela capacidade de liderança de identificar e concretizar oportunidades, exigindo assim uma maior transparência e responsabilidade na gestão do impacto do risco na empresa.

A gestão de risco, ajuda as organizações a identificar fatores que representam não apenas risco, mas também mudanças, e como essas mudanças podem afetar a performance e obrigar a revisão da estratégia. Deste modo, a organização aumenta a capacidade de se antecipar e responder a mudanças, aumentando assim a sua resiliência.

A gestão de riscos quando integrada em toda a organização, podem ser obtidos muitos benefícios, como o aumento do leque de oportunidades, identificação e gestão do risco na entidade como um todo (o mesmo risco pode afetar diversas partes da organização), aumento dos resultados positivos e da vantagem com a diminuição das surpresas negativas, diminuição da oscilação da performance, melhor distribuição de recursos e aumento da resiliência da empresa.

A aplicação da gestão de riscos à estratégia, faz todo o sentido, uma vez que essa é a melhor abordagem para fazer escolhas fundamentadas.

O risco deve ser levado em conta em diversos processos de definição estratégica, definindo objetivos estratégicos alinhados com a missão, visão e valores da empresa, no entanto ele costuma ser relacionado com uma estratégia já existente.

Este é um aspeto que pode ter influência no valor da empresa, mas outros aspetos podem ter também influência como a possibilidade da estratégia não estar alinhada com a missão e visão da organização, outro ponto, é avaliar se a estratégia escolhida está alinhada com o apetite ao risco, com os recursos requeridos e com o retorno desejado.

A falta deste alinhamento potencializa o risco da empresa de não criar valor às partes relacionadas, além do que, pode comprometer a sua operacionalidade e desgastar o valor existente. (Brasiliano:n.d.)

Seguidamente, apresenta-se o novo *Framework* (*Enterprise Risk Management – Integrating with Strategy and Performance)*, ressaltando a importância da utilização da gestão de riscos na definição da estratégia alinhada à missão, valores e visão, e determina que o sucesso para um desempenho operacional gerador de riqueza acontece através da integração e equilíbrio de todos os departamentos e funções com foco em riscos. Passa a ser condição “sine que non” a interação entre o planeamento estratégico e a área de riscos corporativos. (Brasiliano:n.d.)

Este Framework, está organizado em cinco componentes, que por sua vez integram vinte princípios que descrevem práticas para serem aplicadas de maneiras distintas para diferentes organizações, independentemente do seu tamanho, tipo ou setor. A adoção

destes princípios pode evidenciar uma razoável certeza de que a organização entendeu e se esforça para gerir os riscos associados à sua estratégia e objetivos de negócios.

O COSO ERM, *Enterprise Risk Management – Integrating with Strategy and Performance, 2017 – Executive Summary*, define os cinco componentes como:

Figura 3 – Componentes COSO ERM 2017 (Fonte: IIA:2017)

Governance and Culture (Governança e cultura): a governança dá o tom da organização, reforçando a importância e instituindo responsabilidades de supervisão sobre a gestão de riscos. A cultura diz respeito a valores éticos, a comportamentos esperados e ao entendimento do risco em toda a entidade.

Strategy and Objective-Setting (Estratégia e definição de objetivos): gestão de riscos, estratégia e definição de objetivos atuam juntos no processo de planeamento estratégico. O apetite ao risco é estabelecido e alinhado com a estratégia; os objetivos de negócio colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder aos riscos.

Performance: os riscos que podem impactar a realização da estratégia e dos objetivos de negócios precisam ser identificados e avaliados. Os riscos são priorizados com base no grau de severidade, no contexto do apetite ao risco. A organização determina as respostas aos riscos e, por fim, alcança uma visão consolidada do portfólio e do montante total dos riscos assumidos. Os resultados desse processo são comunicados aos principais stakeholders envolvidos com a supervisão dos riscos.

Review and Revision (Análise e revisão): ao analisar sua performance, a organização tem a oportunidade de refletir sobre até que ponto os componentes da gestão de riscos estão a funcionar bem ao longo do tempo e no contexto de mudanças relevantes, e quais correções são necessárias.

Information, Communication and Reporting (Informação, comunicação e divulgação): a gestão de riscos demanda um processo continuo de obtenção e compartilhamento de informações precisas, provenientes de fontes internas e externas, originadas das mais diversas camadas e processos de negócios da organização.

E define os vinte princípios, como:

Figura 4 – Princípios COSO ERM 2017 (Fonte: IIA:2017)

1.Exerce supervisão do risco por intermédio do conselho – O conselho de administração supervisiona a estratégia e cumpre responsabilidades de governança para ajudar a administração a atingir a estratégia e os objetivos de negócios.

2.Estabelece estruturas operacionais – A organização estabelece estruturas operacionais para atingir a estratégia e os objetivos de negócios.

3.Define a cultura desejada – A organização define os comportamentos esperados que caracterizam a cultura desejada pela entidade.

4.Demonstra compromisso com os valores fundamentais – A organização demonstra compromisso com os valores fundamentais da entidade.

5.Atrai, desenvolve e retém pessoas capazes – A organização tem o compromisso de formar capital humano de acordo com a estratégia e os objetivos de negócios.

6.Analisa o contexto de negócios – A organização leva em conta os possíveis efeitos do contexto de negócios sobre o perfil de riscos.

7.Define o apetite a risco – A organização define o apetite a risco no contexto da criação, da preservação e da realização de valor.

8.Avalia estratégias alternativas – A organização avalia estratégias alternativas e seu possível impacto no perfil de riscos.

9.Formula objetivos de negócios – A organização considera o risco enquanto estabelece os objetivos de negócios nos diversos níveis, que se alinham e suportam a estratégia.

10.Identifica o risco – A organização identifica os riscos que impactam a execução da estratégia e os objetivos de negócios.

11.Avalia a severidade do risco – A organização avalia a severidade do risco.

12.Prioriza os riscos – A organização prioriza os riscos como base para a seleção das respostas a eles.

13.Implementa respostas aos riscos – A organização identifica e seleciona respostas aos riscos.

14.Adota uma visão de portfólio – A organização adota e avalia uma visão consolidada do portfólio de riscos.

15.Avalia mudanças importantes – A organização identifica e avalia mudanças capazes de afetar de forma relevante a estratégia e os objetivos de negócios.

16.Analisa riscos e performance – A organização analisa a performance da entidade e considera o risco como parte desse processo.

17.Busca o aprimoramento na gestão de riscos – A organização busca o aprimoramento contínuo da gestão de riscos.

18.Alavanca sistemas de informação – A organização maximiza a utilização dos sistemas de informação e tecnologias existentes na entidade para impulsionar a gestão de riscos.

19.Comunica informações sobre riscos – A organização utiliza canais de comunicação para suportar a gestão de riscos.

20.Divulga informações de riscos, cultura e performance – A organização elabora e divulga informações sobre riscos, cultura e performance abrangendo todos os níveis e a entidade como um todo.

3 AUDITORIA INTERNA FOCALIZADA NA GESTÃO DE RISCO

A auditoria interna baseada no risco não se foca exclusivamente nos riscos da área financeira, não se preocupa só com factos passados e em emitir uma opinião sobre a razoabilidade das demonstrações financeiras e o adequado cumprimento das normas, regulamentos e procedimentos de controlo interno da organização. Passou a ter outra preocupação que se trata de analisar, avaliar e controlar os riscos de negócio. Passou a ter uma atitude mais próxima, mais comprometida com a gestão, no cumprimento dos objetivos.

3.1 Processo de Auditoria Interna baseado nos riscos

A auditoria interna é uma atividade independente, de avaliação e de consultoria. O seu papel fundamental em relação à gestão de risco empresarial é fornecer avaliação objetiva a administração quanto à eficácia da gestão de riscos. De facto, pesquisas têm mostrado que o conselho de diretores e auditores internos concordam que as duas formas mais importantes da auditoria interna prover valor à organização são fornecer a avaliação de que a estrutura de gestão de riscos e controlo interno está a ser eficaz.

A AIBR tem como principais objetivos fornecer uma segurança razoável no que diz respeito a se:

- Os processos de gestão de risco que a gestão implementou na organização estão a funcionar corretamente, conforme foram definidos e se são adequados;
- As respostas aos riscos são eficazes e adequadas na gestão do risco inerente, reduzindo esses riscos para níveis aceitáveis pela organização;
- Estão definidos e corretamente implementados controlos que mitiguem eficazmente os riscos de modo a não colocar em causa a concretização dos objetivos definidos pela gestão;
- Os processos de gestão de risco são acompanhados pela gestão de modo a garantir que os riscos, respostas e ações desenvolvidas são eficazes e estão em linha com os objetivos da organização.

A AIBR tem como principal objetivo determinar quais os objetivos primários do negócio da organização, os riscos associados, o apetite ao risco e níveis de tolerância, de modo a avaliar o grau de eficácia das atividades de gestão de risco empresarial desenvolvidas de forma a garantir a prossecução dos objetivos da organização, nomeadamente no que diz respeito às medidas de controlos implementadas e a eficácia das mesmas na redução dos riscos para níveis aceitáveis, de modo a garantir a concretização dos seus objetivos.

Existem várias razões que levam à implementação da gestão de risco numa organização, das quais destacamos o alinhamento e a integração de diferentes visões da gestão de risco, a construção de uma base de confiança em relação aos diferentes parceiros de negócio, o fortalecimento do governo das sociedades, resposta eficaz a eventuais mudanças que possam ocorrer no negócio e o alinhamento da estratégia com a cultura da organização.

A organização ao avaliar os riscos percebe até que ponto os eventos previstos e não previstos podem ter influência no cumprimento dos seus objetivos, bem como avalia qual a probabilidade de tais eventos acontecerem ou não e que impactos podem ter na organização.

A finalidade da análise e gestão do risco de negócio é essencialmente para aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e impactos dos eventos negativos.

Uma característica importante da AIBR é que a priorização é sempre feita tendo em consideração a criticidade dos riscos e a avaliação dos controlos na mitigação desses mesmos riscos.

3.2 O papel do Auditor Interno na Gestão de Risco

No que respeita a auditoria interna, o auditor deverá ter uma independência que lhe permita efetuar uma análise critica e isenta dos procedimentos e processos, para assim poder emitir informação útil que permita à empresa uma adequada tomada de decisões, no sentido de alcançar os objetivos que estão para si estabelecidos.

A auditoria interna tem um papel importante na avaliação da eficácia da gestão de risco na organização. Deve avaliar com regularidade a eficácia dos controlos internos

relativos à quantificação, informação e limitação dos riscos. A avaliação dos diferentes riscos ajudam a auditoria interna a definir o seu plano de trabalho, uma vez que lhe permite determinar quais são as áreas de maior risco, isto é, as áreas prioritárias e sobre as quais devem recair todas as atenções, portanto, as que devem ser analisadas primeiro.

As empresas devem compreender de uma forma integral que a administração é a responsável pela gestão de risco. Os auditores internos devem providenciar conselho e apoiar ou contestar as decisões tomadas pela gestão sobre risco em vez de tomar decisões sobre gestão de riscos.

Deste modo, de acordo com o IIA, a auditoria interna no âmbito do ERM deve (IIA:2004):

- Certificar os processos de gestão de risco
- Certificar que os riscos estão corretamente identificados e avaliados
- Avaliar os processos de gestão de risco
- Avaliar o reporte dos principais riscos
- Rever a gestão dos principais riscos

O IIA (2004), estabelece ainda quais as atividades que a auditoria não deve realizar, por deverem ser da responsabilidade da gestão e quando tomadas pela auditoria interna vão diminuir a independência desta nas competências que o IIA lhe atribui. Assim, algumas das atividades que não devem ser realizadas pelo auditor interno, são as seguintes:

- Estabelecer o apetite ao risco
- Estabelecer processos de gestão de risco
- Tomar decisões quanto às respostas a dar aos riscos identificados
- Implementar medidas que mitiguem os riscos
- Ser responsável pela gestão de riscos

Conforme, Sousa (2007) a auditoria interna deverá deixar de estar virada essencialmente para garantir a correta escrituração do passado, sendo muitas vezes vista como um mal necessário, passando a preocupar-se com a consecução dos objetivos e metas da empresa, através da deteção, análise e gestão dos principais riscos. Deste modo,

acrescenta valor, na medida em que contribui para assegurar que os resultados esperados são alcançados.

Desta forma o risco passa a assumir uma importância fundamental no processo de auditoria interna, devendo ser o centro de toda a atividade, desde o planeamento até à emissão do relatório, passando pela execução e documentação suporte do trabalho realizado (Almeida:2009).

Em organizações com maturidade de riscos menor, a auditoria interna pode optar por alocar tempo para promover a introdução e a melhoria dos processos de gestão de riscos. O objetivo dessa atividade de consultoria é melhorar a maturidade de riscos da organização. A auditoria interna deve ter uma abordagem de trabalho de tal forma que a direção mantenha um senso de posse dos processos que estão sendo desenvolvidos. (Cicco:2007)

3.3 Atualizar o sistema de Gestão de Risco através da Auditoria Interna

A auditoria interna é uma atividade independente, de avaliação e de consultoria. As duas formas mais importantes da auditoria interna prover valor à organização são fornecer avaliação objetiva de que os maiores riscos do negócio são geridos adequadamente e fornecer a avaliação de que a estrutura de gestão de riscos e controlo interno está a operar eficazmente. (IIA:2009)

As organizações cada vez mais solicitam aos auditores internos uma visão global da organização, identificando as perdas e as suas causas, a falta de controlo da qualidade e seus efeitos, verificação das áreas que podem ser aperfeiçoadas, isto é, uma auditoria focalizada nos resultados do negócio.

Estas exigências obrigam o auditor interno a desempenhar a sua atividade com visão holística e proactiva, antecipando-se aos factos, de modo que a sua opinião seja de fundamental importância nas escolhas da organização.

Dada a conjuntura económica atual, o contributo da AI para a gestão, no alcance de metas e objetivos previamente estabelecidos pelos órgãos estratégicos de uma organização é cada vez mais relevante, assim como a importância da existência, nas

organizações de informações fidedignas e em tempo oportuno cruciais ao processo de tomada de decisões pelo órgão de gestão. (Pinheiro:2013)

É através da verificação e análise da eficiência e eficácia do sistema de controlo interno, que a AI auxilia o órgão de gestão a, caso seja necessário, efetuar as devidas correções junto dos departamentos em que os controlos internos não estão a ser devidamente cumpridos.

Pode-se assim concluir, que a auditoria interna desempenha um papel fundamental no apoio ao órgão de gestão, aquando da sua função de tomada de decisões, através das informações recolhidas, contribuindo positivamente para o alcance dos resultados estipulados pelas organizações, facilitando a redução dos riscos a que as empresas estão expostas.

4 APRESENTAÇÃO DO ESTUDO

4.1 Metodologia

A apresentação deste trabalho tem como principal objetivo demonstrar, qual o grau de maturidade da auditoria interna nas empresas do distrito de Leiria e de que modo a gestão de risco é uma das preocupações dos órgãos de gestão e qual a sua importância estratégica.

Neste sentido, para procedermos à recolha dos dados, para fazer a caracterização da amostra e por forma a formular hipóteses de correlação para efetuar a investigação proposta, optou-se pela elaboração de um questionário.

A opção pelo questionário prende-se com o facto de este permitir atingir um grande número de pessoas com baixo custo, permitindo o anonimato das respostas, e que as pessoas respondam no momento que lhes parasse mais apropriado não as expondo à influência do investigador.

O questionário elaborado é de questões fechadas, simples e múltiplas, são apresentadas questões de filtro e consistência relativamente à sua função. Está dividido em quatro partes, a primeira para caracterização da empresa (setor de atividade, volume de negócios, número de funcionários, percentagem de exportação, existência de departamento de AI), na segunda e na terceira parte questões sobre o processo de implementação do departamento de AI e da gestão de risco na empresa e por fim, na última parte, perceber qual a perspectiva das empresas, que ainda não tenham, implementarem um departamento de auditoria interna ou um processo de ERM.

Deste modo, para a realização deste trabalho de investigação, foram formuladas as seguintes hipóteses a ser testadas:

H_1 - O setor de atividade tem influência na existência de departamento de AI

H_2 - O volume de negócios é determinante para a existência de departamento de AI

H_3 - O número de funcionários tem influência na existência de departamento de AI

H_4 - A percentagem de exportação influencia a existência de departamento de AI

A população alvo da investigação efetuada tem por base o universo das 250 maiores empresas (em volume de negócios) do distrito de Leiria durante o ano de 2017.

4.2 Análise dos dados

Neste ponto são apresentados todos os dados recolhidos através dos questionários.

Como já referido anteriormente, apenas se obteve resposta por parte de 40 empresas, representando 16% da população. O número de resposta é inferior ao desejado, no entanto, julga-se que o número de respostas obtidas permitem efetuar o estudo em questão.

A informação obtida será apresentada através de quadros e gráficos, retirados dos softwares utilizados para o tratamento dos dados (Google Forms, MiniTab e SPSS), de modo a permitir uma melhor análise e interpretação da informação.

As questões do questionário serão analisadas individualmente através da **estatística descritiva**, que tem como objetivo a recolha, apresentação, análise e interpretação de dados numéricos, através da criação de instrumentos adequados: quadros, gráficos e indicadores numéricos, visando somente descreverem e analisar um certo grupo (amostra) sem daí retirar conclusões ou inferências sobre a população da qual foi retirada a amostra.

Deste modo:

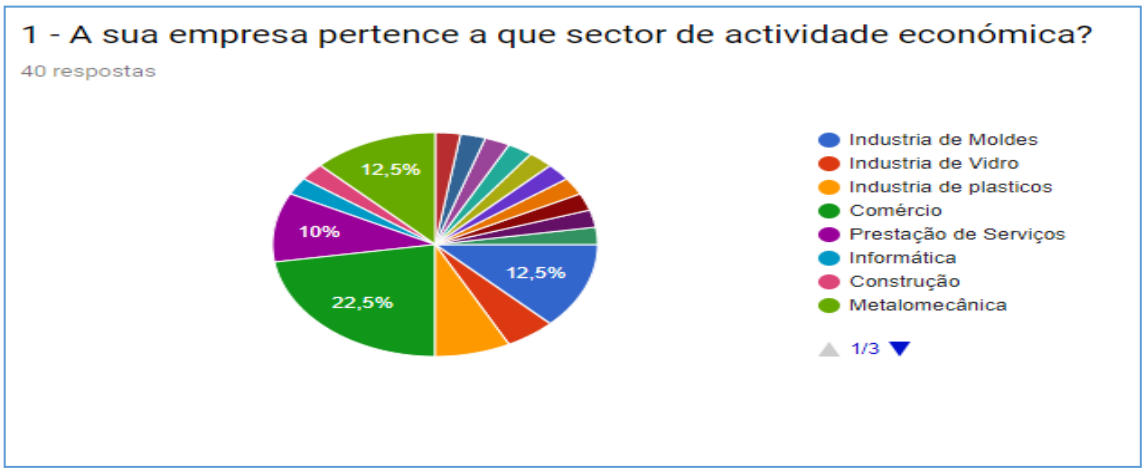


Gráfico 1 – Setor de atividade

Conforme se pode observar pelo gráfico acima, a maioria das empresas que constituem a amostra (n = 40), pertencem ao sector do Comércio, constituindo 22,5% da totalidade

da amostra, seguindo-se os sectores da Indústria de Moldes e Metalomecânica com 12,5% e o sector da Prestação de Serviços com 10%, sendo que os restantes sectores de atividade se distribuem de forma bastante uniforme.

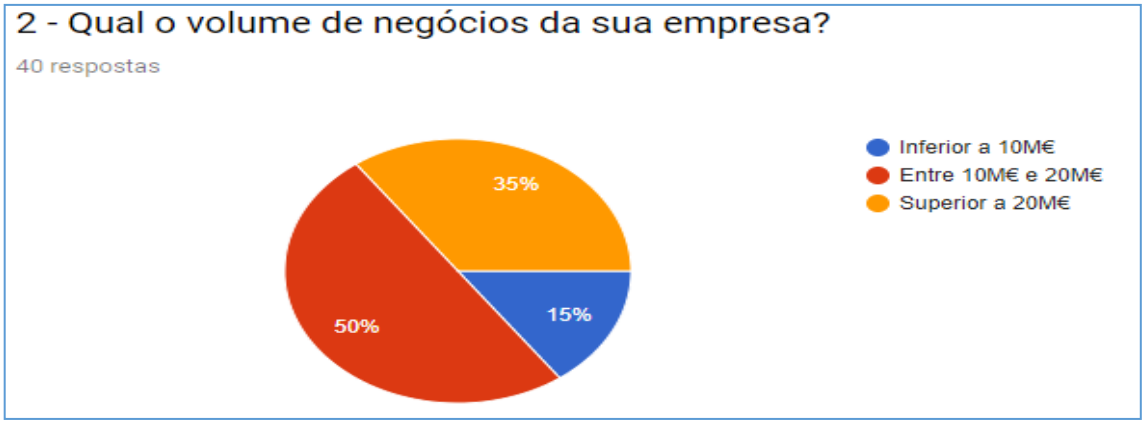


Gráfico 2 – Volume de negócios

De acordo com este gráfico, verifica-se que 50% da amostra (*n* = 40) é constituída por empresas com um volume de negócios compreendido entre 10M€ e 20M€, 35% com um volume de negócios superior a 20M€ e apenas 15% com volume de negócios inferior a 10M€.

Gráfico 3 – Número de funcionários

Relativamente a este gráfico, verifica-se que 77,5% da amostra (*n* = 40) tem mais de 50 funcionários, 17,5% tem entre 10 e 50 funcionários e apenas 5% da amostra tem menos de 10 funcionários.

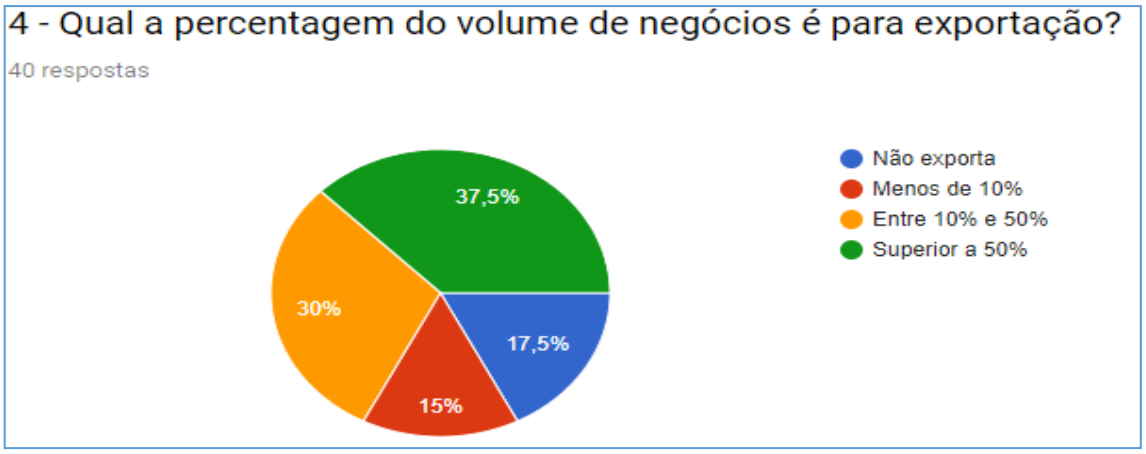


Gráfico 4 – Percentagem exportação

Segundo este gráfico, observa-se que 37,5% das empresas da amostra (*n* = 40) exporta mais de 50% do seu volume de negócios, 30% exporta entre 10% e 50% do seu volume negócios, 15% exporta menos de 10% e 17,5% não faz qualquer exportação.

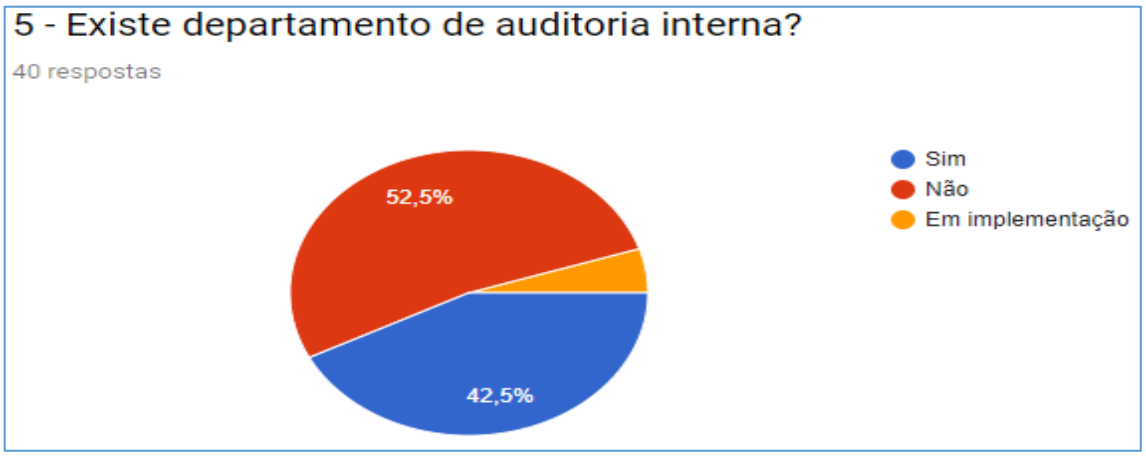


Gráfico 5 – Departamento AI

Quanto a existência de um departamento de auditoria, apenas 42,5% das empresas da amostra (*n* = 40) possuem um, sendo que as restantes empresas da amostra não possuem ou está em implementação.

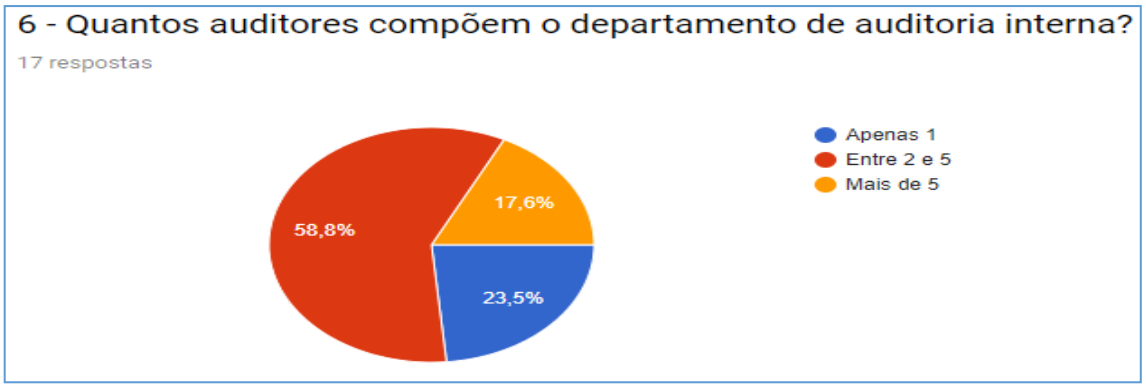


Gráfico 6 – Número de auditores

Das empresas que possuem departamento de auditoria interna (*n* = 17), verifica-se que 58,8% tem um departamento de auditoria interna constituído por 2 a 5 auditores, 17,6% constituído por mais de 5 auditores e 23,5% é constituído por apenas 1 auditor.

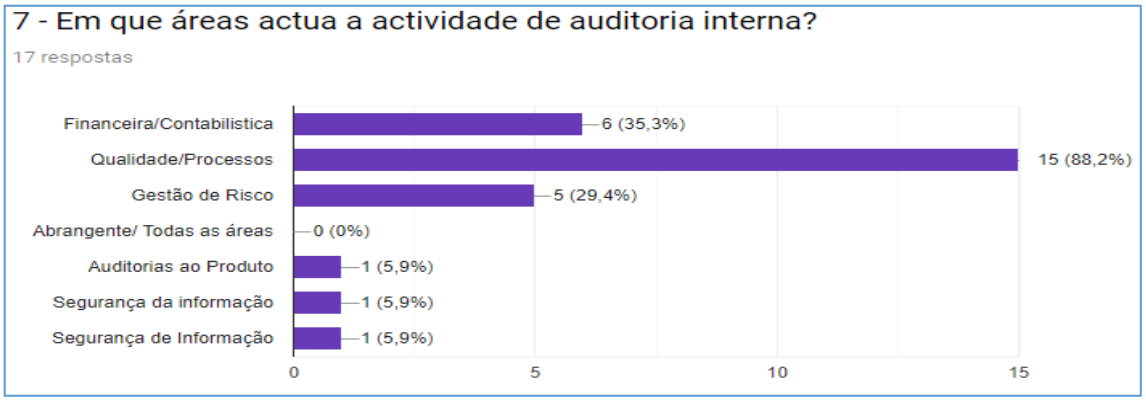


Gráfico 7 – Áreas da atuação da AI

Interpretando o gráfico, podemos concluir que de acordo com a nossa amostra a área de maior atuação da auditoria interna é a área da qualidade/processos (88,2%), seguindo-se a área financeira/contabilística (35,3%), gestão de risco (29,4%). Verifica-se ainda que em nenhuma das empresas da nossa amostra (*n* = 17) a atividade de auditoria interna atua de forma abrangente em todas as áreas.

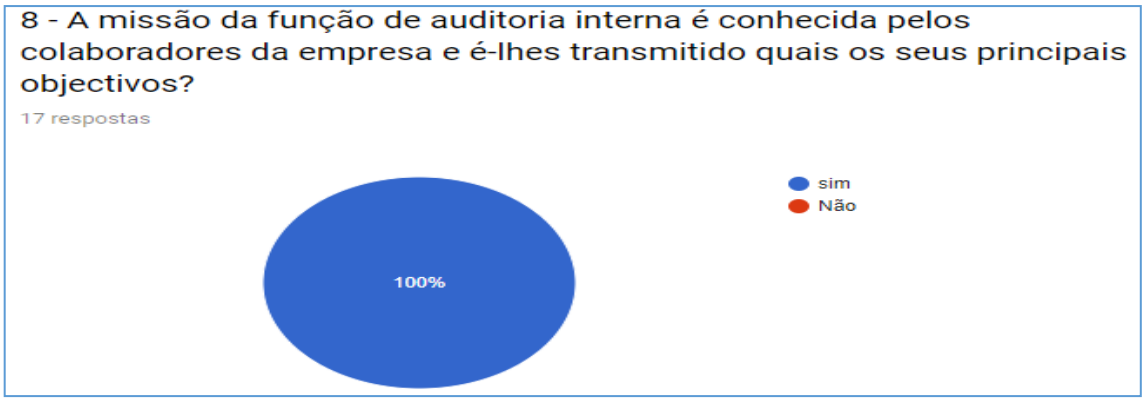


Gráfico 8 – Conhecimento da função de AI

Relativamente a este gráfico, verificou-se que a totalidade da amostra (*n* =17) transmite aos colaboradores da empresa qual é a missão da função de auditoria interna e quais os seus principais objetivos.

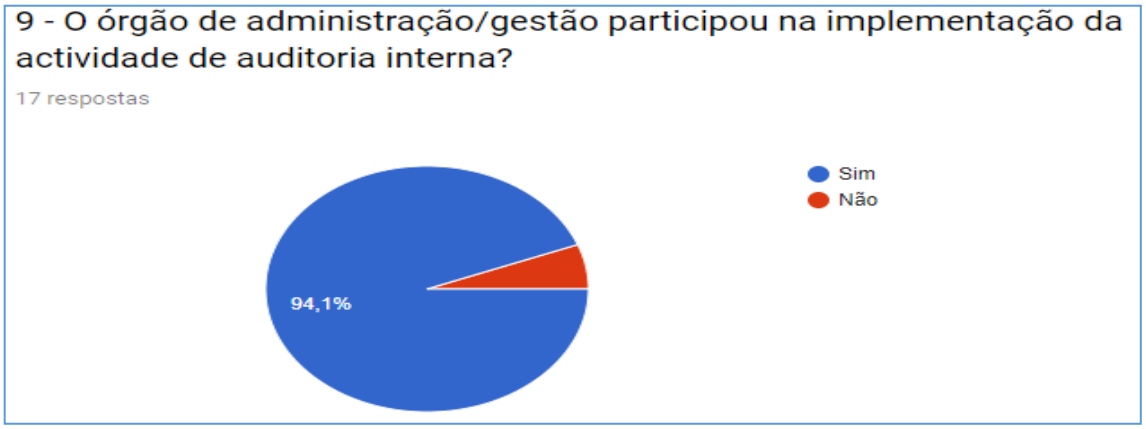


Gráfico 9 – Participação do órgão administração/gestão

Quanto a participação do órgão de administração/gestão na implementação da atividade de auditoria interna, verifica-se que em apenas 1 empresa da nossa amostra (*n* =17), não existiu participação.

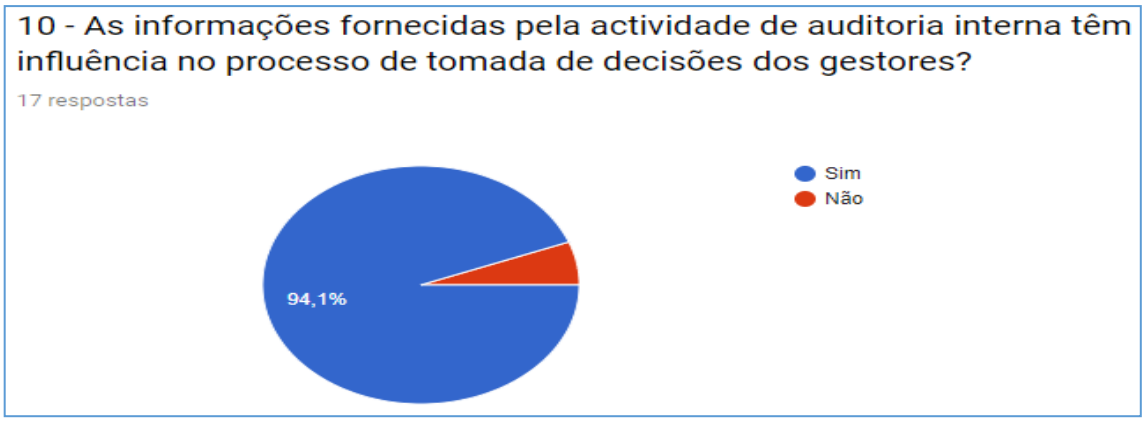


Gráfico 10 – Influência das informações da AI

No que concerne sobre a influência das informações fornecidas pela atividade de auditoria interna no processo de tomada de decisões dos gestores, apenas 1 empresa da nossa amostra (*n* =17), considera que não tem influência.

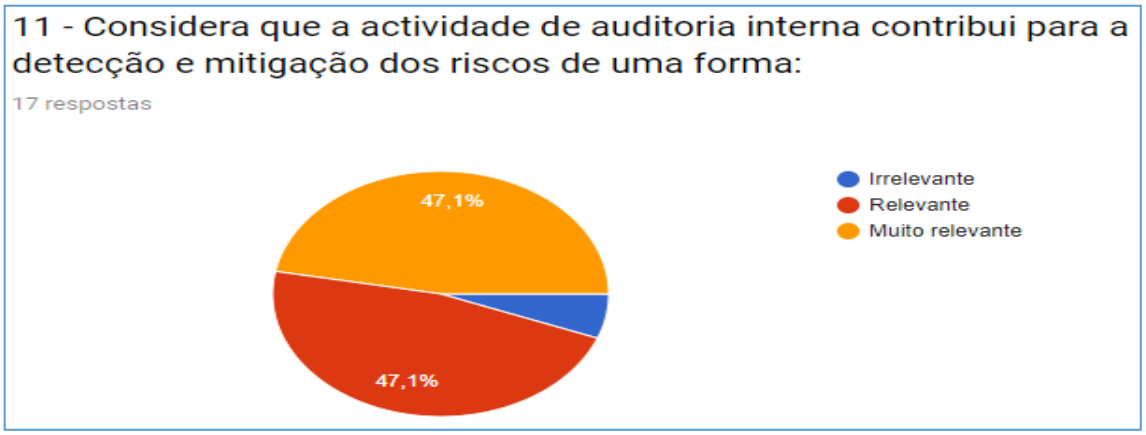


Gráfico 11 – Contribuição da AI para detetar e minimizar o risco

Segundo o gráfico acima, observa-se que 47,1% da amostra (*n* = 17) considera que a atividade de auditoria interna contribui de uma forma muito relevante para a deteção e mitigação dos riscos e 47,1% também considera que contribui de forma relevante.

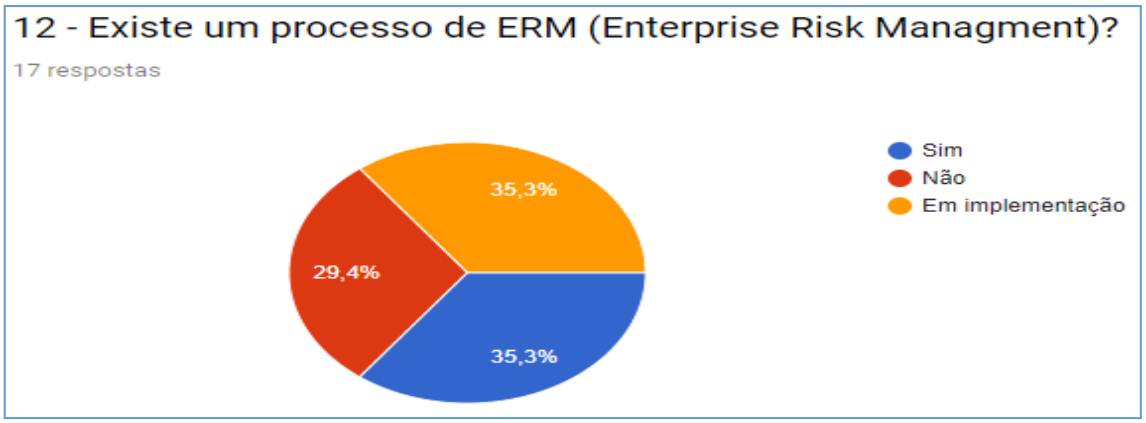


Gráfico 12 – Processo ERM

De acordo com o gráfico, verifica-se que nas empresas que têm departamento de auditoria interna (*n* = 17), 35,3% têm um processo de ERM definido, 35,3% tem o processo em implementação e em 29,4% não existe nenhum processo de ERM.

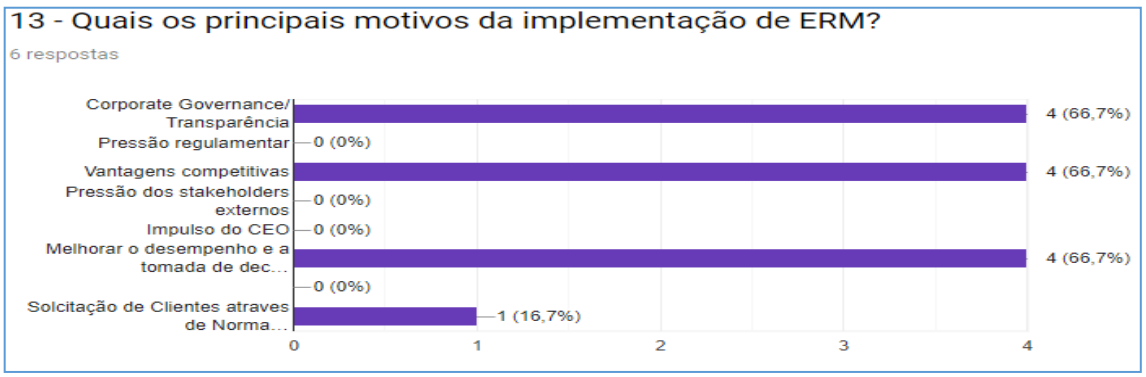


Gráfico 13 – Motivos de implementação de ERM

Analisando o gráfico supra, verifica-se que das empresas que têm um processo de ERM implementado (*n* = 6), 4 dessas empresas que representam 66,7% da amostra identificam como principais motivos para a implementação de ERM o Corporate Governance/Transparência, as vantagens competitivas e melhorar o desempenho e a tomada de decisões. Uma das empresas identificou que o motivo para a implementação de ERM foi uma solicitação de clientes para o cumprimento da norma VDA (norma para fornecimento de produtos e serviços para a indústria automóvel)

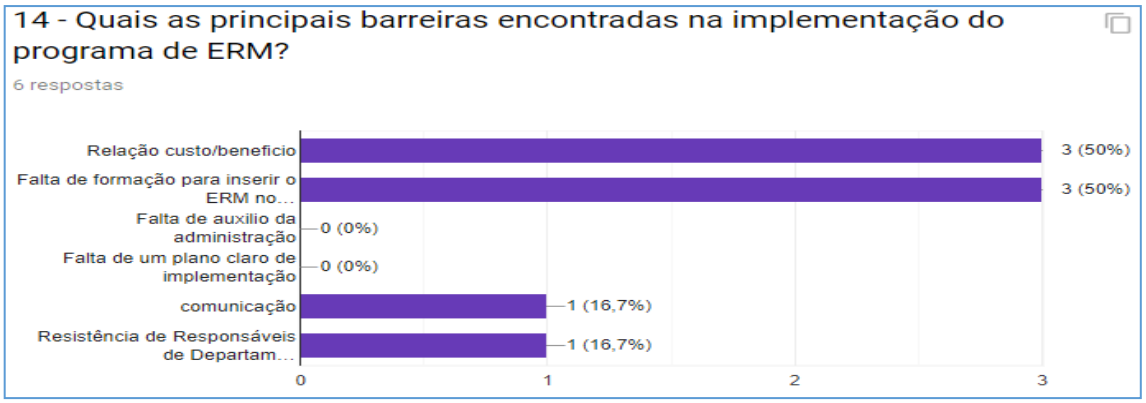


Gráfico 14 – Barreiras para implementação de ERM

Relativamente as principais barreiras encontradas na implementação do programa de ERM, verifica-se da análise do gráfico que 50% das empresas da nossa amostra (n = 6) identifica a relação custo/beneficio e a falta de formação para inserir o ERM no negócio. Tendo sido identificada por uma dessas empresas a falta de comunicação dentro da mesma e por outra a resistência dos responsáveis de departamento.

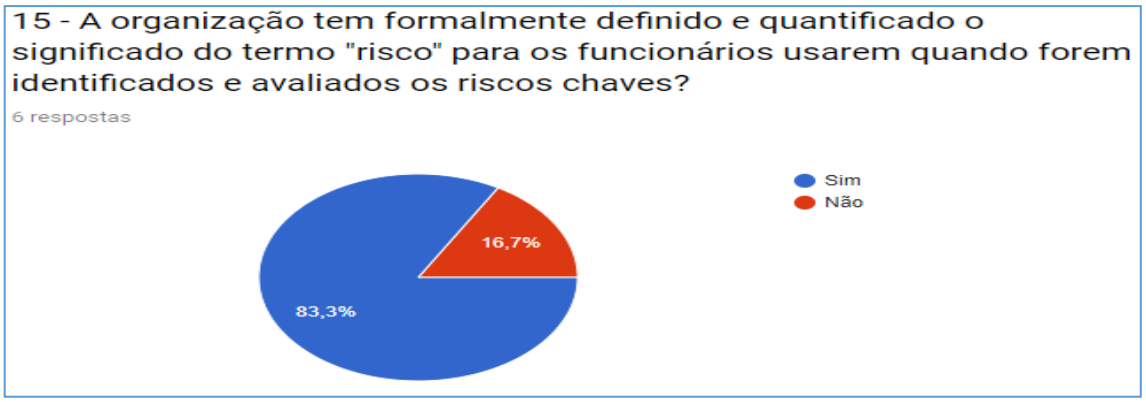


Gráfico 15 – Definição formal do termo “risco”

Segundo o gráfico acima, apenas uma das empresas da amostra que tem implementado um processo de ERM (n = 6), não tem formalmente definido e quantificado o significado do termo “risco” para os funcionários. Todas as outras têm e os funcionários têm conhecimento do mesmo para usarem quando forem identificados e avaliados os riscos chave.

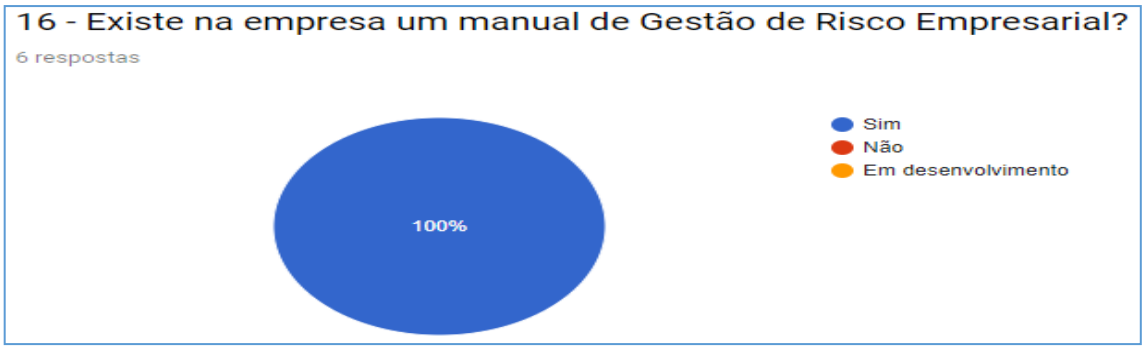


Gráfico 16 – Manual de gestão de risco

De acordo com o gráfico supra, todas as empresas com um processo de ERM implementado (n = 6), possuem um manual de gestão de risco empresarial.

Gráfico 17 – Formação em gestão de risco

No que concerne a formação dos funcionários sobre as ferramentas e técnicas de gestão de risco, apenas uma das empresas da nossa amostra (*n* = 6) não dá essa formação anualmente. Todas as outras fazem formação anual.

Gráfico 18 – Definição do apetite ao risco

Verifica-se que 66,7% das empresas da nossa amostra (*n* = 6) tem definido a exposição total ao risco que está disposta a aceitar, e 33,3% apenas o tem definido parcialmente.

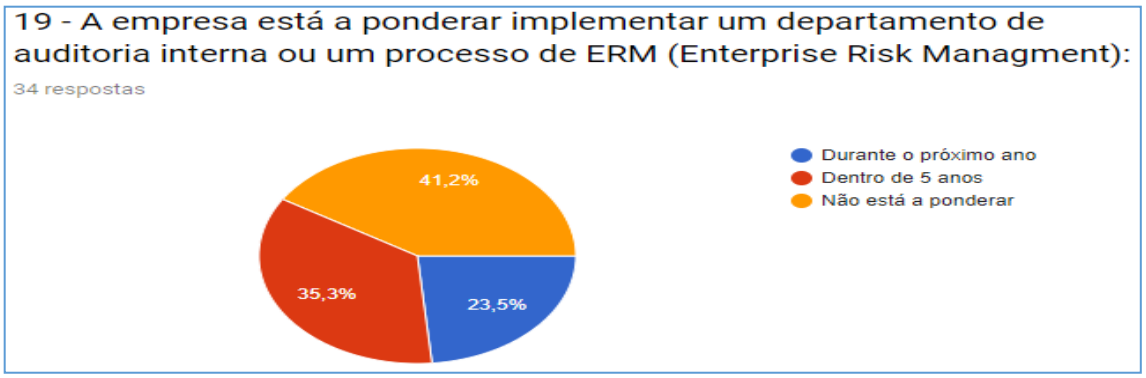


Gráfico 19 – Implementação departamento de AI ou processo ERM

Através da análise ao gráfico acima, verifica-se que 23,5% das empresas da nossa amostra (*n* = 34) está a ponderar implementar um departamento de auditoria interna ou um processo de ERM durante o próximo ano, 35,3% dentro de 5 anos e 41,2% não está a ponderar a implementação.

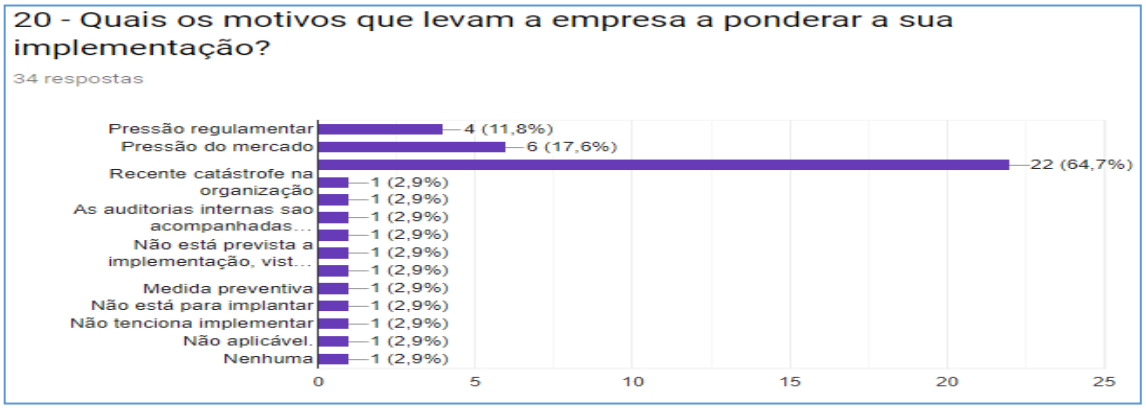
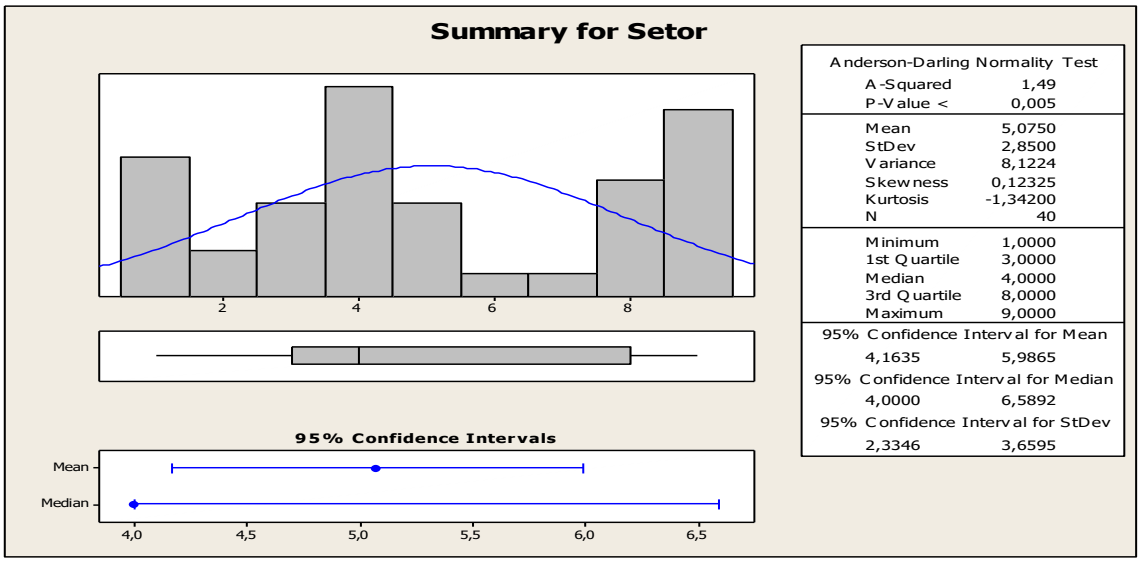


Gráfico 20 – Motivos para implementação

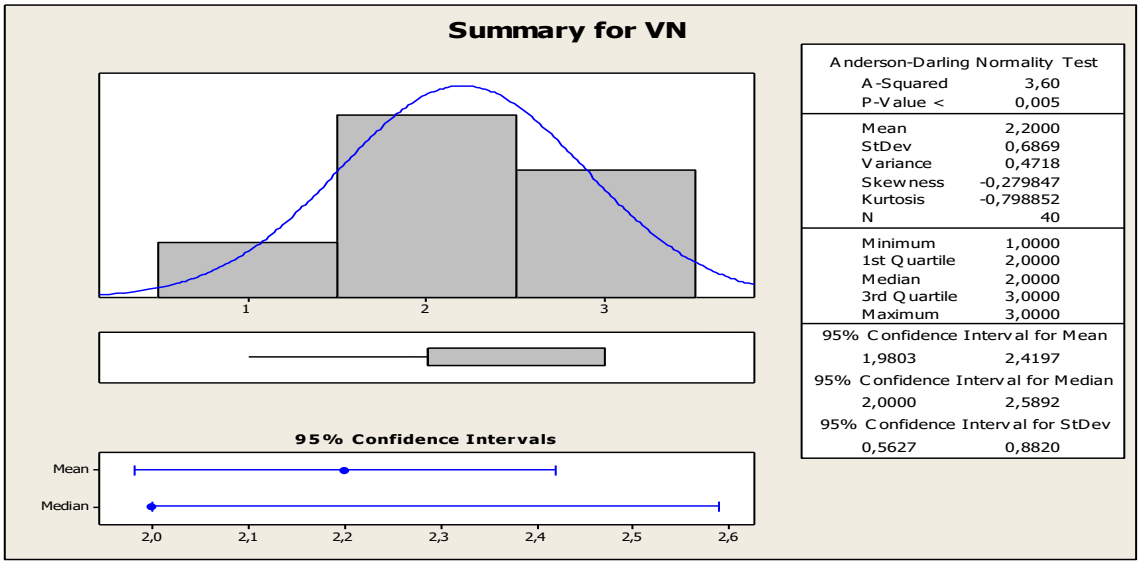
Conforme se verifica-se neste gráfico, 64,7% das empresas da nossa amostra (*n* =34) identificam a melhoria dos processos internos como o principal motivo para a implementação de um departamento de auditoria interna ou de um processo ERM. A pressão do mercado é identificada por 17,6% das empresas e a pressão regulamentar por 11,8%.

De modo a testar as hipóteses formuladas anteriormente e dessa forma responder adequadamente à questão de investigação, recorreu-se às técnicas de inferência estatística.

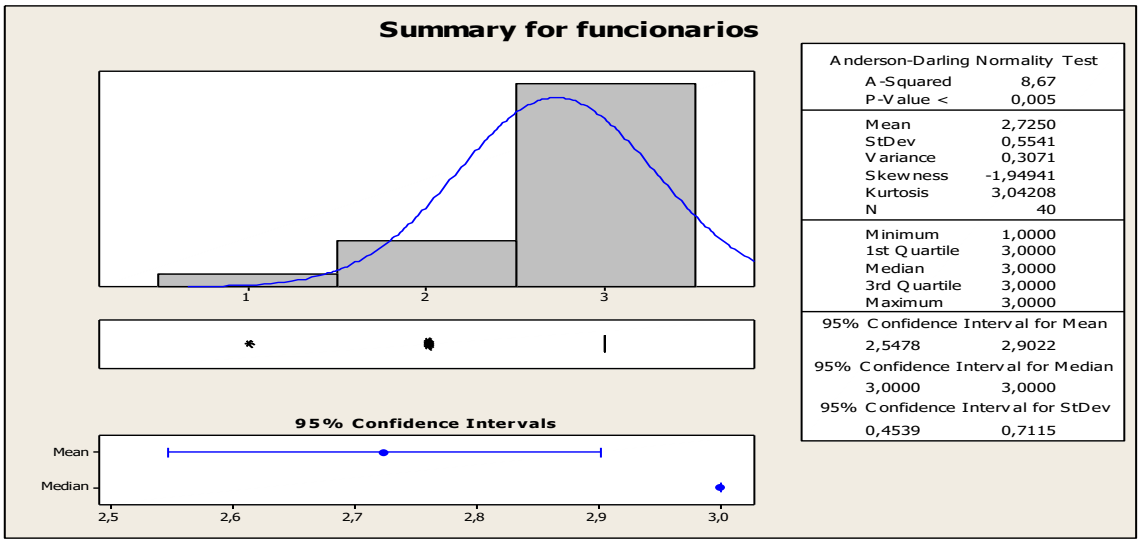
Entende-se por **estatística inferencial** o conjunto de técnicas que permitem identificar relações entre variáveis, relações de associação e extrapolar dados amostrais para a população.



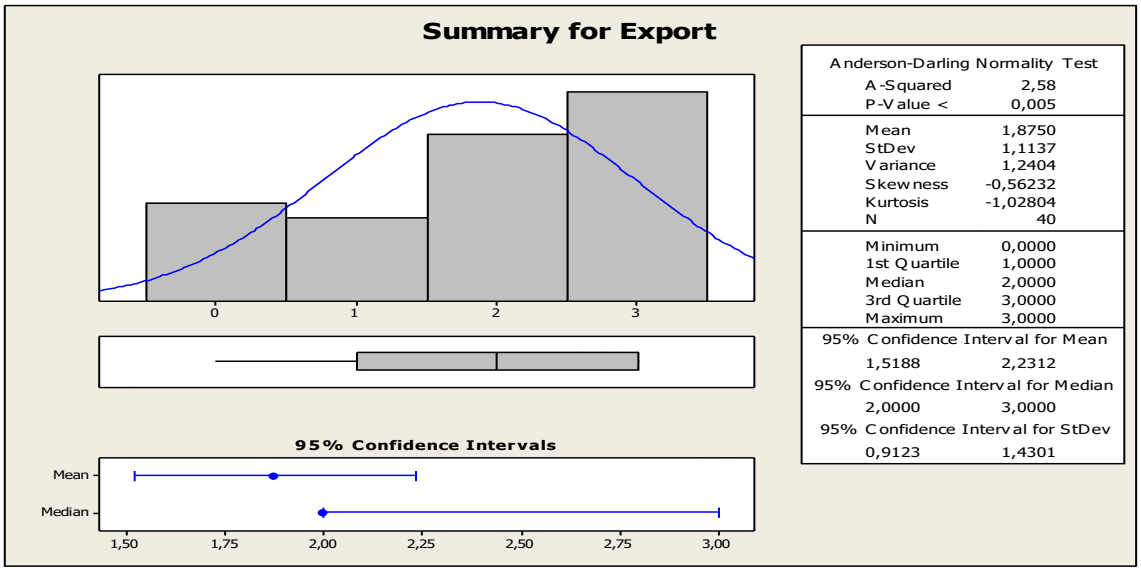
Quadro 1 – Curva de normalidade da variável Setor



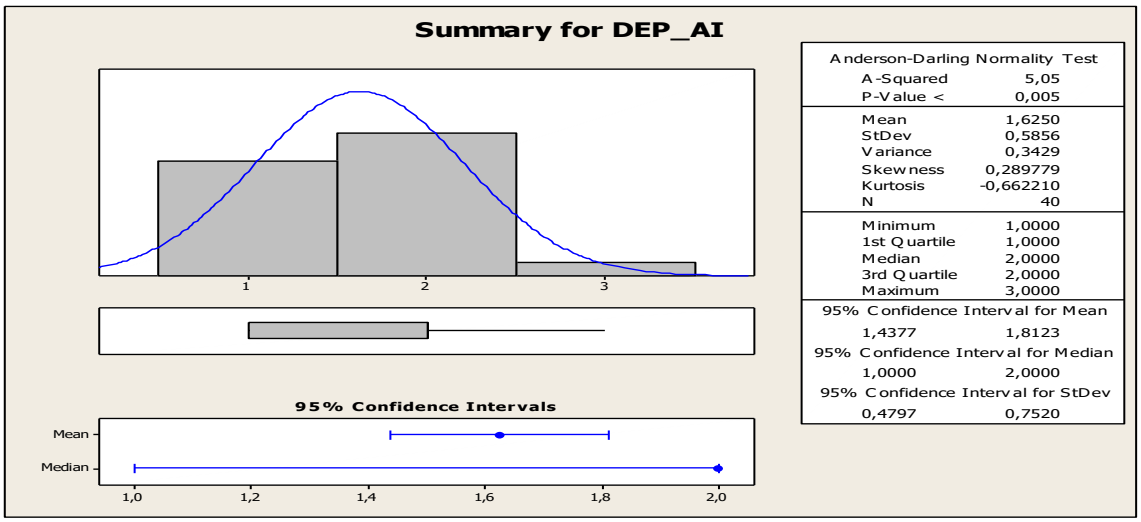
Quadro 2 – Curva de normalidade da variável VN



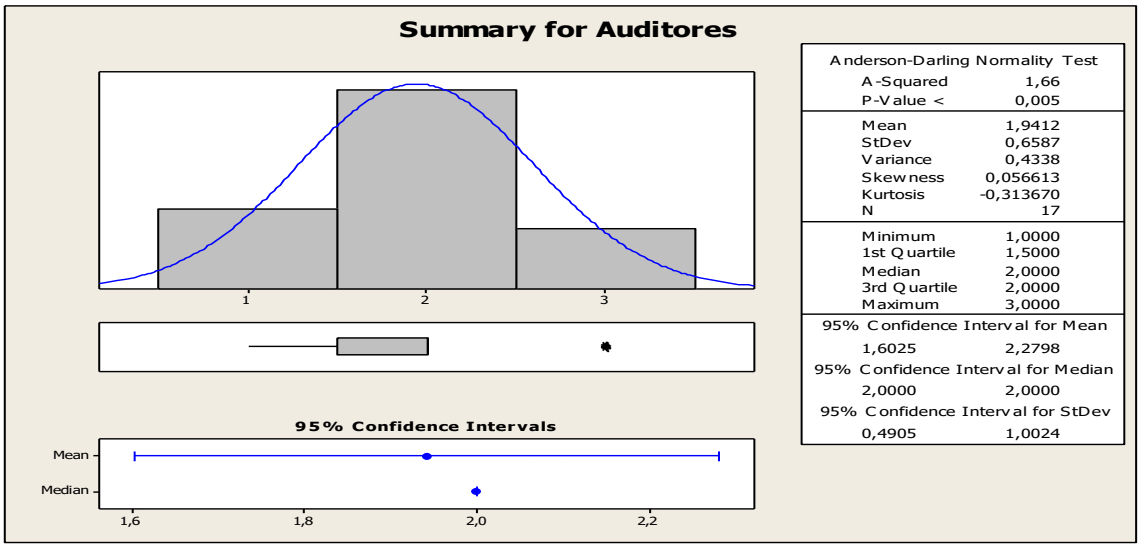
Quadro 3 – Curva de normalidade da variável funcionários



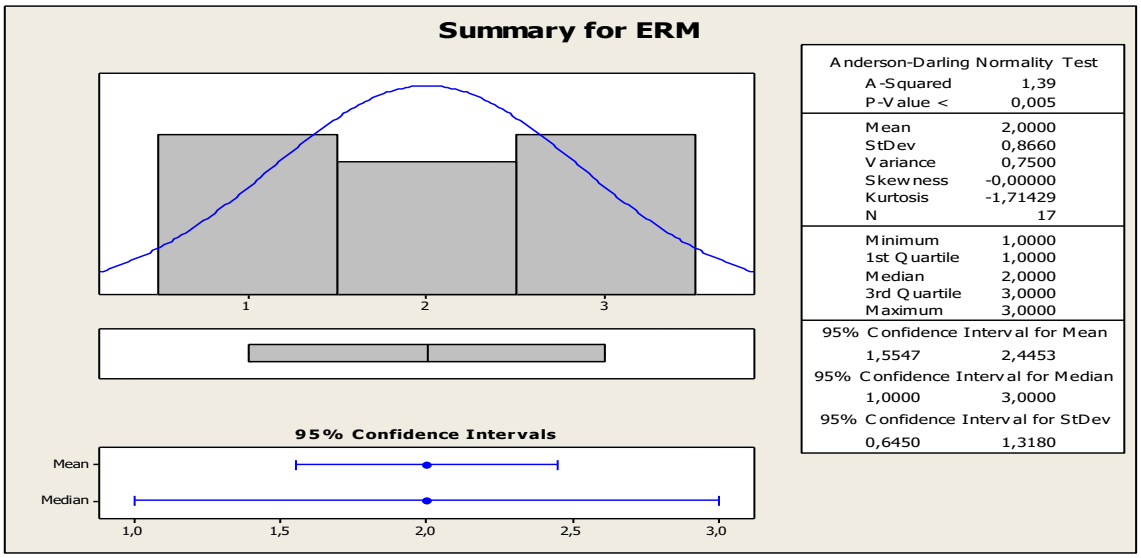
Quadro 4 – Curva de normalidade da variável Export



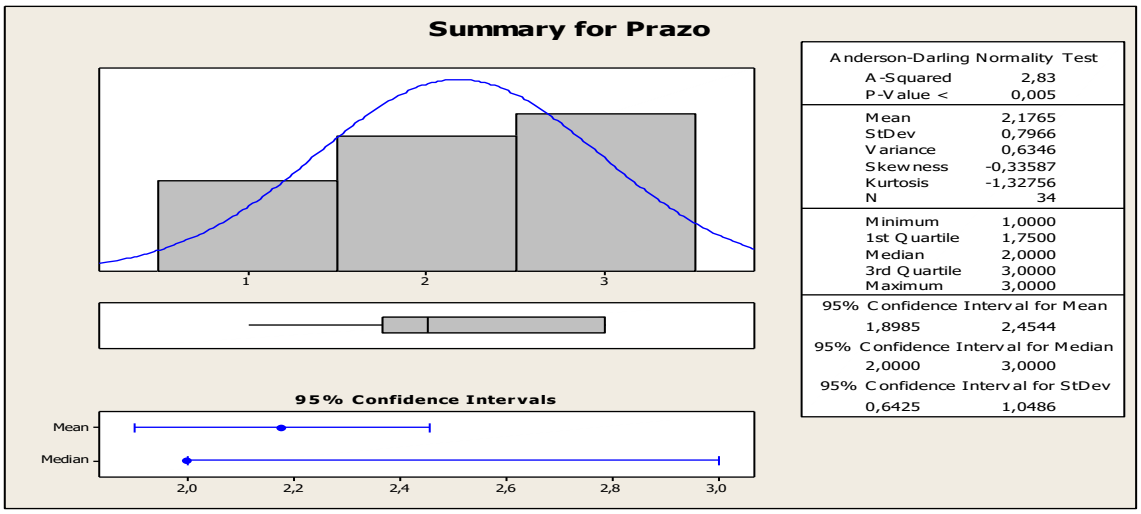
Quadro 5 – Curva de normalidade da variável DEP_AI



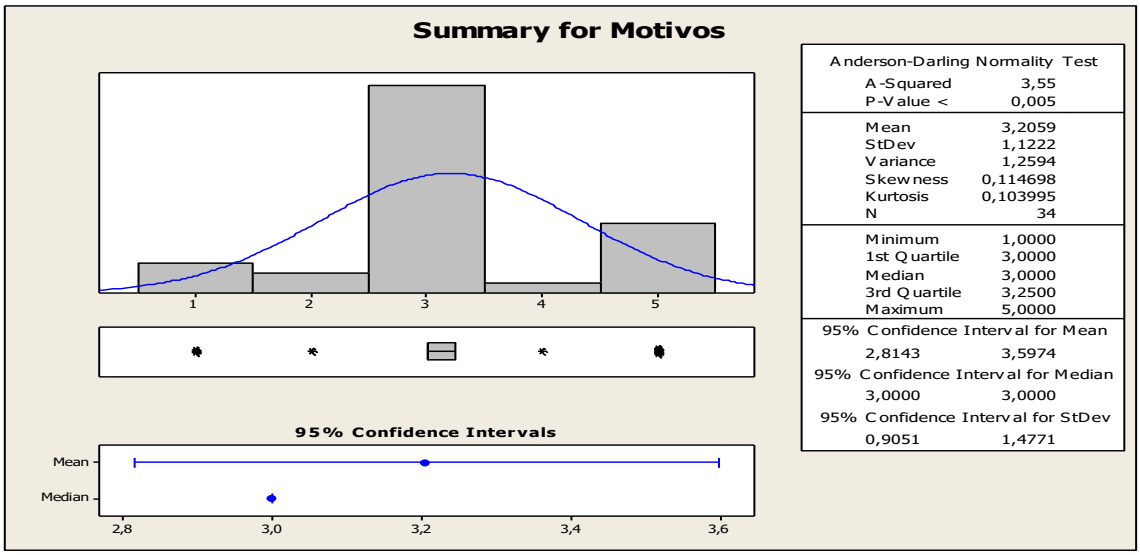
Quadro 6 – Curva de normalidade da variável Auditores



Quadro 7 – Curva de normalidade da variável ERM



Quadro 8 – Curva de normalidade da variável Prazo



Quadro 9 – Curva de normalidade da variável Motivos

Através da análise dos histogramas e respectivas curvas de normalidade obtidas pelo teste de Anderson-Darling (Minitab), conclui-se que os dados não são provenientes de uma população com uma distribuição normal, uma vez que, em todos eles o p-value < 0,05.

Assim, como não existe uma distribuição normal serão utilizados testes não paramétricos que não exigem a existência dessa normalidade nos dados, para análise da questão da investigação, em especial o teste Tau-b de Kendall e Rô de Spearman.

Foi atribuído um nível de significância de 5% ($\alpha = 0,05$), de forma a ser possível afirmar com uma "certeza" de 95% a validade das hipóteses em estudo, ou seja, testar as hipóteses com uma probabilidade de 95%. Deste modo, se a probabilidade for inferior a 0,05 rejeita-se a hipótese nula (H0) e aceita-se a hipótese alternativa (H1).

Hipótese 1

($H0_1$) – O sector de atividade não tem influência na existência de departamento de auditoria interna;

($H1_1$) - O sector de atividade tem influência na existência de departamento de auditoria interna;

Correlações

			Setor	Dep_Auditoria_Interna
tau_b de Kendall	Setor	Coeficiente de Correlação	1,000	,098
		Sig. (bilateral)	.	,476
		N	40	40
	Dep_Auditoria_Interna	Coeficiente de Correlação	,098	1,000
		Sig. (bilateral)	,476	.
		N	40	40
rô de Spearman	Setor	Coeficiente de Correlação	1,000	,124
		Sig. (bilateral)	.	,445
		N	40	40
	Dep_Auditoria_Interna	Coeficiente de Correlação	,124	1,000
		Sig. (bilateral)	,445	.
		N	40	40

Quadro 10 – Testes Tau-b de Kendall e Rô de Spearman às variáveis Setor e DEP_AI

Pelo quadro 10, pode-se verificar que o valor de $p > 0,05$ (Sig.(bilateral) =0,476 e 0,445), o que leva a concluir que a hipótese nula (H0) é aceite com um nível de significância de 5%, isto é, deve concluir-se que o setor de atividade não influencia a existência de um departamento de AI.

Hipótese 2

($H0_2$) – O volume de negócios não influencia a existência de departamento de auditoria interna;

($H1_2$) - O volume de negócios influencia a existência de departamento de auditoria interna;

Correlações

			Dep_Auditoria_Interna	Volume_Negócios
tau_b de Kendall	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,374*
		Sig. (bilateral)	.	,013
		N	40	40
	Volume_Negócios	Coeficiente de Correlação	-,374*	1,000
		Sig. (bilateral)	,013	.
		N	40	40
rô de Spearman	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,393*
		Sig. (bilateral)	.	,012
		N	40	40
	Volume_Negócios	Coeficiente de Correlação	-,393*	1,000
		Sig. (bilateral)	,012	.
		N	40	40

*. A correlação é significativa no nível 0,05 (bilateral).

Quadro 11 – Testes Tau-b de Kendall e Rô de Spearman às variáveis VN e DEP_AI

No que se refere à hipótese 2, verifica-se que o valor de $p < 0,05$ (Sig. Bilateral = 0,013 e 0,012), logo conclui-se que os resultados são significativos, existe uma correlação entre as variáveis, pelo que rejeita-se a hipótese nula (H0) e conclui-se que o volume de negócios influencia a existência de um departamento de AI.

Hipótese 3

($H0_3$) – O número de funcionários não tem influência na existência de departamento de auditoria interna;

($H1_3$) - O número de funcionários tem influência na existência de departamento de auditoria interna;

Correlações

			Dep_Auditoria_Interna	Numero_Funcionários
tau_b de Kendall	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,213
		Sig. (bilateral)	.	,166
		N	40	40
	Numero_Funcionários	Coeficiente de Correlação	-,213	1,000
		Sig. (bilateral)	,166	.
		N	40	40
rô de Spearman	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,222
		Sig. (bilateral)	.	,168
		N	40	40
	Numero_Funcionários	Coeficiente de Correlação	-,222	1,000
		Sig. (bilateral)	,168	.
		N	40	40

Quadro 12 – Testes Tau-b de Kendall e Rô de Spearman às variáveis funcionários e DEP_AI

Segundo o quadro …., o valor de $p > 0,05$ (Sig. Bilateral = 0,166 e 0,168), o que permite afirmar que nesta hipótese aceita-se a hipótese nula (H0), pelo que conclui-se que o número de funcionários não tem influência na existência de um departamento de AI.

Hipótes 4

($H0_4$) – A percentagem de exportação não influencia a existência de departamento de auditoria interna;

($H1_4$) - A percentagem de exportação influencia a existência de departamento de auditoria interna;

Correlações

			Dep_Auditoria_Interna	Percentagem_Exportação
tau_b de Kendall	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,247
		Sig. (bilateral)	.	,087
		N	40	40
	Percentagem_Exportação	Coeficiente de Correlação	-,247	1,000
		Sig. (bilateral)	,087	.
		N	40	40
rô de Spearman	Dep_Auditoria_Interna	Coeficiente de Correlação	1,000	-,282
		Sig. (bilateral)	.	,078
		N	40	40
	Percentagem_Exportação	Coeficiente de Correlação	-,282	1,000
		Sig. (bilateral)	,078	.
		N	40	40

Quadro 13 – Testes Tau-b de Kendall e Rô de Spearman às variáveis Export e DEP_AI

No que se refere a hipótese 4, também $p > 0,05$ (Sig.bilateral = 0,087 e 0.078), pelo que aceita-se a hipótese nula (H0), e conclui-se que a percentagem de exportação não influencia a existência de um departamento de AI.

4.3 Discussão dos resultados

Após a apresentação dos resultados e do seu respectivo tratamento estatístico, irá proceder-se à sua análise e interpretação.

De acordo com os resultados obtidos no questionário, de um universo de 250 empresas, responderam apenas 40.

Em termos médios, estas 40 empresas são predominantemente do setor do comércio, com um volume de negócios entre os 10M€ e os 20M€, em regra com mais de 50 funcionários e normalmente com exportações acima de 10% do seu volume de negócios.

Verifica-se também que das 40 respostas obtidas, 42,5%, ou seja, 17 destas empresas têm um departamento de AI que em média é constituído por 2 a 5 auditores.

Estes departamentos de AI, de acordo com as respostas atuam principalmente na área da qualidade/processos e na área financeira/contabilística.

Pode-se também concluir, pela análise das respostas que o órgão da administração/gestão participa na implementação da atividade de AI, e que a missão da função de AI é conhecida pelos colaboradores da empresa, sendo-lhes transmitido quais os seus principais objetivos.

Pode-se concluir assim, que nas empresas onde está implementada a atividade de AI, existe o envolvimento de todos, desde o órgão de gestão aos funcionários da empresa, para o sucesso dessa implementação.

As empresas que responderam, consideram também que a AI fornece informações relevantes para o processo de tomada de decisões dos gestores, contribuindo para a deteção e mitigação dos riscos.

Também de acordo com as respostas, verifica-se que apenas em 6 dessas empresas existe um processo de *Enterprise Risk Management*, estando a ser implementado em outras 6.

Foram identificados três motivos principais para a implementação do processo de ERM: corporate governance/transparência; vantagens competitivas e melhorar o desempenho e a tomada de decisões. Conclui-se assim, que estas empresas estão atentas à constante volatilidade dos mercados e pretendem posicionar-se numa posição de destaque relativamente à sua concorrência, pela introdução do processo de gestão de riscos na empresa.

Verificou-se que as 2 principais barreiras para a implementação de um processo de ERM são a relação custo/benefício e a falta de formação para inserir o ERM no negócio.

Constata-se também, que das empresas onde existe um processo de ERM, todas têm um manual de gestão de risco empresarial e em 83,3% destas o termo "risco" está formalmente definido e quantificado.

Estas empresas, em regra, formam os seus funcionários anualmente sobre as ferramentas e técnicas de gestão de risco, e em apenas 2 delas não existe uma definição do apetite ao risco, ou seja, do risco que a empresa está disposta a aceitar.

Finalmente, verifica-se que 58,8% das empresas que não têm departamento de AI nem um processo de ERM, estão a ponderar a sua implementação durante os próximos 5 anos, e apontam como principal motivo para essa implementação a melhoria dos processos internos.

Pode-se assim concluir que as empresas do distrito de Leiria, ainda que muito timidamente, estão a começar a olhar para a gestão de risco como uma ferramenta bastante importante na criação de valor para a empresa.

Através da formulação de algumas hipóteses, com o objetivo de aprofundar o tema em investigação, e do seu tratamento estatístico no SPSS, através dos testes Tau-b de Kendall e Rô de Spearman, conclui-se que das várias variáveis analisadas, apenas o volume de negócios pode influenciar a existência ou não de um departamento de AI.

5 CONCLUSÃO E RECOMENDAÇÕES

Pretendeu-se com a realização deste trabalho, discutir qual a importância da auditoria interna e da gestão de riscos nas empresas, e até que ponto estas incorporam estes dois conceitos como "boas práticas" empresariais para auxiliar os decisores na prossecução do seu negócio.

Inicialmente foi feita uma revisão de literatura, revisitando os conceitos de auditoria interna, controlo interno, gestão de risco, ERM, entre outros. Numa segunda parte foi realizado um trabalho de investigação, com a formulação de hipóteses, para verificarmos, se a implementação da auditoria interna e da gestão de risco nas empresas do distrito de Leiria, dependem de alguma forma das características da própria empresa (volume negócios, setor de atividade, número de funcionários, percentagem de exportação).

Assim, verificamos que a auditoria interna passou por várias fases, onde inicialmente era conhecida como "o controlo dos controlos", por centrar a sua função essencialmente na avaliação da fiabilidade dos controlos internos. Posteriormente houve uma mudança de paradigma onde a auditoria interna deixou de estar focalizada no controlo e transferiu a sua focalização para os riscos, passando a sua atividade a ser mais abrangente destinada a acrescentar valor e a melhorar as operações de uma organização.

Correr riscos é um facto inerente à própria existência de uma empresa, pressupondo contudo, que esta tenha capacidade e vontade de inovar e gerar riqueza, aproveitando assim as oportunidades que lhe vão surgindo de todo o meio envolvente.

A gestão de risco é um meio para atingir um fim e, não um fim em si mesmo. É um processo educativo que nos consciencializa que de facto existem riscos, e que aos gestores cabe a responsabilidade de os gerir.

O processo de ERM adota uma perspectiva que coordena a gestão de risco ao longo de toda a organização, o que o caracteriza em relação as formas tradicionais de gestão de risco que encaram o risco individualmente por áreas.

Segundo o COSO (2204), toda a estrutura de gestão de risco é conduzida com o fim de alcançar os objetivos de uma organização que são, concretamente, classificados em quatro categorias (objetivos estratégicos, operacionais, relato e conformidade).

Por sua vez, existe uma relação direta entre os objetivos, que as organizações tentam alcançar, e os componentes de gestão de risco, que representam os meios para atingir os mesmos objetivos. Neste sentido o COSOERM reconhece oito componentes que, relacionados entre si, permitem um processo de gestão de risco eficaz, e que são o ambiente interno; fixação de objetivos; identificação de eventos; avaliação do risco; mitigação dos riscos; atividades de controlo; informação e comunicação e, por fim, o acompanhamento. A associação destes componentes permitem compreender se a gestão do risco é eficaz. (COSO: 2004).

A gestão de riscos, como vinha a ser praticada, ajudou muitas organizações a identificar, avaliar e gerir os riscos da estratégia. No entanto as causas mais referidas de destruição de valor, residem na possibilidade de a estratégia não suportar a missão e a visão da entidade, e nas implicações decorrentes da estratégia escolhida.

O novo f*ramework (Enterprise Risk Management – Integrating with Strategy and Performance)* elaborado pelo COSO em 2017, ressalta a importância da utilização da gestão de riscos na definição da estratégia alinhada à missão, valores e visão, e determina que o sucesso para um desempenho operacional gerador de riqueza acontece através da integração e equilíbrio de todos os departamentos e funções com o foco em riscos.

A Auditoria Interna no âmbito do ERM, tem como principais objetivos: certificar os processos de gestão de risco; certificar que os riscos estão corretamente identificados e avaliados; avaliar os processos de gestão de risco; avaliar o reporte dos principais riscos e rever a gestão dos principais riscos.

É através da verificação e análise da eficiência e eficácia do sistema de controlo interno, que a AI auxilia o órgão de gestão a, caso seja necessário, efetuar as devidas correções junto dos departamentos em que os controlos internos não estão a ser devidamente cumpridos.

Pode-se assim concluir, que a auditoria interna desempenha um papel fundamental no apoio ao órgão de gestão, aquando da sua função de tomada de decisões, através das informações recolhidas, contribuindo positivamente para o alcance dos resultados estipulados pelas organizações, facilitando a redução dos riscos a que as empresas estão expostas.

As organizações continuaram a enfrentar um futuro repleto de volatilidade, complexidade e ambiguidade, sendo a gestão de riscos um fator importante para a maneira como a organização conduzirá os seus negócios.

Todas as entidades precisam apresentar características que determinem respostas eficazes a mudanças, o que inclui agilidade na tomada de decisões, habilidade de responder de maneira coesa e capacidade de se adaptar e se reposicionar, mantendo durante todo esse processo altos níveis de confiança de todos os *stakeholders*. (COSO:2017).

Podem-se identificar diversas tendências que terão impacto na gestão de riscos no futuro, das quais se destacam: lidar com a proliferação de dados (cada vez são disponibilizados mais dados e a gestão de risco tem de se adaptar quanto à velocidade para analisar esses dados); alavancar inteligência artificial e automação (a gestão de risco devem analisar o impacto de novas tecnologias e tirar proveito das suas capacidades); administrar o custo da gestão de riscos e construir organizações mais fortes (ao conhecer os riscos que terão maior impacto na entidade, as organizações podem usar a gestão de riscos para apoiá-las na criação de competências que lhes permitam atuar com antecedência, criando novas oportunidades).

Quanto a questão inicialmente proposta para análise, ou seja, qual o grau de maturidade da Auditoria Interna nas empresas do distrito de Leiria e de que modo a Gestão de Risco é uma das preocupações dos órgãos de gestão e qual a sua importância estratégica, conclui-se que apesar de já se verificarem alguns avanços relativamente a estas matérias, as empresas do distrito de Leiria, ainda não olham para a gestão de risco como uma ferramenta bastante importante na criação de valor para a empresa.

Constatou-se pela investigação que quase 50% das empresas da amostra tem um departamento de auditoria interna, no entanto relativamente a gestão de risco apenas 6 dessas empresas têm um processo de ERM definido, concluindo-se assim quês estas ainda não são uma prioridade dos órgãos de administração/gestão das empresas do distrito de Leiria.

No entanto, apesar dos resultados obtidos, a reduzida dimensão da amostra não permite a sua generalização, consistindo esta uma limitação do estudo.

Para finalizar, salienta-se que no decorrer deste trabalho surgiram algumas questões que poderão constituir um desafio para futuras pesquisas, entre elas, a importância do órgão

de gestão na definição dos processos de gestão de risco e qual a importância da utilização da gestão de riscos na definição da estratégia alinhada com a missão.

REFERÊNCIAS BIBLIOGRÁFICAS

- Almeida, D.(2009) – *"Auditoria Interna e Gestão do Risco"*. XVI Conferência Anual do IPAI.
- Arens, A. & Beasley, M. & Elder, R. (2010) – *"Auditing and Assurance Services – An integrated approach"*. New Jersey: Pearson Education, Inc.
- Attie, W. (2006) – *"Auditoria – Conceitos e Aplicações"*. São Paulo: Editora Atlas, SA.
- Almeida, M. (2003) – *"Auditoria – Um curso moderno e completo"*. 6ª Edição. São Paulo: Editora Atlas, SA.
- Basile, O. (2010) – *"Auditoria Interna do Futuro: Você está preparado?"*. Congresso Latino Americano de Auditoria Interna 2010. Disponível em https://portal.tcu.gov.br/en_us/biblioteca-digital/clai-2010-auditoria-interna-do-futuro-voce-esta-preparado.htm e acesso em 15 Dezembro de 2018.
- Boynton, William C. & Johnson, R. & Kell, W. (2001) – *"Auditoria"*. São Paulo: Editora Atlas, SA.
- Brasiliano, A. – *"COSO II (ERM) se adapta ao mundo VICA – mudando seu Framework para o nível estratégico"* Disponível em https://www.linkedin.com/pulse/coso-ii-erm-se-adapta-ao-mundo-vica-mudando-seu-para-brasiliano e acesso em 2 de Março de 2019.
- Castanheira, N. & Rodrigues, L. (2006) – *"Gestão de risco – Da abordagem tradicional à gestão de risco empresarial (ERM)"*. Revisores e Empresas (Julho/Setembro 2006).
- Cicco, F. (2007) – *"Auditoria baseada em riscos – Como implementar a ABR nas organizações: uma abordagem inovadora"*. Disponível em http://www.risktecnologia.com.br/AMOSTRA_%20Manual_ABR.pdf e acesso em 12 de Março de 2019.
- Cicco, F. (2014) – *"Auditoria baseada em riscos aplicada a sistemas de gestão"*. Disponível em http://www.academia.edu/33692712/AUDITORIA_BASEADA_EM_RISCOS_APLICADA_A_SISTEMAS_DE_GEST%C3%83O e acesso em 12 de Janeiro de 2019.
- COSO (2017) – *"Enterprise Risk Management – Integrating with Strategy and Performance – Frequently Asked Questions"*

- COSO (2017) – *"Enterprise Risk Management – Integrating with Strategy and Performance – Executive Summary"*
- COSO (2004) – *"Enterprise Risk Management – Integrated Framework"*
- Costa, B. (2010) – *"Auditoria Financeira: Teoria e Prática"*. Rei dos Livros.
- Deloitte (2012) – *"Inteligência em gestão de riscos – Dois estudos e uma abordagem diferenciada para apoiar sua empresa a se preparar melhor para o futuro"*
- Deloitte (2017) – *Os cinco pilares dos riscos empresariais – Como gerenciá-los em um cenário económico e de negócios desafiador"*. Disponível em https://www2.deloitte.com/content/dam/Deloitte/br/Documents/risk/Os-Cinco-Pilares-dos-Riscos-Empresariais-Deloitte.pdf e acesso em 15 Dezembro de 2018.
- Dias, Alcina A. (2018) – *"A more effective audit after COSO ERM 2017 or after ISO31000:2009?"*. Disponível em https://www.occ.pt/dtrab/trabalhos/xviicica/finais_site/70.pdf e acesso em 2 de Março de 2019.
- Ferreira, Albertina C. (2010) – *"A Gestão de Rico aplicada à Auditoria Interna"*. Dissertação de Mestrado de Contabilidade e Auditoria, Universidade de Aveiro.
- Gomes, E. (2014) – *"A importância do Controlo Interno no Planeamento de Auditoria"*. Revisores e Auditores (Jan-Mar2014).
- Gonçalves, A. (2008) – *"PME'S – A Evolução das Metodologias de Auditoria"*. Revisores e Auditores (Jul/Set 2008).
- Hussein, H. (2008) – *"Using COBIT as a Guide Risk Assesment Assurance Services"*
- IIA (2013) – "*Declaração de Posicionamento do IIA: As três linhas de defesa no gerenciamento eficaz de riscos e controles"*
- IIA (2009) – *"Declaração de Posicionamento do IIA: O papel da Auditoria Interna no gerenciamento de riscos corporativo"*
- IIA (2009) – *"Why Enterprise Risk Management is Vital"*. Disponível em https://bookstore.theiia.org/why-enterprise-risk-management-is-vital-learning-from-company-experiences-with-sarbanes-oxley-404-compliance e acesso em 8 Dezembro de 2018.

- IIA (2004) – *"The Role of Internal Auditing in Eterprise-wide Risk Management"*.
- IIA (2007) – "*Internal Auditing and ERM: Fiting in and Adding Value"*
- KPMG (2013) – *"Gestão do Risco em Portugal: Desafios para as empresas"*. Disponível em http://www.empresasfamiliares.pt/estudos?article=7529-estudo-kpmg-gestao-de-risco-em-portugal-2013 e acesso em 15 Dezembro de 2018.
- Madariaga, J. (2004) – *"Manual Prático de Auditoría"*. Barcelona: Ediciones Deusto.
- Marques, M. (1997) – *"Auditoria e Gestão"*. Lisboa: Editorial Presença
- Morais, G. & Martins, I. (2013) – *"Auditoria Interna – Função e Processo"*. 4ª Edição. Lisboa:Áreas Editora.
- Oliveira, J. (2011) – *"Modelo Integrado para uma Gestão Eficiente e Controlo do Risco"*. Porto: Vida Económica
- Pardini, Eduardo P. (2017) – *"Estrutura do COSO gestão de riscos – Conhecendo os principais pontos da actualização"*. Disponível em https://www.linkedin.com/pulse/estrutura-do-coso-gest%C3%A3o-de-riscos-conhecendo-os-da-person-pardini, acesso em 11 de Janeiro de 2019
- Pinheiro, C. (2013) – *"Acrescentar valor à organização com a Auditoria Interna"*. Dissertação de Mestrado em Auditoria no Instituto Superior de Contabilidade e Administração do Porto.
- Pinheiro, J. (2008) – *"Auditoria Interna – Manual Prático para Auditores Internos"*. Editora Rei dos Livros.
- Pinheiro, J. (2005) – *"Auditoria Interna – Criar sucesso"*. Revista de Auditoria Interna. (Out/Dez 2005).
- Pires, M. & Pacheco, L. & Tavares, F. (2016) – *"Gestão do Risco nas PME de Excelência Portuguesas"*. Disponível em http://www.scielo.mec.pt/scielo.php?script=sci_abstract&pid=S2182-84582016000200015&lng=pt&nrm=iso e acesso em 18 de Janeiro de 2019.
- PWC (2018) – *"Tendências emergentes de Gestão de Risco"*. Disponível em http://www.ipai.pt/fotos/gca/pwc_pms__ipai_conferencia_anual_1542647794.pdf e acesso em 15 de Fevereiro de 2019.

- PWC (2012) – *"Posicionamento da auditoria interna. Você está no nível certo?"*. Estudo sobre a situação da profissão de Auditoria Interna em 2012. Brasil
- RIMS e IIA(2012) – *"Risk Management and Internal Audit – Forging a Collaborative Alliance"*
- Sá, Tiago N. (n.d.) – *"A evolução do conceito de gestão do risco e a sua ligação com o governo das sociedades"*. Disponível em https://www.occ.pt/news/comcontabaudit/pdf/80.pdf e acesso em 12 de Janeiro de 2019.
- Silva, A. (2012) – *"Técnicas Estatísticas em Auditoria"*. Apontamentos do Mestrado de Auditoria Empresarial e Pública. ISCAC.
- Sousa, O. (2007) – *"Auditoria Interna – Evolução para além da Sarbanes-Oxley"*. Revista nº26 do IPAI