INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

ISCAL

ADOÇÃO DAS ISO PELAS ORGANIZAÇÕES – CONTRIBUTOS DA AUDITORIA E DO CONTROLO INTERNO – ESTUDO DE CASO

Ana Sofia Fontinha Duarte

Lisboa, novembro de 2019

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

ADOÇÃO DAS ISO PELAS ORGANIZAÇÕES – CONTRIBUTOS DA AUDITORIA E DO CONTROLO INTERNO- ESTUDO DE CASO

Ana Sofia Fontinha Duarte

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica da Professora Especialista, Mestre Ana Isabel Marinho Pires da área de Riscos Empresariais e Controlo Interno.

Constituição do Júri:

- Prof. Especialista Gabriel Alves – Presidente

- Prof.ª Doutora Ana Catarina Kaizeler – Arguente

- Prof.ª Especialista Ana Marinho Pires - Vogal

Lisboa, novembro de 2019

Agradecimentos

Em primeiro lugar, gostaria de agradecer à minha família, em especial à minha mãe, avó e irmão, por terem estado sempre a meu lado, incentivando-me a nunca desistir dos objetivos e desafios a que me proponho e ainda pela compreensão que sempre tiveram, pela vontade de ajudar e pelos conselhos dados. Ao meu namorado, por ao longo destes anos me ter incentivado a lutar por aquilo em que acredito, me ter acompanhado e ter sempre uma palavra de apoio para me dar.

Gostaria ainda de mostrar a minha gratidão à Professora Especialista, Mestre Ana Isabel Marinho Pires pela disponibilidade demonstrada na orientação pedagógica deste projeto, pelas linhas orientadoras e sugestões que ao longo deste último ano me foi facultando.

A todos os inquiridos e colegas de trabalho, pela cooperação nas respostas ao inquérito, e pela disponibilidade demonstrada, permitindo assim que os objetivos da investigação fossem cumpridos.

A todos, muito obrigada.

Resumo

Para fazer face às exigências cada vez mais vincadas do mercado e dos clientes, as empresas necessitam de formas de se destacarem. A implementação de sistemas de gestão certificados têm ganho particular interesse em diversos sectores de negócio, principalmente o sistema de gestão da qualidade e o sistema de gestão de segurança da informação.

Os objetivos da presente investigação são evidenciar o papel da profissão de auditoria e do controlo interno na implementação de tais sistemas numa determinada organização e as sinergias decorrentes do sistema de controlo interno com os requisitos das normas que regem esses mesmos sistemas.

A metodologia utilizada para o suporte empírico da presente dissertação foi o estudo de caso, por meio da utilização de inquéritos por questionário, dirigido aos colaboradores da empresa e realizados através de uma plataforma online, tendo as respostas alcançado o total da amostra selecionada, cujas questões, suportadas pela revisão teórica, permitiram responder às perguntas de investigação e validar ou não as hipóteses formuladas.

Concluiu-se que os requisitos das normas são em muito semelhantes às componentes do controlo interno e as exigências que delas resultam levam à adoção de diversos documentos como manuais, políticas, procedimentos entre outros que permitem o aumento da robustez do controlo interno.

Conclui-se ainda que a auditoria interna e externa são fundamentais para estes processos através das atividades que realizam, e que da implementação destes sistemas resultam diversos benefícios, mas também algumas limitações. Conseguir a certificação, origina um maior reconhecimento comprovando assim que é uma das formas de destaque mais bem-sucedidas.

Palavras chave: Auditoria; Sistema de Gestão de Qualidade, Sistema de Gestão de Segurança da Informação; Controlo Interno.

Abstract

To meet the growing demands of the market and customers, companies need ways to exceed themselves. The implementation of certified management systems has gained interest in several business sectors, mainly the quality management system and the information security management system.

The aim of the present investigation is to highlight the role of the audit and internal control in the implementation of such systems in a certain organization as well as the synergies arising from the internal control system with the requirements of the standards governing those systems.

The methodology used for the empirical support of the present dissertation was the case study, through the use of questionnaires, directed to the company's employees and conducted through an online platform, the answers reached the total of the selected sample, whose questions, supported by the theoretical review, allowed to answer the research questions and validate or not the formulated hypotheses.

It was concluded that the requirements of standards are very similar to the components of internal control and the resulting requirements lead to the implementation of several documents such as manuals, policies, procedures, among others, which increase the strength of internal control.

It is also concluded that internal and external audit are fundamental to these processes through the activities they perform, and that the implementation of these systems result in several benefits, but also some limitations. Achieving certification results in greater recognition, thus proving to be one of the most successful forms of prominence.

Key words: Audit; Quality Management System; Information Security Management System; Internal Control.

Índice

Índice Tabelas

Índice Figuras

Índice Gráficos

Lista de Abreviaturas

APCER - Associação Portuguesa de Certificação

BSI - *British Standards Institution*

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

COBIT - *Control Objectives for Information and Related Technologies*

DAF – Departamento Administrativo Financeiro

EIC - Empresa Internacional de Certificação

GARH – Gestão Administrativa de Recursos Humanos

IPAI - Instituto Português de Auditoria Interna

IPQ - Instituto Português da Qualidade

ISO - *Internacional Organization for Standardization*

PDCA – Plan-Do-Check-Act

RH – Recursos Humanos

SCI - Sistema de controlo interno

SGQ – Sistemas de Gestão da Qualidade

SGSI - Sistemas de Gestão de Segurança da Informação

TI – Tecnologia de Informação

1.Introdução

Cada vez mais, as empresas são confrontadas com a evolução e competitividade existentes no mercado em que operam, surgindo por isso a necessidade de se destacarem de forma positiva das restantes.

As formas escolhidas para tal destaque podem ser diversas, tendo vindo a ganhar relevância a melhoria dos sistemas de gestão, nomeadamente o sistema de gestão da qualidade e o sistema de gestão de segurança da informação.

Assim sendo, será feita uma breve apresentação da relevância do tema, seguindo-se a descrição do objeto e objetivos do estudo, qual a metodologia selecionada para a elaboração deste estudo e a estrutura do mesmo.

1.1. Relevância do tema

A presente investigação vem abordar dois aspetos que são hoje uma preocupação nas organizações, a Qualidade e a Segurança da Informação e em como a auditoria auxilia a adoção da implementação das normas emitidas pela *Internacional Organization for Standardization* (ISO). Nomeadamente, foi estudada a implementação da ISO 9001:2015 - Sistemas de Gestão da Qualidade (SGQ) e a ISO 27001:2013 - Sistemas de Gestão de Segurança da Informação (SGSI) em determinada organização.

A qualidade é hoje considerada um fator determinante de sucesso e de competitividade de qualquer organização e tem vindo a intensificar-se devido à globalização dos mercados, à evolução tecnológica, às exigências dos clientes e à competitividade entre as diversas empresas do mesmo ramo de negócio.

Implementar um SGQ pode ser considerado um desafio dado que exige mudanças e sacrifícios de toda a organização, mas é considerado uma garantia de subsistência e rentabilidade devido à eficácia e eficiência organizacional que atribui. Assim, por mais complexo que seja a sua implementação, ser distinguido com um certificado, pode ser uma mais-valia que distingue a organização das restantes.

Dando resposta a esta necessidade, a Norma ISO 9001:2015 vem definir « […] *a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement*. »

Por outro lado, são cada vez mais as empresas cujas áreas produtivas e administrativas dependem de sistemas informatizados fazendo com que os sistemas de informação e as

tecnologias de informação (TI) sejam mecanismos indispensáveis ao funcionamento e à gestão da organização.

Dada a sua importância é fundamental que exista uma preocupação relacionada com o controlo dos processos, a segurança dos ativos, a eficiência de toda atividade e a qualidade associada. Neste sentido a Norma ISO 27001:2013

> *specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.*

Perante a adoção destas duas normas, surge a relevância do papel da auditoria uma vez que todo o processo carece de auditorias internas e externas, com o foco na qualidade e na segurança da informação. Reveste ainda particular relevância, a detenção por uma entidade de um adequado sistema de controlo interno (SCI), existindo a convicção de que esta, estará em melhores condições de implementar os sistemas referidos.

Assim combinando as ISO mencionadas e o SCI, a organização pode potencializar a sua eficácia e sustentabilidade, uma vez que satisfaz necessidades das diversas partes interessadas.

1.2. Objeto e Objetivo

A presente investigação tem como objeto de estudo a adoção pelas organizações de duas ISO e os contributos quer da auditoria quer do controlo interno, tendo por base o caso de uma empresa de contabilidade a operar em Portugal.

O objetivo principal do presente trabalho é apresentar um estudo que evidencie o papel da profissão de auditoria e do controlo interno na adoção daquelas normas assim como as sinergias decorrentes do SCI com os requisitos das normas que regem os sistemas.

Assim sendo, as perguntas que compõem esta investigação são:

1. A auditoria e o controlo interno representam um papel importante na adoção das normas ISO?
2. Existem sinergias entre as componentes do controlo interno e as exigências das normas ISO adotadas?

De forma a dar resposta a estas perguntas, foram elaboradoras 7 hipóteses que têm como objetivo não só dar respostas às perguntas anteriormente referidas como demonstrar a importância que estes processos têm nas organizações. As hipóteses que se pretendem comprovar são as seguintes:

H1: De uma auditoria interna adequada resultam colaboradores preparados

H2: Da ausência de uma auditoria interna derivam colaboradores desconfortáveis

H3: A auditoria externa é vista como útil aos processos de implementação das ISO

H4: A implementação de sistemas de gestão de qualidade e segurança da informação aportam benefícios para as organizações

H5: Os processos de certificação garantem maior reconhecimento às empresas

H6: A adoção dos requisitos das normas ISO, contribuem para a robustez do controlo interno

H7: A auditoria é importante para todo o processo de implementação das ISO

1.3. Metodologia

A metodologia utilizada para o suporte empírico da presente dissertação foi o estudo de caso.

Inicialmente, foi realizada uma revisão teórica, com o objetivo de fazer uma apresentação da literatura associada à temática em questão, que demonstra diversas perspetivas e fundamentos teóricos de diferentes autores através de periódicos e não periódicos, revistas científicas e teses académicas.

De seguida, para dar resposta às questões de investigação a metodologia de investigação adotada foi a utilização de inquéritos por questionário, considerando-se uma forma eficaz e rigorosa de recolher e analisar os dados. Este irá debruçar-se sobre se as diversas áreas que compõem a empresa alvo de investigação, com o objetivo de obter uma visão mais alargada dos procedimentos aplicados. Assim sendo, os destinatários dos questionários serão os colaboradores que estiveram envolvidos no processo de adoção das ISO. De forma a garantir a integridade da informação, os questionários serão anónimos e as perguntas incluídas terão como principal objetivo responder às hipóteses colocadas, e consequentemente às questões. De forma a permitir a proteção dos dados da organização e

garantir que a informação é fiável, ou seja, não influenciada, a presente investigação irá adotar o nome Empresa X sempre que for feita qualquer referência à empresa objeto deste estudo.

1.4. Estrutura da dissertação

De forma cumprir com os objetivos propostos, esta dissertação encontra-se estruturada em 6 capítulos, sendo o primeiro a presente introdução e contextualização do estudo onde é apresentada a relevância do tema, o objetivo e objeto de estudo assim como a metodologia a adotar.

O segundo capítulo apresentará uma análise à revisão da literatura acerca da temática em questão, que se inicia com as auditorias realizadas no processo de implementação dos sistemas. Serão também alvo de apresentação, as duas normas ISO implementadas e quais os princípios que as regem e ainda as evoluções e conceitos quer da qualidade quer da segurança de informação, a sua importância no dia a dia para as organizações e quais os benefícios e limitações associadas aos dois sistemas. Por último, é fundamental que a empresa detenha um sistema de controlo interno eficaz. Para além desta necessidade, será possível observar semelhanças entre os princípios das normas e as componentes do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e a finalidade das mesmas. Desta forma são apresentadas sinergias entre as normas ISO, o COSO e o *Control Objectives for Information and Related Technologies (*COBIT).

No terceiro capítulo, apresentar-se-á a empresa que serviu de objeto de estudo fazendo-se referência ao organograma que compõe a empresa, aos diversos ramos de negócio em que atua, assim como as principais áreas geográficas onde se encontra.

A metodologia de investigação adotada para dar respostas às perguntas de investigação e hipóteses de estudo descrever-se-á no quarto capítulo, incluindo os métodos e técnicas utilizadas no estudo e a sua forma de recolha, a estrutura do inquérito e a descrição da amostra. Sendo a presente investigação, um estudo de caso será realizada uma pequena caracterização do mesmo.

No quinto capítulo, são apresentados os dados recolhidos nos inquéritos por questionário através de gráficos e tabelas de suporte que facilitam a posterior análise. Complementarmente será também apresentado o conjunto de melhorias identificadas através de uma inventariação dos procedimentos e políticas implementadas no âmbito deste processo.

Por fim, no sexto capítulo serão apresentadas as conclusões obtidas no estudo e a verificação ou negação das hipóteses formuladas, as limitações do estudo e as sugestões para futuras investigações.

2. Revisão da Literatura

2.1. Introdução à Auditoria

A auditoria tem vindo a sentir uma extrema pressão para evoluir e encontrar respostas a um meio empresarial cada vez mais complexo. Esta evolução deve-se à dimensão das organizações, aos diversos segmentos de negócio, e ao facto de estes serem suportados por complexos sistemas de informação e colaboradores altamente qualificados, pelo que a auditoria teve de acompanhar este processo de evolução e complexidade. (Carneiro, 2013).

O Tribunal de Contas de Portugal (1999, p.30), define auditoria como

> um exame ou verificação de uma dada matéria, tendente a analisar a conformidade da mesma com determinadas regras, normas ou objetivos, conduzido por uma pessoa idónea, tecnicamente preparada, realizado com observância de certos princípios, métodos e técnicas geralmente aceites, com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada.

Para Teixeira (2006, p.5), «O conceito de auditoria tem evoluído com o decurso do tempo, refletindo não só as mutações operadas no desenvolvimento das organizações e na ponderação dos interesses em jogo, mas também os objetivos cada vez mais vastos que lhe têm vindo a ser fixados.»

Para Marra e Franco (2001), os acontecimentos que marcaram a evolução da auditoria contabilística, foram os seguintes:

- Controlo dos gastos públicos;
- Aparecimento de grandes organizações internacionais;
- Complexidade dos negócios;
- Prática financeira impulsionadora do desenvolvimento da economia de mercado;
- Necessidade de informações contabilísticas verdadeiras;
- Complexidade dos sistemas contabilísticos;
- Desenvolvimento e implementação de sistemas de controlos internos

Estes acontecimentos, permitiram na perspetiva de Teixeira (2006) um maior envolvimento de pessoas nas organizações o que levou à divisão do trabalho, segregação de funções de posse dos bens e dos registos contabilísticos, criando, assim, novos controlos internos para proteger os bens, detetar e evitar fraudes.

Hoje em dia, são diversos os tipos de auditorias que existem, assim como os objetivos e áreas de aplicação. Segundo Gil (1999, p.23) a auditoria de qualidade assume «[…] dois subconjuntos, auditoria externa da qualidade (realizada pelos certificadores públicos da ISO 9000/auditores externos da qualidade) e auditoria interna da qualidade (realizada pelos auditores internos da qualidade).» Assim, o auditor interno representa um papel cooperativo enquanto que o externo tem a preocupação de avaliar a conformidade da empresa.

Tendo em conta o presente estudo ser focado nas normas de qualidade e segurança da informação, irá dar-se destaque quer às auditorias internas, quer às externas que decorreram para a adoção dos sistemas, incluindo os conceitos que as caracterizam, as funções e objetivos e os benefícios e limitações associados.

2.1.1. Auditoria Externa

2.1.1.1. Definições

De acordo com Gil (1999, p.21), a auditoria externa pode ser classificada como:

- Auditoria da segunda parte - realizada pelo comprador
- Auditoria da terceira parte – levada a cabo por entidades certificadoras

Estas auditorias de terceira parte, de acordo com Hammar (2015) « […] *occurs when a company has decided* […] *hire an independent company to perform an audit to verify that the company has succeeded in this endeavor.* » Assim sendo, um dos focos do presente estudo será a auditoria externa levada a cabo por entidades certificadoras.

Moller (2008, p.287) destaca o papel destas entidades certificadoras porque embora as «*[e]nterprises can then take the necessary steps to comply with standard, but to certify their compliance they must contract with a certified outside auditor, with skills in that standard, to attest to their compliance*. » Ou seja, mesmo que estejam a agir em conformidade, precisam de recorrer a auditores externos para obter a certificação e garantirem perante as partes interessadas que estão a operar de acordo com a legislação e assegurarem a sua posição no mercado.

Segundo Marques (2013, p.7), a auditoria externa «[…] é exercida por pessoas independentes à empresa debruçando-se sobre a conformidade das operações, avalia e baseia-se na auditoria interna e, se apropriado, no controlo interno.»

Se a empresa estiver de facto agir em conformidade, os auditores externos atribuem a certificação à empresa que comprova qualidade ao ambiente ou área auditada. A atuação do auditor externo, deve segundo Oliveira (2013, p.25) «[…] abranger todas as áreas da empresa em determinado período e deve promover a redução dos custos, tempo e esforços. Por meio das recomendações inovadoras deve aumentar a eficácia e trazer benefícios à entidade.»

No entanto a auditoria externa, é ainda muito vista como uma auditoria financeira cujo principal foco remete às demonstrações financeiras da empresa. Esta visão é contestada por Brito (2015, p.47):

> a profissão de auditor já não se resume a verificar as contas financeiras de uma determinada empresa, tendo passado a ser considerado como um consultor que ajuda no controlo interno, dando a sua opinião e recomendações, quer para a utilização interna da própria empresa como para o exterior servindo de ligação entre os vários sectores de atividade com o objetivo da sustentabilidade e continuidade da organização.

Esta visão é suportada pelo Instituto Português de Auditoria Interna (IPAI) (2008, p.5) ao afirmar que a contratação desta auditoria «[…] não visa exclusivamente comprar um parecer sobre a informação financeira, mas contrata-se a competência e idoneidade técnica, a capacidade de julgamento, a integridade dos profissionais e a elaboração de relatórios objetivos […]».

2.1.1.2. Funções e Objetivos

Na perspetiva do International Navigation Association (1999) as funções de um auditor externo podem diversificar-se em:

- Consultor que auxilia uma empresa no desenvolvimento das suas atividades;
- Atuar em nome de um cliente que deseja assegurar eficiência por parte dos seus prestadores de serviços;
- Como um organismo de certificação que contribui para a emissão de certificados.

Desta forma e de acordo com Marra e Franco (2001), para ser eficaz e merecedora de confiança, a performance do auditor precisa de ser executada por um profissional independente, de forma a não ser influenciado pela opinião de terceiros, não afetando desta forma as suas conclusões. Esta característica vai de encontro aos objetivos da auditoria externa que segundo Costa (2010), se centram na capacidade de expressar uma opinião por parte de um profissional competente e independente.

Para Oliveira (2013) os objetivos fundamentais passam por:

- Dar credibilidade às demonstrações financeiras junto não só dos seus utilizadores como também das demais partes interessadas;
- Conhecer os pontos fracos existentes ao nível do controlo interno das empresas auditadas;
- Exercer ação pedagógica e de controlo sobre a estrutura;
- Concluir se as demonstrações financeiras apresentam de forma verdadeira e apropriada a posição financeira da empresa.

2.1.1.3. Benefícios e Limitações

Uma das vantagens mais destacadas na auditoria externa é a independência. Ao ser realizada por uma entidade que não pertence à empresa auditada, obtém-se, uma maior objetividade relativamente à auditoria interna, devido a um maior distanciamento entre auditores e auditados. (Carneiro, 2004).

O facto de o acompanhamento ser intermitente, já que opera em várias organizações pode levar a uma vasta experiência, resultado de auditar numerosas entidades, mas a um menor entendimento de cada empresa auditada, uma vez que o seu foco não se destina apenas a uma (Morais & Martins, 2003). De seguida, a Tabela 2.1. resume os benefícios e limitações desta auditoria.

Tabela 2.1. Benefícios e Limitações da Auditoria Externa

Benefícios	Limitações
Conhecimento e experiência vinda do exterior, fornecem novas perspetivas	Envolve custos que podem ser elevados e que se destinam a membros exteriores
Maior credibilidade do funcionamento da empresa perante terceiros	Distanciamento entre os colaboradores e demais pertences à organização, que pode originar desconfiança e medo
É mantida uma relação estritamente profissional, evitando conflitos departamentais ou questões de superioridade	As atividades da empresa auditada podem não ser totalmente entendidas, levando a erros de julgamento
Sendo exterior à empresa, consegue ter uma melhor perspetiva do que pode ser melhorado	

Fonte: Adaptado de International Navigation Association (1999)

2.1.2. Auditoria Interna

2.1.2.1. Definições

A auditoria interna tem evoluído ao longo do tempo devido não só às novas exigências por parte da sociedade e dos mercados, mas também aos diversos riscos a que as organizações estão sujeitas. Para Morais e Martins (2013), esta evolução deve-se essencialmente às mudanças das entidades, ao desenvolvimento de novas tecnologias e às novas áreas de atuação.

Segundo o IPAI (2009, p.10), a auditoria interna pode ser definida como

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

Completando esta visão, Morais & Martins (2013, p.91), defendem que a auditoria interna pode ser definida como uma

> função continua, completa e independente, desenvolvida na entidade, por pessoal desta ou não, baseada na avaliação de risco, que verifica a existência, o cumprimento, a eficácia e a otimização dos controlos internos e dos processos de Governance, ajudando-a no cumprimento dos seus objetivos.

Para Attie (1992, p.26) é «[…] uma atividade necessária à organização e desenvolve-se a fim de seguir a gerência ativa, concedendo-lhe alternativas, como ferramenta de trabalho, de controle, assessoria e administração.»

Na perspetiva de Taborda (2015, p.15), a visão desta auditoria passa por uma «técnica de controlo de gestão que incide na análise, verificação e avaliação das atividades da entidade e da eficácia e conformidade do funcionamento de outras técnicas de controlo.»

A auditoria interna é também conhecida como *first-party audit* e é realizada por alguém de dentro da organização e que se foca em auditar um processo ou um conjunto de processos de forma a garantir que a mesma se encontra de acordo com as normas que deseja implementar. Para Hammar (2015), « *[t]his person can be an employee of the organization or someone hired by the organization to perform the internal audits, such as a consultant, but the important thing is that the person is acting on behalf of the company rather than a customer or certification body*. »

A cooperação entre os auditores internos e externos, é de elevada importância, pelo que segundo Silva (2013, p.16), devem estabelecer «[…] uma comunicação profissional franca e sem restrições, sobre os diversos aspetos do seu trabalho, visto que interessa a ambos otimizar os recursos existentes e a obter, uns dos outros, informação relevante que leve a um aumento da utilidade do seu trabalho face à entidade. »

2.1.2.2. Funções e Objetivos

Os auditores internos executam trabalhos de preparação para os processos de certificação inicial e subsequente, na procura continua de estratégias de melhoria. Estes atuam em cooperação com as áreas auditadas, com a exceção de situações em que o fator surpresa seja determinante para obter conclusões (Gil, 1999).

De acordo com Pinheiro (2008, p.28) a auditoria interna tem como objetivos:

- Analisar e avaliar a segurança, adequação e aplicação de todos os sistemas de controlo;

- Verificar o nível de concordância com as políticas estabelecidas, planos e legislação relevante;
- Determinar a eficácia com que os ativos estão salvaguardados;
- Verificar a exatidão e segurança da informação estratégica para a gestão;
- Analisar as operações do ponto de vista da economia, eficácia e eficiência.

Para que estes objetivos sejam alcançados, o auditor deve ser proactivo e transparente na relação com o auditado para que, na fase da implementação da recomendação, as áreas a melhorar estejam recetivas a ouvir e a aceitar o auditor interno, como um aliado na consecução dos objetivos (IPAI, 2008).

2.1.2.3. Benefícios e Limitações

É possível afirmar, face às definições aqui apresentadas, que uma organização que disponha de auditoria interna, usufrui de diversos benefícios.

O facto de o auditor interno estar no seio da organização permite a Silva (2013) afirmar que

> há uma maior atenção aos pormenores e uma fiscalização interna constante, fazendo com que os funcionários possam ter maior rigor no seu trabalho, evitando os erros, promovendo medidas corretivas nas diversas áreas de intervenção (contabilística, gestão), aumentado assim a credibilidade do Sistema de Controlo Interno e promovendo o alinhamento de todos os níveis da organização, descentralizando a gestão e dando autonomia no desempenho das diversas tarefas.

Segundo Furtado (2009) os benefícios podem resumir-se em:

- Fiscalização da eficiência dos controlos internos;
- Identificação das falhas na organização e nos controlos internos;
- Assegurar uma maior correção dos registos contabilísticos;
- Contribui para a obtenção de melhores informações sobre a situação da empresa;
- Garante maior atenção e rigor dos trabalhadores evitando erros e fraudes.

No entanto, e como na maioria das áreas, também existem limitações. Uma das limitações mais apontadas à auditoria interna é a independência. Segundo Marques (1997, p.60) «[a] independência […] é uma das questões fundamentais para o bom desempenho da função da auditoria e, consequentemente, para a utilidade do serviço prestado».

De acordo com Strategor (1993, p.340) «[…] a realização de uma avaliação estratégica pode ser externa ou interna» embora «[…] um analista externo independente estará mais à vontade para o fazer». Isto porque quando é realizada por auditores internos, estes são parte integrante da organização ao contrário dos auditores externos.

Esta questão de independência tem na perspetiva de Gil (1999), origem nos laços de amizade criados pelo próprio auditor interno com os demais funcionários, acabando por vezes, por gerar um menor rigor nos controlos. De forma a ultrapassar esta limitação, a administração e a auditoria interna devem unir esforços e ter em conta que as atividades da auditoria interna não tem como finalidade prejudicar ou danificar a imagem da empresa, mas sim identificar possíveis melhorias.

Os impedimentos causados pela independência, «[…] poderão incluir, mas não se limitam a conflitos de interesse pessoal, limitações de âmbito, restrições ao acesso de registos, pessoal, e ativos, e limitação de recursos, tais como financeiros.» (IPAI, 2009, p.19),

De seguida é apresentada a Tabela 2.2., que resume os benefícios e limitações aqui apresentados.

Tabela 2.2. Benefícios e Limitações da Auditoria Interna

Benefícios	Limitações
As falhas ou situações mais problemáticas são mantidas dentro da empresa	A informação pode ser distorcida ou omitida pela insegurança em criticar a própria empresa
Construção de conhecimento interno sobre os temas avaliados	As conclusões podem ser erradas porque são baseadas com menor conhecimento
A metodologia pode ser integrada em outras atividades de planeamento	Podem perder-se observações importantes por falta de experiência
Os custos e o conhecimento adquirido são mantidos dentro da organização	Podem não ter a devida atenção da gestão de topo

Fonte: Adaptado de International Navigation Association (1999)

2.2. Os sistemas de gestão, as normas ISO e as suas certificações

Neste subcapítulo, o objetivo é o de dar a conhecer o SGQ, o SGSI e as normas que permitem as certificações destes sistemas. Para isso, serão definidos conceitos assim como a relevância que a qualidade e a informação têm nas organizações, seguido da apresentação dos sistemas e dos princípios e requisitos que regem as normas. De forma a finalizar este subcapítulo, serão ainda demonstrados os benefícios e limitações inerentes aos sistemas. Relativamente ao SGSI, destaca-se ainda o papel que os sistemas de informação têm e a sua ligação ao COBIT.

Por último, descreve-se o processo de certificação e quais as fases que compõem o mesmo, e ainda uma análise da evolução dos certificados emitidos no mundo e em particular em Portugal.

2.2.1. Sistema de Gestão de Qualidade e ISO 9001

2.2.1.1. Evolução da qualidade

Durante a I Guerra Mundial, e como resultado das falhas dos equipamentos, surgiu a necessidade de criar uma função ligada à qualidade, que tinha como objetivo assegurar a conformidade dos equipamentos.

No entanto na II Guerra Mundial, foram identificadas falhas de controlo na conceção, originando especificações incompletas, derivadas da incorreta utilização de tecnologias e materiais, ou ainda desvios à normalidade dos processos. Estas falhas eram analisadas pelos inspetores que rapidamente concluíram que o facto de a análise ser feita produto a produto não era eficaz, pelo que depressa foi substituído pelas técnicas estatísticas de controlo de qualidade desenvolvidas por Walter Shewhart (António, Teixeira & Rosa, 2016).

Segundo Ribeiro (2012, p.10) tudo começou com o artesão «[…] que garantia a qualidade do produto, verificando e atuando para que não houvesse defeitos na cadeia de produção. Com o decorrer do tempo, surgiu o cargo de mestre que chefiava vários artesãos e que, posteriormente, deu lugar ao cargo de inspetor.»

Contudo este método não era o mais correto na perspetiva dos japoneses, porque os defeitos apenas eram detetados após a produção e não de forma a serem evitados. Assim a revolução da qualidade pode ser atribuída aos Union of Japanese Scientists and Engineers e aos estatísticos William Deming, Shewhart, Kaoru Ishikawa e Joseph M. Juran (Santana, 2014).

Para António, Teixeira & Rosa (2016, p.24) a evolução da qualidade possui dois marcos a considerar, sendo que «[o] primeiro desses marcos é o advento da produção em massa associado à Revolução Industrial (no século XIX) e o segundo, mais recente, respeita à importância crescente assumida pelo setor dos serviços.»

Pires (2007) afirma que a evolução dos conceitos, pode ser resumida pela sequência abaixo apresentada:

- Inspeção - atividade de medição, comparação, verificação;
- Controlo da qualidade - atividades que se centram na monitorização, nomeadamente na análise dos desvios e reposição dos parâmetros dos processos nas condições desejadas;
- Garantia da qualidade - atividades planeadas e sistemáticas que podem garantir que a qualidade desejada está a ser alcançada;
- Gestão da qualidade - atividades coincidentes com as da garantia, mas em que é enfatizada a integração na gestão global da empresa;
- Qualidade total - cultura de empresa capaz de assegurar a satisfação dos clientes.

O progresso da qualidade, está hoje presente em diversas indústrias, serviços privados e públicos e a diversificação continua à medida que os processos se tornam mais complexos, os consumidores mais exigentes e a competitividade maior. A escolha pela qualidade é cada vez mais uma questão de sobrevivência e destaque.

2.2.1.2. Conceitos e Relevância

A qualidade é definida por Cruz e Carvalho (1994, p.18) como sendo a «[…] conformidade em relação a especificações e parâmetros definidos, conhecidos por todos na empresa e estabelecidos pelos clientes, em permanente revisão para que se encontrem em cada momento dinamicamente ajustados às suas reais necessidades […]».

De acordo com Pires (2016, p.35) a qualidade «[…] começa com a identificação das necessidades e expetativas do consumidor […]».

É um processo dinâmico, de melhoria continua e sistemática, mas também uma forma de estar, agir e pensar. Na perspetiva de Cruz e Carvalho (1998, p.18), a qualidade deve ser observada em duas óticas a humanística e a empresarial, isto porque «qualquer processo de

qualidade total é, em si mesmo, um processo cultural […]». Ou seja, quando aplicamos a qualidade à vertente empresarial, deve ser tido em conta que o conceito qualidade tem por bases questões éticas.

Para Juran & Godfrey (1998, p.26) o termo qualidade significa « […] *freedom from deficiencies—freedom from errors that require doing work over again (rework) or that result in field failures, customer dissatisfaction, customer claims, and so on.* »

Está presente nos produtos e serviços prestados, nos sistemas, na organização, nos métodos, critérios e processos utilizados, nos recursos disponíveis e em como estes são utilizados e é transversal a todas as atividades e departamentos de uma empresa. Quanto mais clarificada e divulgada for a política de qualidade, mais fácil será alcançar os seus objetivos.

Na perspetiva de Pires (2016), a qualidade de um produto ou serviço está relacionada com:

- Satisfazer as necessidades e expectativas dos clientes;
- Ser disponibilizado nas condições e tempo desejado, a um preço que o cliente esteja disposto a pagar.

Segundo Santana (2014, p.7) «[a]s empresas e os serviços que não se pautarem por parâmetros de qualidade, não sobreviveram seja qual for o setor, a idade da empresa ou o local de operação.»

Assim sendo, a sua importância pode ser explicada através das condicionantes abaixo apresentadas na Figura 2.1.

Figura 2.1. Impulsionadores da importância da qualidade

Fonte: Elaboração Própria

De acordo com Pires (2004) & Wiendahl (2003) cada um dos setores acima observados podem ser explicados através de:

- Mercado – devido à concorrência sofisticada, globalização dos mercados, desenvolvimento tecnológico, customização dos produtos, segmentação do mercado;
- Acionistas e Outras Partes Interessadas – ao dar mais valor à organização e maiores expetativas dos empregos;
- Clientes – pelo preço, serviço e maior e melhor capacidade de resposta;
- Políticas e Sociais – devido às alterações demográficas e sociais, ao ambiente, saúde e segurança no trabalho e também à regulamentação existente.

Sampaio (2017) defende 25 mandamentos sobre aquilo que consideram ser o futuro da qualidade. De entre eles, destacam-se os seguintes:

- Deve ser alcançada com muito trabalho, sem considerar o sucesso como garantido;
- Ser capaz de antecipar as necessidades dos clientes, acionistas e empresas e contribuir para o seu crescimento;
- Explorar o desenvolvimento tecnológico, e torná-lo mais eficiente e útil;
- Abandonar a perspetiva de departamento, e tornar-se num sistema integrado e bem estruturado;
- Ser implementada em diferentes níveis, incluindo produtos, processos, sistemas, pessoas, organizações, serviços entre outros;
- Ficará fortemente ligada à cultura organizacional e social e ao sucesso alcançado.

De acordo com Sampaio (2017, p.24), o futuro da qualidade « […] *should be continuously understood, assimilated and implemented, both in public and private organizations. However, each one of us is responsible to push and pull quality forward, always doing more and better.* »

É imperativo para as empresas, entenderem que se encontram em constante mudança e serem capazes de seguir as tendências que se impõem. Estas devem ser entendidas como novas oportunidades e implementadas consoante a capacidade organizacional de cada uma.

2.2.1.3. Sistema Gestão Qualidade e as fases de implementação

De acordo com Pires (2016, p.49), o sistema da qualidade pode ser definido como o «[…] conjunto das medidas organizacionais capazes de transmitirem a máxima confiança de que um determinado nível de qualidade aceitável está [a ser] alcançado ao mínimo custo.»

Para Santana (2014, p.19) o SGQ é influenciado pelo «[…] ambiente em que a organização opera, mudanças e riscos associados a esse ambiente, necessidades várias, objetivos particulares, bem como pelos produtos que fornece, processos utilizados, dimensão e estrutura da organização.» Assim sendo deve ser amplo e ajustável às alterações do mercado, contando que os meios humanos e organizacionais operem para um mesmo final.

Para que a sua implementação tenha sucesso, a empresa deve segundo a Associação Portuguesa de Certificação (APCER) (2010), assegurar que estão definidos os critérios e métodos que assegurem quer a operação quer o controlo dos processos, certificar-se que existem recursos e informação para suportar a operação e monitorização dos mesmos e por fim desenvolver ações para atingir os resultados delineados e alcançar a melhoria continua.

De acordo com o Instituto Português de Qualidade (IPQ) (2015, p.7), «[a] adoção de um sistema de gestão da qualidade é uma decisão estratégica de uma organização que pode ajudar a melhorar o seu desempenho global e proporcionar uma base sólida para iniciativas de desenvolvimento sustentável.»

Contudo para Fernandes (2016, p.1) o SGQ é benéfico, mas «[…] não vai por si só, resolver os problemas de uma organização, mas pode aumentar significativamente as hipóteses de identificação e eliminação de causas do erro e desperdício, e daí a melhoria de processos e informações.»

Um dos maiores pilares do SGQ é o ciclo *Plan-Do-Check-Action* (PDCA). Segundo Ribeiro (2012, p.17) o ciclo da qualidade deve «[…] otimizar a realização dos processos, possibilitar a redução de custos e o aumento da produtividade levando ao aperfeiçoamento e ajustamento do sistema de gestão da qualidade da organização.»

Este ciclo, é uma ferramenta que pode ser utilizada de diversas formas e que se tornou conhecida pela sua enorme utilização em processos de controlo de qualidade, dado que é cíclica, objetiva e promove a melhoria de processos estando incorporada na estrutura das normas ISO. Utiliza, para isso, 4 fases: *plan, do, check e act*. Se for utilizada corretamente, acarreta grandes benefícios para a organização, não apenas na manutenção e melhoria de

processos, como também financeiramente (APCER, 2015). Este ciclo é apresentado na Figura 2.2.

Figura 2.2. Ciclo PDCA

Fonte: Quality Management System (2018)

Relativamente às fases de implementação de um SGQ, estas são iguais para todas as organizações, no entanto, devem ser adaptadas à dimensão, atividade, recursos disponíveis, envolvimento das pessoas, entre outros fatores.

Fernandes (2016) apresenta 10 fases de implementação do sistema, compiladas através da consulta da ISO 9001 e de autores como Hernad & Gaya (2013), Hammar (s.d.) e Pinto (s.d.). Estas fases podem ser descritas como:

1. Suporte da gestão de topo - a ideia de iniciar este processo deve partir da gestão de topo e o seu suporte deve ser eficaz perante os restantes colaboradores.

2. Conhecimento dos colaboradores - o envolvimento destes é considerado essencial, uma vez que são eles quem desenvolvem no dia a dia a atividade da organização. Assim, a gestão deve apostar na sua formação.

3. Diagnóstico - esta fase serve essencialmente para analisar quais os processos e documentos que já se encontram de acordo com a norma, quais os que são necessários modificar e quais os que ainda são necessários implementar.

4. Definir o âmbito, objetivos e política de qualidade - estas ações tornam o processo mais claro e objetivo uma vez que representam o compromisso da organização com a qualidade e a respetiva implementação.

5. Definir a documentação de apoio e processos - a documentação selecionada deve auxiliar a organização na implementação da gestão da qualidade e fornecer as indicações necessárias para o adequado funcionamento.

6. Implementação da documentação e processo - após a sua definição, segue-se a implementação, que pode suscitar as maiores dificuldades, quer na compreensão das medidas quer na aceitação da mudança.

7. Auditorias internas- o SGQ é avaliado com o objetivo de ver se está de acordo com a norma e com a documentação definida pela organização. Se das auditorias resultarem não conformidades, deverão ser analisadas e definidas ações corretivas.

8. Revisão pela gestão - esta revisão deve focar-se no resultado das não conformidades, das auditorias internas, dos inquéritos de satisfação dos clientes e do desempenho dos processos entre outros.

9. Auditoria de concessão - é realizada por uma entidade certificada em que os auditores verificam se foram implementados os requisitos da norma, emitindo um relatório onde são apresentadas as conformidades e as não conformidades, de modo a que a organização realize ações corretivas. De seguida, ocorre nova verificação, de forma a concluir se as ações implementadas corrigiram as não conformidades. Quando é conseguida a certificação, são realizadas auditorias de acompanhamento e passados 3 anos tem de ser feita a renovação do certificado.

10. Melhoria Contínua - a procura pelas oportunidades de melhoria e novas ações a implementar, deve continuar após a obtenção da certificação, de forma a que os objetivos do SGQ sejam continuamente alcançados.

2.2.1.4. Apresentação da Norma, os seus princípios e requisitos

A ISO foi fundada em 1947 como uma federação sem fins lucrativos dos organismos nacionais de normalização com sede em Genebra. As normas publicadas por este organismo, debruçam-se sobre diversos temas que vão desde a tecnologia, à segurança alimentar, à agricultura, à saúde ou qualidade e tem por base consensos internacionais entre grupos de peritos reconhecidos e nomeados pelos seus respetivos organismos membros. Entre estes membros estão por exemplo o IPQ em Portugal, o American National Standards Institute nos Estados Unidos, a Associação Brasileira de Normas Técnicas no Brasil, a Asociación Española de Normalización y Certificación, a British Standards Institution (BSI) no Reino Unido, entre outros.

De acordo com APCER (2015, p. 24), «[a] missão generalizada da ISO é facilitar o comércio mundial promovendo a harmonização global.» Ao facilitar o comércio, é também facilitada a troca de bens e serviços a nível internacional e a cooperação a nível intelectual, científica, tecnológica e económica.

Em 1987, foram divulgadas as normas da família ISO 9000 definindo um conjunto de boas práticas de gestão que se tornam uma referência na implementação de um SGQ. Esta família é composta por quatro normas essenciais que são sustentadas por um elevado número de normas de suporte e de documentos orientadores

A norma ISO 9001 foi submetida a quatro revisões desde então, em 1994, 2000, 2008 e a mais recente, na qual é focada este estudo, a publicada em 2015. Estas revisões originaram uma forte evolução da norma, dado que em 1987, a preocupação centrava-se na garantia de qualidade, e desde então, tem sofrido diversas alterações no que toca a processos, enfâse do cliente, melhoria continua até à norma que hoje se encontra em vigor.

No entanto, para Lopes & Capricho (2007, p.40), «[…] apesar das normas da série 9000 não garantirem a qualidade do produto ou serviço, elas especificam os critérios para a obter, sendo obrigatória para as empresas ou outras organizações que pretendam certificar os seus sistemas.»

Relativamente à ISO 9001:2015, é composta por 7 princípios e segundo a ISO (2015, p.1) os princípios são importantes porque definem "*a set of fundamental beliefs, norms, rules and values that are accepted as true and can be used as a basis for quality management*."

De acordo com Perdigão (2016), estes princípios refletem o senso comum e o pensamento de muitos especialistas da qualidade e são essenciais à orientação de boas práticas de gestão de qualidade numa organização.

A ISO em 2015, elaborou um manual onde constam os 7 princípios definidos pela norma ISO 9001:2015, em que por cada um é apresentada a razão pelo qual existem e quais os seus fundamentos, assim como os benefícios e as ações que a organização pode realizar para que os mesmos sejam atingidos. A APCER no mesmo ano, elaborou um guia de implementação que vem auxiliar as empresas a compreender melhor o funcionamento desta norma e que complementa o manual da ISO. Os princípios podem ser observados na Figura 2.2., seguida das razões, os benefícios e as ações a realizar por cada um dos princípios.

Figura 2.3. Princípios da ISO 9001:2015

Fonte: APCER (2015, p.38)

- Foco no Cliente

Razão: A preocupação principal na gestão da qualidade é atender às necessidades dos clientes e exceder as suas expetativas e o sucesso é alcançado quando a organização consegue atrair e reter clientes e outras partes interessadas.
Benefícios: Maior a satisfação e lealdade do cliente, renovação de negócios, maior número de clientes alcançados, maior receita e participação no mercado.
Ações a realizar: Entender as necessidades atuais e futuras dos clientes, comunicar as necessidades e expetativas a toda a organização, para que em conjunto consigam planear,

desenvolver e entregar bens/produtos adequados, medir o grau de satisfação para o caso de ser possível melhorá-lo e cultivar as relações com tais clientes.

- Liderança

Razão: Os líderes devem estabelecer prepósitos e direções e criar condições nas quais as pessoas fiquem motivadas a alcançar os objetivos de qualidade de acordo com as políticas, processos e recursos da organização.
Benefícios: melhor comunicação entre os diversos departamentos e níveis hierárquicos, maior eficácia em atingir os objetivos e melhor coordenação dos processos.
Ações a realizar: partilhar a missão, visão, estratégia e políticas da organização, implementar uma cultura de confiança e integridade e incentivo por parte de todos, garantir que todos os líderes são um exemplo a seguir e fornecer às pessoas os recursos necessários, formação e autoridade para agirem em conformidade.

- Compromisso das pessoas

Razão: Se as pessoas forem competentes, capacitadas e estiverem envolvidas em todos os níveis, maior será a capacidade de criar valor. Para isto, é importante que sejam reconhecidas, respeitadas e encorajadas a atingir os objetivos.
Benefícios: Maior envolvimento e confiança, melhoria na compreensão dos objetivos e motivação para alcançá-los, maior partilha de valores e cultura em toda a organização.
Ações a realizar: Reconhecer a contribuição, melhoria e aprendizagem de cada um, promover discussões abertas e a partilha de conhecimento e experiência, realizar pesquisas que permitam avaliar a satisfação assim como autoavaliações.

- Abordagem por processos

Razão: Os resultados consistentes e previsíveis são atingidos de modo mais eficaz e eficiente quando as atividades são compreendidas e geridas como processos inter-relacionados que funcionam como um sistema coerente. Quando a organização compreende que os resultados são obtidos através dos processos, pode otimizar o seu SGQ e consequentemente melhorar

o seu desempenho. A melhoria da interação entre processos, garante que cada um recebe as entradas necessárias para a sua eficácia e que entrega as saídas pretendidas.
Benefícios: Uso eficiente de recursos, concentração de esforços nos principais processos e eficácia e eficiência perante terceiros.
Ações a realizar: Garantir que as informações necessárias estão disponíveis, operar e melhorar os processos, definir os objetivos dos sistemas e quais os processos para alcançá-los e estabelecer autoridade e responsabilidade para os gerir.

- Melhoria contínua

Razão: As organizações de sucesso estão sempre focadas na melhoria continua. Isto porque a melhoria permite reagir às mudanças internas e externas e criar oportunidades.
Benefícios: Maior capacidade para antever riscos e oportunidades, melhor desempenho do processo e satisfação do cliente e maior conhecimento sobre melhorias
Ações a realizar: Reconhecer as melhorias, acompanhar e rever o planeamento, implementação e conclusão de resultados, desenvolver processos que permitam a melhoria continua.

- Tomada de decisão baseada em evidências

Razão: Confere maior número de resultados desejados. A tomada de decisão pode ser complexa, pelo que as evidências constatadas levam a uma maior objetividade e confiança na tomada de decisões.
Benefícios: Melhoria na tomada de decisões, maior eficácia operacional assim como melhoria da capacidade de avaliar as decisões tomadas.
Ações a realizar: Garantir que as pessoas são competentes para analisar e avaliar dados, assim como os dados e informações são precisos, confiáveis e disponibilizados a quem deles precisa.

- Gestão das relações

Razão: O desempenho de uma organização está fortemente dependente de como as partes interessadas se relacionam com a mesma. Se as relações forem geridas e adequadas, mais benéfico será o seu impacto no decorrer das suas atividades.
Benefícios: Maior capacidade em criar valor através da partilha de recursos, competências e gerenciamento de riscos, melhoria da comunicação e do desempenho através da resposta às oportunidades e restrições de cada parte interessada.
Ações a realizar: Definir quem são as partes interessadas relevantes entre fornecedores, clientes, investidores, colaboradores entre outros, partilhar informações, conhecimentos e recursos, medir o desempenho e reconhecê-lo e melhorar as atividades pelas quais se relacionam.

Tal como a ISO 9001:2015, a ISO 27001:2013, apresenta um conjunto de 7 requisitos. Cada princípio deve ser analisado e estudado para que seja atingido o sucesso na implementação da norma que cada organização deseja. Na Figura 2. são apresentados os 7 requisitos e o que se depreende para cada um, sendo possível observar que os mesmos estão direcionados para o SGQ, no entanto e sendo iguais para ambas as normas, a única diferença reside para o facto da ISO 27001 abordar o SGSI e não o SGQ.

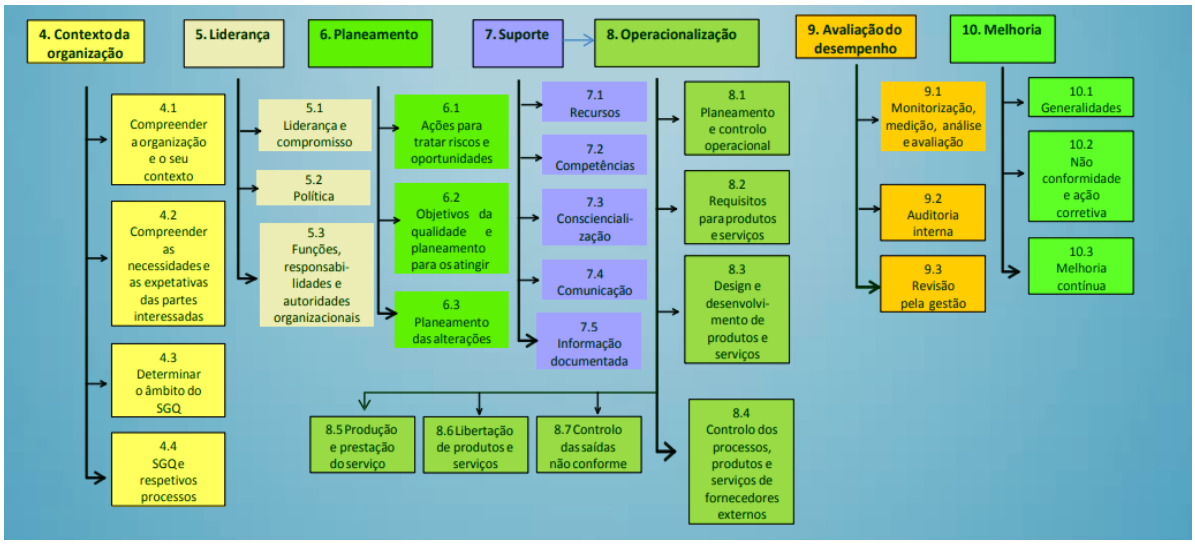


Figura 2.4. Requisitos do SGQ e do SGSI

Fonte: Adaptado de Fonseca (2016)

Os requisitos da norma, juntamente com o ciclo PDCA compõem o funcionamento do SGQ. O processo que se inicia com identificação das necessidades do cliente e que termina com a satisfação das mesmas originando produtos e serviços, pode ser demonstrado de seguida na Figura 2.5.

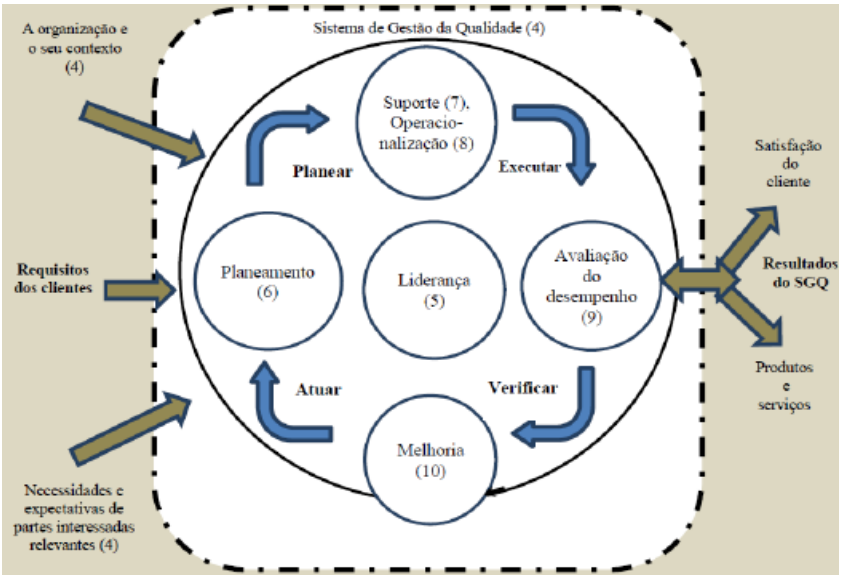


Figura 2.5. Funcionamento do SGQ

Fonte: ISO 9001:2015 (2015)

2.2.1.5. Benefícios e limitações na adoção de um Sistema de Gestão de Qualidade

A implementação deste sistema para além de ser importante e uma forma de responder às exigências das diversas partes, oferece também muitos benefícios ao funcionamento da empresa. Segundo a ISO (2015), estes benefícios podem ser:

- Maior satisfação do cliente;
- Melhoria da qualidade de produtos e serviços;
- Satisfação dos trabalhadores e mais compromisso com a organização;
- Melhor gestão e uma organização mais eficiente;
- Melhoramento das relações com os fornecedores e expansão para novos mercados;
- Identificação e resolução dos riscos associados à organização.

As organizações devem refletir, sobre os benefícios e motivações que as levam à implementação da norma. Para Sampaio (2008), na maioria das organizações não se encontra presente apenas um tipo de motivação, mas sim uma mistura de ambas. Ou seja, motivações internas e externas que por sua vez originam benefícios internos e externos. Estes benefícios, são de seguida apresentados na perspetiva do mesmo autor na Tabela 2.3.

Tabela 2.3. Benefícios Externos e Internos resultantes da ISO 9001

Benefícios Externos	Benefícios Internos
Acesso a novos mercados	Aumentos de produtividade
Melhoria da imagem da empresa	Diminuição da percentagem de produtos não conformes
Aumento da quota de mercado	Maior consciencialização para o conceito da qualidade
Ferramenta de marketing	Clarificação de responsabilidades e obrigações
Melhoria da relação com os clientes	Melhorias a nível dos tempos de entrega
Aumento da satisfação dos clientes	Melhorias organizacionais internas
Melhoria na comunicação com o cliente	Diminuição das não conformidades
	Diminuição do número de reclamações
	Melhorias na comunicação interna
	Melhorias na qualidade dos produtos
	Vantagens competitivas
	Motivação dos colaboradores
	Diminuição dos níveis de sucata

Fonte: Sampaio (2008, p.37)

No entanto, verificam-se também diversas limitações aquando a implementação do SGQ. Para Santana (2014) estas podem ser:

- Escassez de recursos humanos, que podem ter qualificações reduzidas ou falta de formação na área;

- Instalações e equipamentos antigos, que por não cumprirem a legislação necessitam de investimento;
- Investimento inicial requerido;
- Meio envolvente, de forma a consciencializar toda a organização da necessidade de mudança;
- Custos de implementação e manutenção do sistema de gestão da qualidade significativamente elevados

Os custos são em regra geral, uma das maiores condicionantes ao processo. No entanto, Casadésus et al (2004 citado em Sampaio, 2008) defende que ao longo do tempo, com o processo já estabelecido, verifica-se uma redução dos custos e um aumento dos benefícios.

2.2.2. Sistema de Gestão de Segurança da Informação e ISO 27001

2.2.2.1. Conceitos e Importância da Informação

A informação pode ser entendida como um conjunto de dados dotados de relevância e com um objetivo (Druker, 1993).

Para Zorrinho (1991), a informação é vista como um fator de sucesso nos mercados altamente concorrenciais. O mesmo autor defende ainda, que a informação é considerada e utilizada em muitas organizações como um fator estruturante.

Segundo Rivas (1989, p.85) a informação pode ser descrita como «[…] tudo quanto nos reduza à incerteza, permitindo-nos assim escolher e atuar de tal forma que as nossas organizações tenham possibilidades de sobreviver e prosseguir os seus planos.» Esta inclui tudo o que diz respeito a clientes, serviços ou produtos, fornecedores e todos os demais que estejam relacionados com o negócio.

Importa compreender que a informação pode assumir diferentes significados, em diferentes meios e circunstâncias devido aos objetivos que são tidos em conta assim como as necessidades sentidas e a sua importância, sendo diferentes de organização para organização.

A classificação da informação é um dos primeiros passos para a implementação de uma política de segurança da informação. Assim sendo, devem ser respeitadas todas as características e critérios que assegurem confiança e eficiência na forma como é utilizada.

Segundo Marques (1997) a informação reúne 3 características principais, ser adequada, de qualidade e oportuna. Adequada no sentido de ir de encontro ao sector de atividade, negócio ou posto de trabalho, ser de qualidade, ou seja, objetiva, precisa, fiável e rentável e por último ser oportuna, estando disponível em tempo útil e permitindo obter resultados vantajosos.

A Figura 2.6. apresenta as 3 principais características associadas à informação.

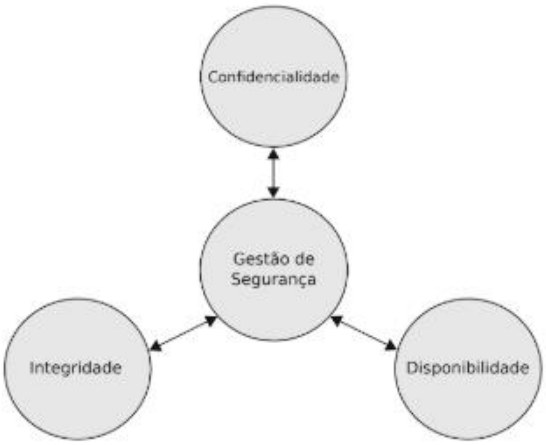


Figura 2.6. Caracteristicas da Informação

Fonte: Hintzbergen, J., Hintzbergen, K., Smulders, A. & Baars, H. (2010, p,21)

A confidencialidade pode ser posta em causa, segundo Correia (2016, p.16) por «[…] razões técnicas ou organizacionais: mecanismos de controlo de acesso insuficientes, transmissão de informação não cifrada pela rede, partilha de senhas entre utilizadores, definição desadequada de privilégios dos utilizadores, falta de cuidado no manuseio da informação, etc.» Esta característica deve ser aplicada a cada elemento de processamento de dados e impede que os mesmos sejam divulgados sem a devida autorização (Hintzbergen, J. et al 2010).

Já a indisponibilidade pode ocorrer devido a avarias nos equipamentos ou no ambiente onde operam como falhas de energia, de aplicações, erros no manuseamento do sistema, ataques intencionais, causas naturais como incêndios ou inundações e ainda insuficiência de recursos Correia (2016).

Relativamente à integridade, é importante que a informação a circular ou armazenada seja a mesma aquando a sua criação, sem que haja interferência externa para comprometê-la ou danificá-la. Assim esta característica corresponde à preservação, à consistência e

confiabilidade das informações e sistemas. A perda de integridade pode originar falhas na execução de atividades, na comunicação entre departamentos e a incapacidade de alcançar certos objetivos.

Para Casaca (2010), existem outros conceitos associados à segurança da informação que estão relacionados com a utilização da Internet e que podem ser:

- Autenticação – assegurar que o utilizador é quem afirma ser;
- Não-repudiação – assegurar que o utilizador não pode negar posteriormente a não realização de determinada atividade;
- Responsabilidade - estipular as responsabilidades e papéis dos utilizadores.

Sendo a informação um ativo tão importante, a empresa deve ser capaz de identificar a sua importância, de forma a garantir que esta chega a todos os envolvidos, com o objetivo de aumentar a eficiência e eficácia do seu tratamento, otimizando o negócio. A importância da informação é reforçada em Druker (1993, p.189) ao afirmar que «[…] a informação serve de eixo e como estrutura central de apoio […]».

Na perspetiva de Vasudevan, V., et al (2015, p.11), *«[i]t is a truism to say that information is the currency of the information age. Information is, in many cases, the most valuable asset possessed by an organisation, even if that information has not been subject to a formal and comprehensive valuation.* »

2.2.2.2 Segurança da Informação

Para Martins (2007, p.21), a informação «[…] seja a forma que adote, ou o meio pelo qual é partilhada ou armazenada, deve ser sempre devidamente protegida […]» dada a sua importância.

Segundo Hintzbergen, J., et al (2010, p,16) a segurança da informação é «[…] a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e oportunidades de negócio».

No entanto, as organizações têm sofrido diversas perdas dado que os seus sistemas de informação e de comunicação estão expostos diariamente, a diversos tipos de ameaças à

segurança da informação, como espionagem, sabotagem, vandalismo, incêndios, inundações, danos causados por códigos maliciosos, hackers entre outros.

Na perspetiva de Oliveira (2015, p.19), os riscos enfrentados prendem-se com a «[…] crescente nível e complexidade, da sua utilização, das tecnologias utilizadas e ligação a redes externas cada vez mais sofisticadas».

Na Figura 2.7. abaixo apresentada, é possível observar várias ameaças que podem ocorrer que originam graves consequências para as empresas e quais os impactos que as mesmas têm no negócio.

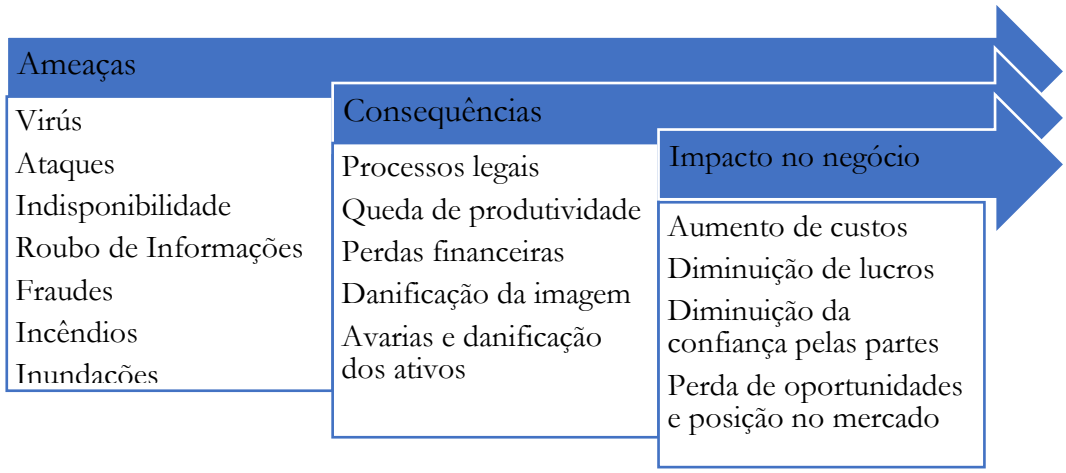


Figura 2.7. Consequências e impacto no negócio resultantes das ameaças à informação

Fonte: Adaptado de Ferreira (2009)

As ameaças referidas anteriormente deve ser identificadas e então definir quais os controlos a aplicar para que a informação esteja efetivamente em segurança. A Figura 2.8. resume as ameaças físicas e quais os controlos que podem ser acionados, enquanto que a Figura 2.9. identifica as ameaças ambientais e os respetivos controlos.

Ameaças Físicas	Controlos
Roubos	Delimitação de acessos e utilização de passwords
Danos Físicos	Cofres
Cópias e divulgações não autorizadas	Cadeados
Terrorismo	Firewalls eficientes

Figura 2.8. Ameaças físicas e Controlos associados

Fonte: Elaboração Própria

Ameaças Ambientais	Controlos
Incêndios	Detetores de fumo
Inundações	Detetores de água
Falhas de energia	Sistemas de energia e refrigeração

Figura 2.9. Ameaças ambientais e Controlos associados

Fonte: Elaboração Própria

Estes controlos devem ser combinados com a implementação de políticas, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Na perspetiva de Sequesseque (2017, p.22), «[a] informação deve ser mantida em segurança, assim como o ambiente e os equipamentos utilizados para o seu processamento.»

É fundamental ainda, que exista um elevado controlo na forma em como a informação é documentada e quais os controlos que tal documentação exige. Vasudevan, V., et al (2015, p. 29) apresentam um conjunto de 5 atividades relacionadas com esta temática que se definem como:

- *How the information will be distributed, accessed, retrieved and used;*
- *How the information is to be stored and preserved, including preserving legibility;*
- *How changes are controlled;*
- *Rules governing how the information is retained and disposed of;*
- *Information of external origin must be appropriately identified and controlled.*

2.2.2.3. Sistemas de Informação

Atualmente, grande parte das empresas têm as suas áreas produtivas e administrativas de tal forma informatizadas que tornam os sistemas de informação, bem como as tecnologias de informação, instrumentos imprescindíveis (Carneiro, 2016).

A generalidade da informação é armazenada nos *softwares* e *hardwares*, pelo que importa garantir que os sistemas de informação funcionam corretamente de modo a preservar a informação neles contida. Para Kosutic (2016, p.1) a relação entre a informação e os sistemas de informação tem relevancia porque a « […] *information security, cybersecurity, or data protection are not the things that are reserved any more for IT geeks only – this is something that concerns virtually any person on this planet, as well as any company*. »

É também possível justificar a importância dos sistemas pelo facto de quer os computadores, quer as redes serem suscetíveis de avarias ou danos e também pelo facto de os dados processados e programas utilizados poderem ser acessíveis e modificados sem deixar evidencias, por isso, as organizações que deles dependem, devem planificar eventuais emergências, levando com seriedade os aspetos técnicos dos mesmos.

A evolução das tecnologias tem criado novas possibilidades, mas também novas necessidades junto das demais organizações que delas dependem. Desta forma, toda a organização tem que estar apta a entender as novas tecnologias e em como estas podem mudar a forma como se trabalha. De acordo com Oliveira (2006) existem 10 controlos gerais que podem ser testados para conferir a fiabilidade dos sistemas de informação. Estes controlos gerais são a base para as operações informatizadas da empresa, sendo eles:

- Gestão dos sistemas de informação
- Planeamento e gestão do programa de segurança de toda a entidade

- Controlo de acessos
- Segurança física
- Seleção e implementação de aplicações informáticas
- Desenvolvimento e alteração das aplicações informáticas
- *Software* de sistema
- Segregação de funções
- Continuidade do serviço
- Internet

Dos controlos acima referidos, destacam-se os seguintes:

Controlo de acessos – consiste em permitir ou negar a utilização de recursos informatizados tais como dados, programas, equipamentos e instalações por indivíduos que podem modificar, perder ou danificar a informação. Embora não elimine totalmente os riscos à segurança da informação, diminui a ocorrência de incidentes. As regras de acesso devem ser pensadas, de acordo com o nível de segurança que a informação exigir assim como as responsabilidades de cada usuário. Os objetivos do controlo de acessos passam por:

- Garantir que o número de utilizadores com acessos é reduzido, justificado e que as listas de autorização estão atualizadas;
- A criação de senhas com determinadas características (número de caracteres, tipo de caracteres e tempo de validade) dificultando o acesso a pessoas não autorizadas;
- As passwords serem únicas por colaborador e a inserção de passwords incorretas é limitada;
- Após um determinado tempo, sem exercer qualquer tipo de função, o computador é suspenso automaticamente.

Segurança física - é também essencial que esteja assegurada a segurança das instalações, equipamentos, *softwares* e todos os ativos que conservem a informação da organização, contra as ameaças exteriores. Como objetivos é possível destacar:

- Os colaboradores terem consciência da localização dos alarmes de incidência, extintores, aparelhos de respiração entre outros;

- Existirem políticas que proíbam certos comportamentos dentro da organização como fumar, beber ou comer uma vez que podem danificar por exemplo faturas, computadores entre outros documentos e equipamentos.

Continuidade do serviço - quando ocorrem eventos inesperados, a informação critica, deve manter-se protegida de forma a dar continuidade ao negócio da organização. Os objetivos passam por:

- Os recursos que suportam as operações fundamentais são conhecidos e protegidos
- São criados frequentemente backups que contem a informação que permite a continuação. As instalações onde são mantidos os backups, estão devidamente protegidas quer em termos de condições físicas e de pessoas

Internet - o acesso à Internet deve ser monitorizado de forma a garantir que a utilização da mesma tem como finalidade atingir os objetivos de negócio assim como os possíveis riscos que tal serviço acarreta. Os objetivos são:

- Os firewalls e anti-vírus estão configurados e atualizados para proteger os acessos à internet e à informação;
- O email de cada colaborador tem definido uma estrutura própria e comum a toda a organização de modo a garantir uniformidade;
- A informação recolhida do portal da empresa como o contacto de clientes, é acedido através de acessos únicos por trabalhador, ficando registada a hora de acesso e tendo por base as necessidades da organização.

2.2.2.4. COBIT

A *framework* COBIT foi desenvolvida em 1996 pelo *Information Systems Audit and Control Foundation's*, devido ao reconhecimento da importância da governação em TI.

Para Bailey & Becker (2014, p.2), o COBIT é « […] *an IT governance control framework that helps organizations address the areas of regulatory compliance, risk management and aligning IT strategy with organizational goals.* »

Já Moeller (2008, p.119), defende que « […] *is an important internal control framework that can stand by itself but is an important support tool for documenting and understanding COSO and Sarbanes-Oxley (SOX) internal controls.* »

A importância do COBIT numa organização pode ser demonstrada pelos princípios básicos apresentados de seguida na Figura 2.10.

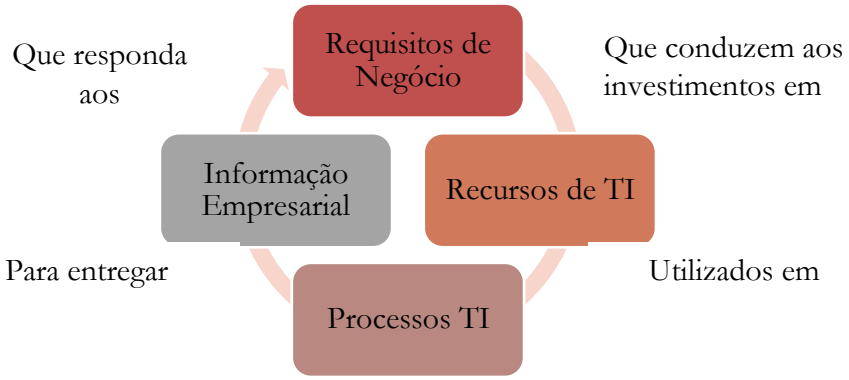


Figura 2.10. Princípios básicos do COBIT

Fonte: Adotado de ISACA

Já a sua importância no que respeita à segurança da informação, Sheikhpour (2012, p.17) afirma que

> *effective information security requires a comprehensive, integrated set of security, management and governance processes to plan, organize and counter the organizations information security risks. COBIT provides an integrated governance, management and process framework to implement and execute information security.*

Segundo Morais e Martins (2013), o COBIT apresenta uma estrutura semelhante à do COSO e, embora esteja mais focado para ambientes tecnológicos, adotou o conceito de controlo interno desenvolvido pelo COSO. A sua composição inclui 4 domínios, sendo eles planear e organizar, adquirir e implementar, entregar e suportar e por último monitorizar e avaliar. O domínio entregar e suportar compreende 13 tipos sendo que o DS5 - Processo de Segurança dos Sistemas contém diversos objetivos que vão de encontro aos requisitos da ISO 27001 (Sheikhpour, 2012).

Para Rodrigues (2014) estes objetivos incluem gestão da segurança de TI, plano de segurança de TI, gestão de identidade, gestão das contas de usuário, teste de segurança, vigilância e monitoramento, definição de incidentes de segurança, proteção da tecnologia de segurança, gestão de chaves criptográficas, prevenção, deteção e correção de *software*, segurança de rede, comunicação de dados confidenciais entre outros.

2.2.2.5. Sistemas de Gestão de Segurança da Informação

Segundo Martins (2007, p.31) o SGSI, é «[…] uma parte do sistema global de gestão, baseado numa abordagem de risco, que permite definir, implementar, operacionalizar, monitorizar, manter e melhorar a segurança da informação segundo a norma.»

Na perspetiva de Vasudevan, V., et al (2015, p.19), o SGSI é apresentado como « […] *structured, coherent management approach to information security which is designed to ensure the effective interaction of the three key components of implementing an information security policy: process, technology and user behaviour.* »

A implementação de um SGSI, resulta de decisões estratégicas, sendo que as necessidades e objetivos da organização, os requisitos de segurança, os processos organizacionais utilizados, a dimensão e estrutura da organização, constituem fatores influenciadores IPQ (2013).

O modelo PDCA, tem também um papel importante na implementação de um SGSI dado que estabelece, implementa, mantem e melhora de forma continuada os processos a ele associados. A explicação do funcionamento deste modelo, foi já anteriormente abordada no SGQ e pode ser aplicado ao SGSI como se pode observar de seguida na Figura 2.11.

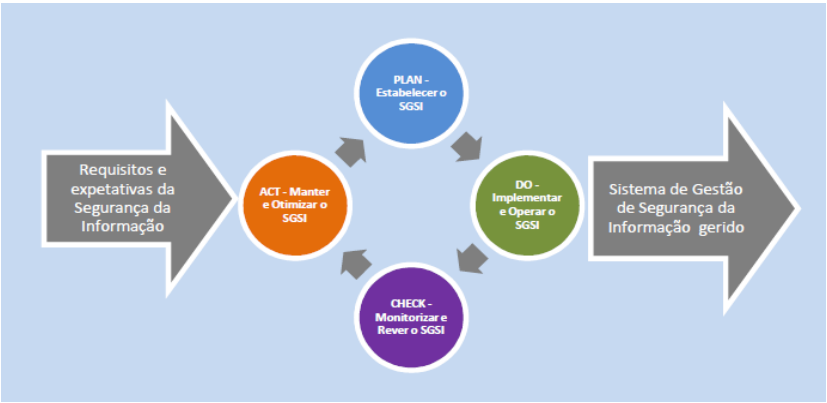


Figura 2.11. Ciclo PDCA aplicado ao SGSI

Fonte: Correia (2016, p.19)

2.2.2.6. Apresentação da Norma, os seus princípios e requisitos

Em 1995, a *BSI* publicou uma norma, a BS 7799-2 também designada *por Information security management systems—Specification with guidance for use*, permitindo às empresas certificar os seus processos. Posteriormente a ISO harmonizou a BS 7799-2 com outras normas ISO, surgindo a primeira versão da ISO 27001 em 2005. A mais recente é a publicada em 2013, na qual é focado o presente estudo.

A norma ISO 27001:2013 especifica os requisitos referentes a um SGSI, permitindo que as organizações avaliem os seus riscos e implementem os procedimentos necessários para a preservação da confidencialidade, integridade e disponibilidade da informação.

Segundo Correia (2016, p.5), esta norma veio «[…] ajudar as organizações a manter os seus ativos de informação, de forma segura, tais como, informações financeiras, propriedade intelectual, dados pessoais dos colaboradores, dos clientes, dos utentes ou informação que foi confiada a terceiras entidades.»

A mesma opinião é partilhada por Kosutic (2016, p.2) na medida que explica « […] *where to start from, how to run your project, how to adapt the security to the specifics of your company, how to control what the IT and security experts are doing, and much more*. »

Para Martins (2013, p.33), a ISO 27001:2013 tem como objetivo «[…] a recetividade por parte das instituições de um conjunto de regras juntamente com a aceitação de processos e controlos desenvolvidos com o intuito de combaterem e gerirem os riscos que a empresa incorre relativos à sua informação.»

De acordo com Calder (2013, p.17), a última versão da ISO 27001 « […] *shifted the focus towards creating aan ISMS that complements the organisation and its processes, and reduced redundancy within the specification and controls*. »

Assim a implementação desta ISO, requer a gestão de diversas políticas, procedimentos, pessoas, ativos, entre outros e a norma vem descrever como combinar todos estes elementos de forma coerente no sistema de gestão de segurança da informação. Pode ser implementada em qualquer tipo de organização e possibilita a obtenção da certificação, caso o sistema esteja em conformidade com os requisitos da norma.

Segundo Kosutic (2016, p.11) dado o crescimento de empresas certificadas pela ISO 27001, esta « […] *already become a number-one, framework worldwide for managing information security, achieving very similar status to what ISO 9001 has become to quality management*. »

É possível dividir a norma em 2 componentes:

- ✓ Na primeira componente, estão incluídas as regras e os requisitos de cumprimento da norma. Estes são semelhantes aos da ISO 9001, e podem ser observados no subcapítulo anterior.
- ✓ Na segunda, intitulada como Anexo A, são definidos os controlos que as organizações devem adotar.

O Anexo A da ISO 27001 é um dos mais reconhecidos anexos de todas as normas ISO porque promove uma ferramenta essencial para gerir a segurança, ao apresentar uma lista de controlos de segurança para serem utilizados para melhorar a segurança da informação (Kosutic, 2016).

Ao todo, são 114 controlos incluídos em 14 seções e em 35 categorias de controlo e cada empresa deve personalizá-los consoante as suas necessidades. De seguida, na Figura 2.12. são apresentadas as 14 seções do anexo em questão.

Figura 2.12. Seções do Anexo A da ISO 27001

Fonte: INTEGRITY (s.d.)

As 14 seções são detalhadamente explicadas nas obras de Kosutic (2016) e THYCOTIC (s.d), as quais reportam o seguinte:

5. Políticas de Segurança da Informação - definem como as políticas são escritas e revistas, com o objetivo de fornecer direção e suporte para a segurança da informação de acordo com os requisitos dos negócios e com as leis e regulamentos relevantes. As políticas devem ser definidas e aprovadas pela gestão e comunicadas aos colaboradores e restantes partes interessadas e revistas entre determinados períodos de tempo.

6. Organização da segurança da informação - controla a forma como as responsabilidades são designadas e também inclui os controlos para dispositivos móveis. O objetivo desta secção é estabelecer uma estrutura de gestão que controle a segurança dentro da organização e garantir que o teletrabalho e o uso de dispositivos moveis detêm de igual forma, segurança.

7.Segurança em recursos humanos - são controlos para antes, durante e após a contratação. Antes da contratação, devem ser descritas quais as responsabilidades e funções a desempenhar. Durante a contratação devem ser claras as responsabilidades que tal colaborador terá perante a segurança da informação, e por fim depois de ser contratado, há que assegurar que irá proteger os interesses da organização.

8. Gestão de ativos - os ativos devem ser identificados assim como as medidas para os proteger, garantindo que consoante a sua classificação, a informação está segura e não é modificada, removida ou destruída.

9. Controlos de acesso - inclui controlos de acesso a sistemas e aplicações, gestão de acesso de usuários e as suas responsabilidades, tendo como objetivos limitar o acesso à informação e às instalações que contêm a informação e garantir que apenas os usuários com acesso obtêm a informação, impedindo o acesso não autorizado.

10. Criptografia - as chaves criptográficas devem ser desenvolvidas e implementadas de forma a garantir o uso adequado e proteger a confidencialidade, autenticidade e integridade de informação.

11. Segurança física e do ambiente - controlos que definem as áreas seguras, controlos de entrada, proteções contra ameaças, segurança de equipamentos, política de mesa ecrã organizados entre outros, impedindo acesso físico não autorizado, assim como danos ou interferências na informação e instalações onde a mesma é processada.

12. Segurança nas operações - abrange os controlos relacionados a gestão da produção de TI: gestão de capacidade, *software* malicioso, cópia de segurança, registo de eventos, monitoramento, instalação, vulnerabilidades, entre outros. Assim, são garantidas instalações corretas e seguras, os recursos são devidamente protegidos contra ações maliciosas, existe maior probabilidade de não perder dados quando são realizadas cópias ou backups, são prevenidas as exposições contra vulnerabilidades técnicas e a integridade do sistema é mais facilmente alcançada.

13. Segurança nas comunicações - controlos relacionados a segurança de rede, segregação, serviços de rede, transferência de informação, emails, entre outros. Os objetivos passam por garantir a segurança das informações na rede assim como na troca de informações com entidades externas.

14. Aquisição, desenvolvimento e manutenção de sistema - envolve requisitos de segurança em processos de desenvolvimento e suporte. A informação deve ser protegida durante todo o ciclo de desenvolvimento dos sistemas de informação assim como os dados utilizados em testes.

15. Relações com fornecedores - estes devem controlar o que incluir em acordos e como gerir os fornecedores. Assim, são controlados os ativos acessíveis pelos fornecedores e é mantido um nível de segurança de informação quando são realizados contratos com os mesmos.

16. Gestão de incidentes de segurança da informação - existência de controlos que reportam eventos e fraquezas, definindo responsabilidades, procedimentos de resposta e de evidências.

17. Aspetos da segurança da informação na gestão da continuidade do negócio - abrange os controlos que requisitam o planeamento da continuidade do negócio, procedimentos, verificação, revisão e redundância da TI. A continuidade da segurança da informação deve ser incorporada na gestão de continuidade de negócios da organização.

18. Conformidade - controlos que implicam a identificação de leis e regulamentos aplicáveis, proteção da propriedade intelectual, proteção de dados pessoais e revisões da segurança da informação. O objetivo é evitar incumprimentos de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança e assegurar que esta está de acordo com as políticas e procedimentos.

2.2.2.7. Benefícios e limitações na adoção de um Sistema de Gestão de Segurança da Informação

Para Vasudevan, V., et al (2015), existem 4 razões principais que motivam as empresas a adotar um SGSI. Estas são:

- Estratégia: devido à exigência do governo ou decisão da administração, para gerir melhor a segurança da informação dentro do contexto de seus riscos gerais de negócios.
- Confiança cliente: a necessidade de demonstrar aos clientes que a organização cumpre as melhores práticas de segurança da informação, ou a oportunidade de obter uma vantagem competitiva sobre os seus concorrentes, tanto no relacionamento com o cliente como com o fornecedor.
- Regulamentar: o desejo de atender a vários requisitos estatutários e regulamentares, especialmente em relação ao uso indevido de computadores, proteção de dados e privacidade.
- Eficiência Interna: a apetência de gerir informações de forma mais eficaz dentro da organização

Assim quer a finalidade da implementação da norma seja a certificação ou não, a adoção das práticas de gestão documentadas na norma, resulta num conjunto de benefícios. Para Correia (2016) estes podem ser:

- Identificação e possibilidade de novas oportunidades de melhorias, sendo um processo de melhoria continua;
- Aumento da fiabilidade e segurança da informação e dos sistemas;
- Incremento dos níveis de participação e motivação dos colaboradores em protegerem a informação;
- Demonstração do compromisso e preocupação com um tema que é importante na atualidade;
- Melhoria do desempenho operacional devido a controlos que provêm da norma e da análise de risco;
- Aumenta a satisfação dos clientes, parceiros, utentes entre outros, pois sentem-se confortáveis com uma organização que tem o compromisso em proteger a informação.

Segundo Casaca (2010, p.28), os benefícios da segurança da informação «[…] não se restringem apenas a uma redução do risco ou uma redução no impacto se ocorrer um evento de risco. Estes benefícios incluem o acesso a informações de forma rápida e eficaz, maior integridade e veracidade da informação, maior segurança no acesso, redução de custos operacionais, administrativos e ganhos de produtividade e otimização do processo de decisão e do fluxo de informação a circular dentro da organização.»

No entanto, também podem ser observadas limitações. Uma das limitações apontadas à ISO 27001 até à versão de 2005, era o facto de ser da responsabilidade da organização, definir quais os requisitos que compunham o seu sistema. Segundo Silva (2006), o resultado foi o «[…] o surgimento de deficiências que impactaram a eficácia do próprio sistema de gestão. Surgiram empresas certificadas com escopos excessivamente reduzidos.»

Esta foi corrigida com a ISO 27001:2013 quando a ISO passou a exigir que o escopo abrangesse minimamente os processos relevantes da organização. Esta readaptação levou a que muitas empresas perdessem a certificação por ser evidente que o seu sistema não era o mais adequado.

Outra limitação associada ao SGSI é pensar que os sistemas de informação são seguros por serem atuais e que a existência de antivírus e firewall são suficientes para protegerem a informação. Embora sejam mecanismos de controlo, Kosutic (2016, p.12) defende que « […] *IT security is only half of information security, because information security also includes physical security, human resources management, legal protection, organization, processes etc. »* Ou seja, embora a tecnologia, seja importante para proteger a informação, não é suficiente e deve ser combinada com outros mecanismos, políticas e procedimentos que assegurem a segurança daquele que é o ativo mais importante de qualquer organização.

Contudo, uma das limitações mais destacadas nestes processos de implementação são os custos como referido no subcapítulo da ISO 9001. Os custos associados podem ser a formação de colaboradores, o conhecimento técnico que possuem, as ferramentas e modelos a implementar, a assistência externa que obtêm, mas acima de tudo o custo da tecnologia.

2.2.3. Certificação

O processo de certificação pode ser descrito como a emissão de um certificado de conformidade que assegura que determinado produto, processo ou serviço está em conformidade com os requisitos de um dado referencial como as normas (Santana, 2014).

Este certificado é atribuído por uma entidade certificadora externa e independente, após auditar uma determinada empresa e verificar que estão cumpridos os requisitos especificados na norma aplicável.

A certificação é voluntária e qualquer empresa pode recorrer a este serviço independentemente da sua forma jurídica ou atividade desenvolvida. Não sendo obrigatória, a escolha da certificação pode ser vista como uma vantagem competitiva perante as demais organizações (Santana, 2014).

No entanto as certificações são temporárias. Isto porque para além de as normas estarem constantemente a sofrer alterações, é atribuído um prazo por cada certificado emitido ao fim do qual o processo é reiniciado. Este prazo tem a duração de 3 anos, ao fim do qual pode ser renovado.

Cabe à entidade certificadora fazer visitas regulares à empresa, normalmente com um ano de intervalo, no sentido de confirmar que os requisitos continuam a ser cumpridos. Se estas visitas declararem situações graves ou não conformidades importantes e tais requisitos deixarem de ser cumpridos, a certificação pode ser suspensa ou anulada.

Na perspetiva de Ribeiro (2012) ser detentora de um certificado de conformidade confere à organização:

- Garantia que toda a empresa está em processo continuo de melhoria devido às auditorias periódicas;
- Credibilidade no serviço prestado, aumentando a satisfação do cliente e a confiança;
- Maior desempenho geral, o que poderá conduzir a uma redução de custos;
- Ampliação das oportunidades no mercado;
- O processo de auditoria regular melhora a responsabilidade, o comprometimento e a motivação de todos os envolvidos;
- Demonstrar às partes interessadas que o negócio funciona de forma eficaz;
- Maior capacidade de resposta rápida e flexível às oportunidades.

As necessidades de obter certificação, têm evoluído. Para Moeller (2008, p.289), « […] w*hat was once just nice to have has become almost mandatory. »*

Optar por ser uma empresa certificada, exige um elevado esforço de todos os envolvidos uma vez que é um processo moroso e várias áreas podem ser alvo de mudanças para

cumprirem os requisitos que cada norma defende. Assim, este processo deve ser clarificado e enfrentado de forma consciente para que corra da forma esperada.

As várias fases que compõem o processo de certificação, podem ser descritos na Tabela 2.4. abaixo apresentada.

Tabela 2.4. Etapas da certificação

1	• Empresa demonstra a sua intenção perante a entidade certificadora
2	• É elabora uma proposta, juntamente com a informação do processo
3	• A empresa formaliza o pedido, realiza o pagamento, envia a documentação necessária e agenda a 1ªfase de auditoria
4	• A entidade certificadora, nomeia a equipa auditora que analisa a documentação e elabora um plano de auditoria
5	• É realizada a auditoria e feito um relatório onde constam os factos observados
6	• A empresa responde ao relatório, identificando as causas ds não conformidades, as açoes corretivas ou preventidas e o prazo de implementação
7	• A equipa auditora, analisa a resposta ao relatorio, elabora um plano de auditoria e realiza a auditoria de 2ª fase
8	• São obtidas respostas ao relatório sobre a auditoria de 2ª fase
9	• A entidade analisa por fim todo o processo e toma a decisão de emitir ou não o certificado
10	• São agendadas as auditorias de acompamento até ao fim do prazo do certifiado

Fonte: Adaptado de Empresa Internacional de Certificação (EIC)

Todos os anos a ISO, elabora a ISO *Survey Certifications* onde é realizado um estudo ao número de certificados emitidos por área geográfica, por país e ainda por sector.

Com referência a 31 de dezembro de 2017, e por falta de publicação do estudo para os anos de 2018/2017 à data da elaboração da presente dissertação, as normas neste estudo abordadas, compreendem a seguinte observação:

- Evolução da ISO 9001 entre os anos 2016 e 2017. É possível observar pela Tabela 2.6. que em todas as áreas, houve uma diminuição de certificados à exceção do Leste da Ásia e o Pacífico que verificou um aumento. A ISO esclarece que esta descida se deve apenas à mudança na forma como foram reportados os dados.

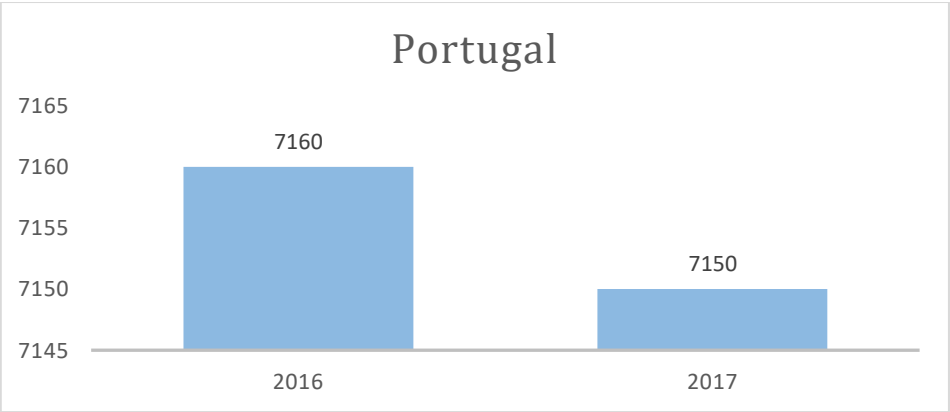
Tabela 2.6. Evolução dos certificados ISO 9001 entre 2016 e 2017

Área	2016	2017
África	13.378	11.210
Centro/Sul da América	52.094	45.541
Norte da América	44.252	38.218
Europa	451.415	389.485
Este da Ásia e Pacífico	480.445	513.742
Centro/Sul da Ásia	41.370	39.887
Total	**1.082.954**	**1.038.083**

Fonte: ISO Survey (s.d.)

No que respeita a Portugal, foram emitidos 7056 certificados, ocupando assim o 14º lugar entre os restantes 52 paises da Europa que foram alvo de pesquisa. Embora não seja um valor muito significativo quando comparado com o número de certificados emitidos em Itália (97.646), Alemanha (64.658) e Reino Unido (37478), Portugal consegue permanecer à frente de paises como Suécia (5742), Rússia (3490) e Bélgica (3121). O Gráfico 2.2. regista a evolução dos certificados entre 2016 e 2017, onde se verifica um decréscimo de 10 certificados. Como referido anteriormente, esta diminuição deve-se à alteração na comunicação dos dados.

Gráfico 2.2. Evolução dos certificados ISO 9001 entre 2016 e 2017 em Portugal



Fonte: ISO Survey (s.d.)

- Evolução da ISO 27001 entre os anos 2016 e 2017 – Perante a Tabela 2.5. é possível observar que em todas as áreas, houve um aumento de certificados. Este aumento é claramente maior na Ásia do Leste e no Pacifico e na Europa.

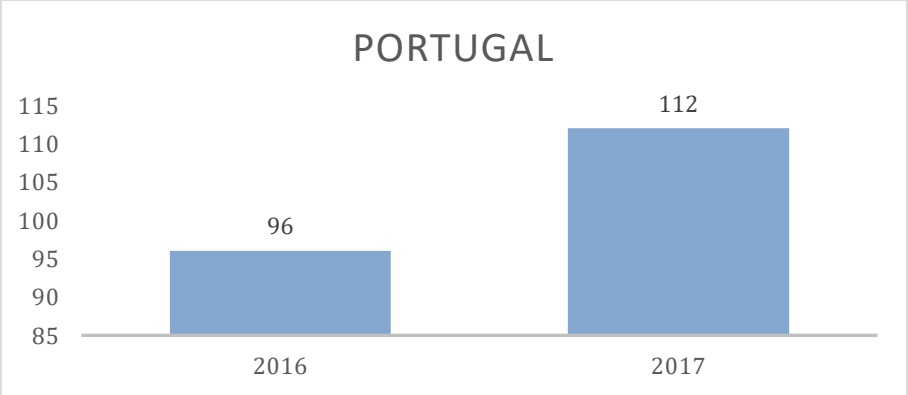
Tabela 2.5. Evolução dos certificados ISO 27001 entre 2016 e 2017

Área	2016	2017
África	224	301
Centro/Sul da América	564	620
Norte da América	1.469	2.108
Europa	12.532	14.605
Este da Ásia e Pacífico	14.704	17.562
Centro/Sul da Ásia	2.987	3.382
Total	**17.776**	**38.578**

Fonte: ISO Survey (s.d.)

No que respeita a Portugal, foram emitidos 112 certificados, ocupando assim o 22º lugar entre os restantes 52 paises da Europa alvos de pesquisa. Comparando com o número de certificados emitidos em Inglaterra (4503), Alemanha (1339) e Itália (958), Portugal tem registado um aumento significativo como se pode observar no Gráfico 2.1.

Gráfico 2.1. Evolução dos certificados ISO 27001 entre 2016 e 2017 em Portugal



Fonte: ISO Survey (s.d.)

2.3. Controlo Interno

Este subcapítulo, tem como objetivo apresentar os conceitos e importância associados ao controlo interno. Serão também identificadas as componentes que compõem o modelo COSO para que sejam depois analisadas as sinergias entre o COSO e as ISO.

2.3.1. Conceitos

A preocupação com o controlo interno, tem vindo a evoluir. Segundo Valente (2014, p.5), este conceito «[…] ganhou ênfase no final do século passado e no início deste, na sequência de um grande número de escândalos financeiros que assolaram os Estados Unidos da América […]». Entre estes escândalos, está o Worlcom, a Enron, Parmalat entre outros.

Para dar resposta a estes escândalos financeiros foi aprovada no ano de 2002, nos EUA, a lei *Sarbanes-Oxley Act* . Esta lei veio proteger os investidores ao exigir que as empresas emitentes de valores mobiliários divulgassem informações, financeiras e não financeiras, apropriadas e rigorosas.

Segundo Morais e Martins (2013, p. 28), o controlo interno surgiu para acompanhar:

- As necessidades da organização e dos gestores no alcance dos seus objetivos;
- A tomada de decisão tendo por base a informação;
- A evolução económica e a competitividade entre empresas;
- As necessidades e expetativas dos clientes que estão em constante mudança, o que exige da organização uma estrutura adaptável a tais alterações.

O COSO (2013, p.3) defende que o controlo interno é um processo « […] *effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.* »

Para Carneiro (2009, p.53) o controlo interno «[…] é um instrumento de organização e integra todos os métodos e mediadas, adotadas por uma empresa para proteger os seus ativos, confirmar a exatidão e a fidelidade dos seus dados […], garantir e aumentar a eficiência operacional".

Segundo Attie (1992) este conceito engloba os meios para dirigir, governar e controlar as várias atividades de uma empresa para que estas alcancem os seus objetivos. Estes meios

podem ser sistemas, políticas, formulários, manuais, relatórios, segregação de funções, autorizações, aprovações, registos entre outros.

Na visão do Tribunal de Contas de Portugal (1999, p.47), «[o] controlo interno é uma forma de organização que pressupõe a existência de um plano e de sistemas coordenados destinados a prevenir a ocorrência de erros e irregularidades ou a minimizar as suas consequências e a maximizar o desempenho da entidade na qual se insere.»

Por sua vez, Costa (2014, p.216), refere que o controlo interno é o «[…] o processo concebido, implementado e mantido pelos responsáveis pela governação, gestão e outro pessoal para proporcionar segurança razoável que permita atingir os objetivos da entidade relativamente à credibilidade do relato financeiro, eficiência e eficácia das operações e cumprimento das leis e regulamentos aplicáveis.»

No entanto, os conceitos de controlo interno e SCI, não devem confundir-se. Segundo Monteiro (2015, p.18), deve ser entendido que

> o Controlo Interno se associa ao processo levado a cabo pela gestão de uma empresa, tendo em vista a concretização dos objetivos referidos nas definições acima apresentadas, enquanto que o Sistema de Controlo Interno compreende as políticas e procedimentos que de facto são implementados na empresa, isto é, os controlos internos existentes na entidade

Completando a visão de Monteiro, Serralheiro (2017, p.2) afirma que o SCI é «[…] um sistema onde a direção das organizações consegue encontrar um apoio para melhorar o controlo na sua organização.» Com este sistema, a organização alcançará mais facilmente os objetivos do controlo interno, ao nível da eficácia e eficiência de recursos, da fiabilidade da informação e, ainda, o cumprimento das normas e leis aplicáveis à organização.

2.3.2. Importância e Objetivos

O controlo interno é importante para toda a organização. Segundo Marques (2013, p.5), esta afirmação é confirmada porque

> Por um lado, a toda a empresa desde a administração e direção, sendo estes também os responsáveis pelo controlo interno, uma vez que este permite-lhe a concretização dos objetivos estabelecidos, como pelos funcionários pois este

> também tem em conta a continuidade da empresa. Por outro lado, também é importante para as pessoas externas à empresa (clientes, fornecedores, bancos, instituições públicas como as Finanças, comunidade em geral) pois um controlo interno eficaz funciona como uma garantia relativamente à fiabilidade da informação oriunda da empresa

Para Osório (2014, p.21), o controlo interno é fundamental porque «[…] interfere diretamente nos processos operacionais, internos e externos, devendo ser adaptado às necessidades dessa organização.»

A importância do controlo interno é ainda explicada por Monteiro (2015, p.19), «[…] quer para a prevenção, como para a deteção e correção de erros e irregularidades a que a empresa se sujeita no normal decorrer das suas operações.» Assim sendo, o controlo interno deve recomendar quais as ações a implementar consoante o seu tipo de controlo.

De acordo com Costa (2010, p.223), «[…] nenhuma empresa ou entidade, por mais pequena que seja, pode exercer a sua atividade operacional sem ter implementado um sistema de controlo interno, ainda que rudimentar.»

Para reforçar esta visão, Attie (1992) destaca que para além das irregularidades por atos voluntários geralmente conhecidos como fraudes, poderão ocorrer outros erros, de carácter involuntário, os quais podem não ser detetados se não houver controlo interno ou for inadequado à realidade da organização.

Relativamente aos objetivos, estes centram-se na procura de boas praticas de gestão e procedimentos, bem como o cumprimento das políticas (Osório, 2014).

Já o COSO (2013) divide os tipos de objetivos do controlo interno em três categorias: objetivo das operações, objetivo da informação e objetivo da conformidade. O objetivo das operações, está relacionado com a eficácia e eficiência das operações e com a salvaguarda dos ativos. Por outro lado, o objetivo de informação, tem como foco a preparação da informação fidedigna e a sua divulgação às demais partes interessadas. Por último, o da conformidade diz respeito ao cumprimento das leis e regulamentos aplicáveis.

Ernest & Young (2010) defendem que quanto melhor for a qualidade dos controlos internos, maior será a probabilidade de a organização minimizar os riscos que encara e a melhor

maneira de uma entidade garantir que as expetativas e as normas podem ser alcançadas, é estabelecer um SCI adequado.

Se o SCI da organização for adequado, as auditorias são mais breves assim como os relatórios. Por outro lado, se o SCI for insuficiente, a auditoria demorará mais tempo e necessitará de um maior esforço o que pode significar custos superiores e uma maior dificuldade em implementar as recomendações.

2.3.3. Modelo COSO

Um dos modelos de controlo interno mais conhecidos e aplicados é o modelo do COSO, publicado em 1992, sendo revisto e atualizado em 2013. A estrutura deste modelo permite à organização centrar-se nas suas componentes chave, valores e processos que compõem o controlo interno. As 5 componentes funcionam de forma articulada, gerando sinergias entre si e estão assentes em 17 princípios. A relação entre os objetivos e as componentes do COSO podem ser apresentadas na forma de um cubo conforme a Figura 2.13. onde se identificam:

- Três categorias de objetivos – representadas nas colunas
- Cinco componentes – descritas nas linhas
- A estrutura organizacional de uma empresa – apresentada na lateral

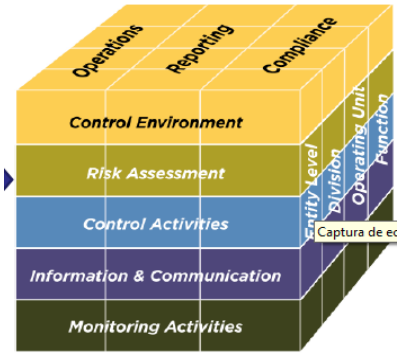


Figura 2.13. Modelo COSO

Fonte: COSO (2013, p.6)

A combinação destes 3 no cubo, é explicada por Inácio (2014, p.36) ao afirmar que

> Há um relacionamento direto entre os objetivos da entidade, que são o que a entidade tem em vista alcançar, e os componentes da estrutura do controlo

> interno, que representam o que é necessário para atingir aqueles objetivos. Acresce que os objetivos estão sempre presentes nos vários níveis em que a entidade se divide (atividades, departamentos, unidades) e onde se devem aplicar os componentes do controlo interno.

As componentes anteriormente referidas incluem:

- Ambiente de Controlo

De acordo com COSO (2013, p.4) engloba um conjunto de « […] *standards, processes and structures that provide the basis for carrying out internal control across the organization*. »

Já na perspetiva de Marques (2013, p.30), «[é] esta componente que permite que o controlo interno garanta disciplina, estrutura e processo.»

Segundo o COSO (1994, p.4), esta componente inclui « […] *integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the wat management assigns authority and responsibility and organizes and develops its people* […] ».

- Avaliação de Risco

Qualquer organização, está diariamente exposta a uma variedade de riscos internos e externos que podem por em causa o alcance dos objetivos. Como riscos externos, existe o desenvolvimento da tecnologia, mudanças nas necessidades ou expetativas dos clientes, desastres naturais, preços e os regulamentos aplicáveis. Por outro lado, os riscos internos podem ser identificados pelos sistemas e a segurança de informação, motivação e formação dos colaboradores, os acessos aos ativos e a falta de interesse da gestão.

A avaliação de riscos passa pela identificação e análise dos riscos relevantes que são responsáveis por influenciar a concretização de objetivos definidos pela organização.

Para Moeller (2008, p.103), é essencial «[a]*n understanding and management of the risk environment is a basis element of the internal control Foundation, and an enterprise should have a process in place to evaluate the potential risks that may impact attainment of it various objectives*. »

Uma vez que a economia, a indústria, os regulamentos e as condições de operar estão em constante mudança, há que introduzir mecanismos que identifiquem e lidem com os riscos que estas mesmas mudanças podem trazer. (COSO, 1994)

Além disso, a avaliação de riscos permite à organização priorizá-los, ou seja, atuar sobre aqueles que se apresentem mais críticos e que mais afetem o desempenho da organização e a consecução dos seus objetivos. (COSO, 2013)

- Atividades de Controlo

A característica desta componente prende-se com políticas e procedimentos que asseguram as respostas aos riscos e o cumprimento das diretrizes, visando o alcance dos objetivos.

Para confirmar esta afirmação, Marques (2013, p.35), defende que estas atividades «[…] existem em todos os níveis da empresa e servem como mecanismos para se proceder a uma gestão da empresa orientada para a realização dos objetivos.»

Estas atividades podem ser segundo COSO (2013, p.4) « […] *preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.* »

Para Monteiro (2015), como atividades de controlo podem enumerar-se a autorização pela gestão de uma venda a crédito ou ainda a numeração sequencial de todos os documentos, desde faturas a guias de remessa, permitindo com isto, detetar situações menos apropriadas.

- Informação e Comunicação

Quer a informação, quer a comunicação, são 2 componentes determinantes. A informação porque permite que a organização consiga ir ao encontro das suas responsabilidades de controlo interno e alcançar os seus objetivos A comunicação, porque é através desta que a organização transmite a informação importante para todos os interessados.

De acordo com Moeller (2008, p.107), a informação « […] *must be communicated up and down the enterprise in a manner and time frame that allows people to carry out their responsibilities. »* Sobre a comunicação, o mesmo autor defende « […] *enterprises must have effective procedures in place to communicate with internal and external parties. »*

Para Inácio (2014, p. 46), a informação e comunicação, prendem-se com «[…] a identificação, recolha e troca de informação por forma a permitir aos empregados levarem a cabo as suas responsabilidades.*»*

A informação deve ser apropriada, atempada, atual, correta e acessível a quem diz respeito. Já a comunicação pode ser feita através de manuais de procedimentos, memorandos, notas internas, newsletters entre outros.

- Monitorização

A monitorização do sistema de controlo interno, consiste num processo que avalia a qualidade do desempenho do sistema ao longo do tempo. Esta componente recorre a monitorizações continuas, avaliações separadas ou uma combinação das duas. Na perspetiva de COSO (2013, p.5), as «[o]*ngoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations.* »

Segundo Monteiro (2015, p.36), «[…] a monotorização do controlo interno permitirá concluir se os controlos implementados estão a operar como o esperado e se são modificados conforme existam alterações das condições que levaram à sua criação.»

Na perspetiva de Valente (2014, p.18), «[…] os resultados serão avaliados em comparação com os critérios estabelecidos pelos reguladores, pelos quadros de normalização reconhecidos ou pela gestão ou quadro de diretores, e as deficiências serão comunicadas para estes órgãos conforme apropriado.»

2.4. Sinergias COSO, COBIT e ISO

O presente subcapítulo, tem como objetivo verificar se existem sinergias entre as componentes do controlo interno com os requisitos das normas que regem os SGQ e SGSI. Uma vez abordado o COBIT e a sua ligação aos sistemas de informação, será também possível cruzar este modelo com o COSO e as ISO.

Depois de serem dadas a conhecer as normas ISO e os modelos COSO e COBIT, é possível identificar diversas semelhanças. Relativamente ao SGQ e o SCI, estes permitem às organizações melhorar continuamente o seu desempenho na qualidade do serviço prestado e dos produtos fornecidos. Assim sendo Serralheiro (2017, p.15) afirma que

> A combinação dos dois sistemas numa organização pode potencializar a continuidade e a sustentabilidade da mesma, na medida em que a aplicação

> conjunta consegue satisfazer, por um lado, as necessidades de gestores, acionistas ou cidadãos através da implementação do SCI e, por outro lado, satisfazer as necessidades dos clientes e partes interessadas, com a implementação do SGQ, evitando as redundâncias e custos.

No que concerne à relação do SGSI e o SCI, é importante que com o desenvolvimento das novas tecnologias, existam formas de o controlo interno atuar. Relativamente aos programas de computador, a preocupação centra-se na sua documentação. Esta deve ser cuidadosamente mantida e quaisquer alterações devem ser aprovadas por pessoas com responsabilidade para tal e refletidas em documentos de suporte. O processamento de informações e dados, deve ser uniforme segundo os manuais de procedimentos elaborados e o seu arquivo deve ser guardado em local seguro e atualizado de forma periódica. O restante equipamento que contenha informação privilegiada sobre a organização, deve ser mantido em segurança, nas condições físicas apropriadas na qual devem ser feitas manutenções regulares.

Na perspetiva de Peláez (2011), as semelhanças dos sistemas de qualidade, segurança da informação e controlo interno são as seguintes:

- Formação, avaliação de competências e necessidade dos colaboradores em corresponder às responsabilidades;
- A atividade de auditoria interna, onde são feitas recomendações para a melhoria do sistema e quais as medidas a implementar para corrigir as não conformidades;
- A procura da eficiência e eficácia dos processos para atingir os objetivos;
- A necessidade de liderança, compromisso e participação de todos os envolvidos.

Contudo, as semelhanças entre estes sistemas não ficam por aqui e podem incluir-se as seguintes:

- São sistemas flexíveis, possíveis de serem adaptados a qualquer organização;
- Requerem o envolvimento dos colaboradores, que são peça chave para atingir os objetivos;

- Em qualquer um dos casos, o sistema deve ser visto como um meio para chegar a um fim, ou seja, consistir num processo que conta com tarefas e atividades contínuas;
- Embora não garantam segurança ou conformidade absoluta, proporcionam-nas de forma razoável;
- Existe a necessidade de ir ao encontro das expetativas dos clientes e de outras partes interessadas e da própria organização.

Ao complementarem-se, surge outra vantagem, a não duplicação de custos e esforços.

De forma a verificar as sinergias existentes entre o controlo interno e as normas ISO, segue-se uma análise entre as 5 componentes do COSO e os requisitos da ISO 9001 e da ISO 27001.

- Ambiente de Controlo versus Requisitos da ISO 9001 e 27001

O envolvimento da gestão é um fator determinante para ambos os sistemas, pois devem supervisionar e garantir o bom funcionamento da organização e do sistema face aos requisitos impostos, realizando avaliações periódicas para verificar a situação em que se encontram e como podem melhorá-la. A segregação de funções, a comunicação interna, a competência e formação dos colaboradores que alcançam os objetivos, assim como a avaliação de desempenho são outros dos fatores em comum. A Tabela 2.7. abaixo apresentada, identifica as semelhanças entre o ambiente de controlo e os requisitos das normas ISO.

Tabela 2.7. Princípios do Ambiente de Controlo versus Requisitos das ISO

Componente do COSO	**Requisitos ISO 9001:2015 e 27001:2013**
P1 - Compromisso face a valores éticos e de integridade	4 – Contexto da organização 4.1. Compreender a organização e o seu contexto
P2 – Demonstra o exercício de responsabilidade pela supervisão	4.2. Compreender as necessidades e as expectativas das partes interessadas 4.4. Sistema de gestão da qualidade e respetivos processos

P3 – Define a estrutura, autoridade e Responsabilidade	5 – Liderança 5.1. Liderança e compromisso
P4 – Demonstra compromisso com a competência dos seus profissionais	5.2. Política 5.3. Funções, responsabilidades e autoridades organizacionais 6.2 - Objetivos da qualidade e planeamento para os atingir
P5 – A organização define as responsabilidades dos colaboradores ao nível do controlo interno para a consecução dos objetivos.	7 – Suporte 7.1. Recursos 7.2. Competências 7.3. Consciencialização 7.4. Comunicação 8 – Operacionalização 8.4. Controlo dos processos, produtos e serviços de fornecedores externos 9 – Avaliação do desempenho 9.1. Monitorização, medição, análise e avaliação 9.3. Revisão pela gestão

Fonte: Adaptação Serralheiro (2017, p.20)

- Avaliação de riscos versus Requisitos da ISO 9001 e 27001

A organização deve ter em consideração fatores internos e externos à organização, estimar a importância dos riscos e determinar como irá responder aos mesmos. Esta preocupação está presente nas duas normas, que ao determinar os riscos e as oportunidades, planeia as ações a realizar. Se por um lado, o controlo interno tem que reagir às mudanças no negócio e na própria organização, bem como às mudanças regulamentares, por outro, na qualidade há que responder às necessidades dos clientes, cada vez mais exigentes informados. Já na segurança da informação, a avaliação de riscos é também importante uma vez que são diversas as ameaças às quais está exposta a informação. A tabela 2.8. abaixo apresentada, identifica as semelhanças entre a avaliação de riscos e os requisitos das normas ISO.

Tabela 2.8. Princípios da Avaliação de riscos versus Requisitos das ISO

Componente do COSO	**Requisitos ISO 9001:2015 e 27001:2013**
P6 – Especifica os objetivos relevantes	4 – Contexto da organização 4.1. Compreender a organização e o seu contexto
P7 – Identifica e analisa riscos	4.2. Compreender as necessidades e as expectativas das partes interessadas
P8 – Avalia o risco de fraude	5 – Liderança
P9 – Identifica e analisa alterações significativas	6 – Planeamento 6.1. Ações para tratar riscos e oportunidades 6.2. Objetivos da qualidade e planeamento para os atingir 6.3. Planeamento das alterações 8.2. Requisitos para produtos e serviços 8.4. Controlo dos processos, produtos e serviços de fornecedores externos 8.6. Libertação de produtos e serviços 9 – Avaliação do desempenho 9.1. Monitorização, medição, análise e avaliação 9.2. Auditoria interna 9.3. Revisão pela gestão 10 –Melhoria 10.1. Generalidades 10.2. Não conformidades e ações corretivas 10.3. Melhoria contínua

Fonte: Adaptação Serralheiro (2017, p.22)

- Atividades de controlo versus Requisitos da ISO 9001 e 27001

As atividades de controlo são essenciais para resolver os riscos e alcançar os objetivos planeados. Em qualquer um dos sistemas, existe a necessidade de criar controlos para fazer

face aos riscos que possam surgir, definindo linhas de orientação que permitam agir perante situações de desvios ou não conformidades. A tabela 2.9. abaixo apresentada, identifica as semelhanças entre as atividades de controlo e os requisitos das normas ISO.

Tabela 2.9. Princípios das Atividades de controlo versus Requisitos das ISO

Componente do COSO	Requisitos ISO 9001:2015 e 27001:2013
P10 – Seleciona e desenvolve atividades de controlo	4 – Contexto da organização 4.1. Compreender a organização e o seu contexto
P11 – Seleciona e desenvolve controlos gerais sobre a tecnologia	4.2. Compreender as necessidades e as expectativas das partes interessadas
P12 – Implementa através de políticas e procedimentos	6 – Planeamento 6.1. Ações para tratar riscos e oportunidades 8.7. Controlo de saídas não conformes 9.3. Revisão pela gestão 10 –Melhoria 10.2. Não conformidades e ação corretiva 10.3. Melhoria contínua

Fonte: Adaptação Serralheiro (2017, p.24)

- Informação e Comunicação

Esta componente defende que as empresas devem identificar a informação necessária e relevante e que seja comunicada de forma clara e objetiva quer internamente, quer externamente. A ISO 9001:2015 refere que a organização deve utilizar meios de comunicação e informação para melhorar o processo de tomada de decisão dentro da organização. No caso da ISO 27001:2013, e dado que esta retrata a importância de proteger a informação, os princípios desta componente são em muito semelhantes ao que é defendido na norma. A tabela 2.10. abaixo apresentada, identifica as semelhanças entre a informação e comunicação e os requisitos das normas ISO.

Tabela 2.10. Princípios da Informação e Comunicação versus Requisitos das ISO

Componente do COSO	ISO 9001:2015 e 27001:2013
P13 – Utiliza informação relevante	5.1. Liderança e compromisso
P14 – Comunica internamente	7.4. Comunicação 7.5. Informação documentada 7.5.2. Criação e atualização 7.5.3. Controlo da informação documentada
P15 – Comunica externamente	8.2. Requisitos para produtos e serviços 8.2.1. Comunicação com o cliente 8.4. Controlo dos processos, produtos e serviços de fornecedores externos 8.4.3. Informação para fornecedores externos

Fonte: Adaptação Serralheiro (2017, p.26)

- Monitorização

A necessidade de supervisão, está presente através de atividades de avaliação e monitorização em qualquer um dos três sistemas em análise. No SCI através de avaliações periódicas independentes e monitorizações contínuas. Já as ISO exigem a monitorização e medição dos processos e ou produtos, mas também a realização de auditorias internas das quais podem resultar não conformidades, que são tratadas de forma semelhante. A tabela 2.11. abaixo apresentada, identifica as semelhanças entre a monitorização e os requisitos das normas ISO.

Tabela 2.11. Princípios da Monitorização versus Requisitos das ISO

Componente do COSO	ISO 9001:2015 e 27001:2013
P16 – Conduz avaliações contínuas e/ou em separado	4 – Contexto da organização 4.1. Compreender a organização e o seu contexto

	4.2. Compreender as necessidades e as expectativas das partes interessadas
P17 – Avalia e comunica deficiências	6.2. Objetivos da qualidade e planeamento para os atingir 8.6. Libertação de produtos e serviços 9 – Avaliação do desempenho 9.1. Monitorização, medição, análise e avaliação 9.1.1. Generalidades 9.1.2. Satisfação do cliente 9.1.3. Análise e avaliação 9.2. Auditoria interna 9.3. Revisão pela gestão 10 – Melhoria 10.1. Generalidades 10.3. Melhoria contínua

Fonte: Adaptação Serralheiro (2017, p.27)

Outro ponto de paralelismo entre a ISO 27001 e o controlo interno é a existência do modelo COBIT. Para Leal (2016), o COSO, o COBIT e a ISO 27001 encontram-se interligados porque tem certos aspetos em comum:

- Orientados por objetivos - enquanto que o COSO e o COBIT possuem objetivos claramente definidos, a ISO 27001 requer que os objetivos de segurança da informação sejam definidos por cada organização de acordo com o seu contexto em termos de confidencialidade, integridade e disponibilidade, para assegurar que os processos de segurança e da organização estão operacionais;
- Direcionados a processos - os três utilizam a abordagem por processos para organizar as suas atividades, o que pode traduzir benefícios na forma de interagir através da visão dinâmica que é obtida;

- Utilização de controlos - enquanto que com o COSO os controlos são mais gerais com o objetivo de cobrir o maior número de processos de negócio quanto possível, o COBIT reduz o foco para as tecnologias da informação, e a ISO 27001 para a segurança da informação. Isto resulta em oportunidades de complementação e na otimização de ações.

Estas interligações podem ser apresentadas na Figura 2.14., que se observa de seguida.

Figura 2.14. Semelhanças entre o COSO, COBIT e ISO 27001

Fonte: Leal (2016)

Para que um SGQ e o SGSI sejam implementados de forma correta, é, portanto, necessário um adequado SCI que vá de encontro ao que é defendido pelas normas, pelo que uma organização que tenha um bom SCI estará em melhores condições de poder implementá-las.

Contudo, salienta-se que quer a norma da qualidade quer a norma da segurança da informação, não obrigam à presença do SCI. No entanto a sua presença tende a garantir uma melhor eficácia e eficiência dos sistemas em causa como se pôde observar.

3.Apresentação da Empresa Objeto de Estudo

A empresa X foi criada em 2010 e dedica-se desde então, à prestação de serviços de consultoria de gestão, com sede em Lisboa. As principais áreas de atuação, são a Contabilidade em regime Insourcing e Outsourcing, Gestão Administrativa de Recursos Humanos (GARH), Consultoria Financeira e Fiscal, Recursos Humanos (RH) e ainda o Departamento Administrativo Financeiro (DAF).

O organograma da empresa pode ser observado na Figura 3.1.

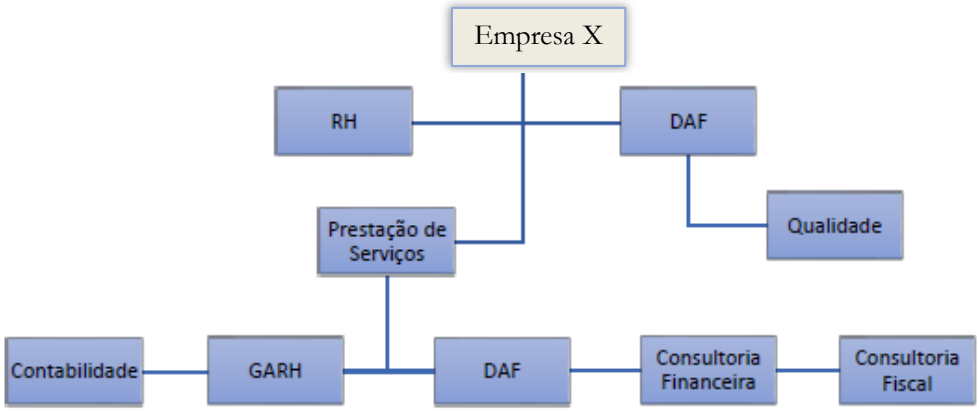


Figura 3.1. Organograma da empresa X

Fonte: Elaboração própria

Esta empresa apresenta como visão o desejo de informar, comunicar e entregar aos seus clientes, informação financeira útil. Esta é alcançada através dos seus valores que se centram na integridade, flexibilidade, competência, responsabilidade e respeito pelas pessoas e organizações.

Hoje em dia, conta com escritórios noutras geografias como é o caso da Guiné-Bissau, Polónia, China, Moçambique, Cabo Verde, Brasil, Angola, Espanha e Madeira.

As atividades e sociedades onde opera são apresentadas na Tabela 3.1.

Tabela 3.1. Atividades e Sociedades de atuação

Atividades	Sociedades
Consultoria	Associações e Fundações
Atividades Financeiras e Seguradoras	Entidades e Organismos Públicos
Atividades Imobiliárias	Fundos de Investimento Imobiliário
Agricultura	Grupos de Sociedades (SGPS)
Alojamento e Restauração	Sociedades Anónimos
Comércio por Grosso e Retalho	Sociedades cotadas em Bolsa
Construção Civil	Sociedades de Transparência Fiscal
Indústria	Sociedades Profissionais
Saúde e Ação Social	Agrupamento Complementar de Empresas
Serviços Coletivos, Sociais e Pessoais	Sociedades Gestoras de Fundos Investimentos Imobiliários
Transportes e Comunicação	Sociedades por Quotas

Fonte: Elaboração própria

4.Metodologia

O presente capítulo, tem como objetivo caracterizar o tipo de estudo escolhido para esta investigação, apresentar as perguntas e hipóteses que se pretendem comprovar e os métodos de pesquisa e recolha de dados selecionados. Definido o método de recolha de dados por meio de questionários, será apresentada a estrutura que os compõem, uma breve caracterização da amostra alvo e quais os procedimentos para a recolha de dados e tratamento da informação.

4.1. Estudo de Caso

O estudo de caso visa «[…] conhecer uma entidade bem definida como uma pessoa, uma instituição, um curso, uma disciplina, um sistema educativo, uma política ou qualquer outra unidade social.» (Ponte, 2006, p.2)

Vilelas (2009) afirma que os estudo de caso são geralmente utilizados na obtenção de dados na área dos estudos organizacionais e enquadram-se numa abordagem qualitativa.

A metodologia associada a este estudo é descrita por Bell (1993, p.23) como

> muito mais que uma história ou descrição de um acontecimento ou circunstância. Tal como em qualquer outra investigação, os dados são recolhidos sistematicamente, a relação entre as variáveis é estudada e o estudo é planeado metodicamente.

De acordo com Canto (2010), as vantagens da realização de um estudo de caso são as seguintes:

- Maior facilidade de acesso ao público do que outros dados em investigação;
- Forte relacionamento entre a teórica e a prática;
- Melhor capacidade de perceção através de exemplos, acontecimentos ou limitações.

Apesar das vantagens acima descritas, podem também ser levantadas algumas limitações ao estudo de caso como:

- Problemas relacionados com a confidencialidade do nome da empresa, dos inquiridos, dos serviços e quaisquer outras informações que permitam identificar a mesma;
- Informação partilhada entre o investigador e a organização não ser fidedigna ou vir a ser distorcida;
- Não poderem ser generalizados aos restantes casos.

4.2. Questões de investigação e hipóteses de estudo

As hipóteses de estudo, são uma parte essencial em qualquer estudo empírico uma vez que segundo Kerlinger (1973) a investigação tem como principal prepósito a verificação de tais hipóteses.

Quivy e Campenhoudt (2005) acrescentam que as hipóteses de estudo funcionam como respostas provisórias à pergunta de partida da investigação.

O presente estudo, tem como perguntas de investigação as seguintes:

1. A auditoria e o controlo interno representam um papel importante na adoção das normas ISO?
2. Existem sinergias entre as componentes do controlo interno e as exigências das normas ISO adotadas?

Tendo em conta os objetivos do estudo já enunciados, surge a necessidade de verificar ou não as hipóteses de estudo que devem assim ser analisadas:

H1: De uma auditoria interna adequada resultam colaboradores preparados;

H2: Da ausência de uma auditoria interna derivam colaboradores desconfortáveis

H3: A auditoria externa é vista como útil aos processos de implementação das ISO

H4: A implementação de sistemas de gestão de qualidade e segurança da informação aportam benefícios para as organizações

H5: Os processos de certificação garantem maior reconhecimento às empresas

H6: A adoção dos requisitos das normas ISO, contribuem para a robustez do controlo interno

H7: A auditoria é importante para todo o processo de implementação das ISO

4.3. Método de pesquisa e de recolha dados

O método adotado para a pesquisa centrou-se na revisão da literatura, enquanto que a recolha de dados se processou através de questionários.

A revisão da literatura ou revisão teórica, é o ponto de partida para a generalidade dos estudos. Isto porque permite, ter contacto com o que já foi escrito sobre o tema e assim acrescentar novos conceitos e opiniões ao estudo em causa.

A importância desta revisão é demonstrada por Ciribelli (2003, p.88) ao afirmar que

> deve conter informações atuais sobre a problemática a ser estudada, razão pela qual se torna muito importante para o pesquisador […] porque o auxilia a definir com precisão o objeto da sua investigação, e também lhe mostra se a pesquisa que realiza pode trazer uma nova contribuição para o conhecimento.

Esta revisão permite estabelecer uma hipótese geral, que pode originar diversas outras hipóteses e diferentes métodos de investigação. Conjugando os métodos de investigação com as hipóteses, e recolhendo dados que são posteriormente analisados, são obtidos resultados que originam conclusões. Estas conclusões comprovam a literatura estabelecida desde o início, e assim desta forma é evidenciada a importância que este passo tem, em qualquer estudo. Na Figura 4.1 abaixo, são demonstrados os diversos passos de uma investigação.

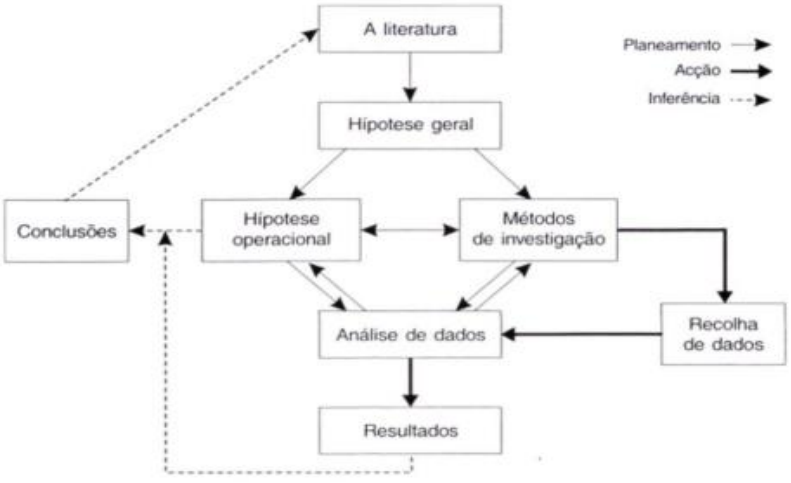


Figura 4.1. Investigação Empírica

Fonte: Hill, M.M. & Hill, A. (2008, p.32)

Após a revisão teórica, é então necessário proceder à recolha de dados. Segundo Roegiers & Ketele (1998), existem 4 métodos de recolha de dados sendo eles:

- ✓ Entrevistas
- ✓ Observação
- ✓ Questionários
- ✓ Estudo de documentos

Tal como referido anteriormente, a presente investigação terá como método de recolha de dados os questionários. Os questionários são instrumentos que permitem a recolha de informação através de um conjunto de questões sobre o tema em estudo.

O objetivo ao realizar questionários, é o de «[…] obter, de maneira sistemática e ordenada, a informação acerca da população que se estuda, das variáveis que são objeto do estudo.» (Vilelas, 2009, p.315).

De acordo com Marconi & Lakatos (2003), existem diversas vantagens e desvantagens associadas a este tipo de instrumento. Como vantagens, podem ser descritas as seguintes:

- Atinge um maior número de pessoas simultaneamente;
- Obtém respostas rápidas e precisas;
- Maior liberdade e fiabilidade quando se recorre ao anonimato;
- Menor risco de distorção da informação, pela não influencia do investigador;
- Há mais uniformidade na avaliação, em virtude da natureza impessoal dos questionários.

Por outro lado, as desvantagens podem ser:

- Não devolução dos questionários;
- Possibilidade de existirem perguntas sem respostas;
- Dificuldade de compreensão, por parte dos participantes que pode influenciar as suas respostas.

De forma a avaliar as respostas dadas, será utilizada a escala de Likert. Para Cunha (2007, p.24), esta escala «[…] é composta por um conjunto de frases (itens) em relação a cada uma das quais se pede ao sujeito que está a ser avaliado para manifestar o grau de concordância […]».

Aquando a criação de uma escala de Likert, devem ser tidos em conta segundo Boone & Boone (2012, p.2) «[…] *a series of four or more Likert-type items that are combined into a single composite score/variable during the data analysis process. Combined, the items are used to provide a quantitative measure of a character or personality trait.* »

Inicialmente, a escala original incluía uma escala de cinco pontos, variando entre a discordância total até a concordância total. (Silva, 2014)

Neste tipo de escala, é dada a oportunidade ao inquirido de selecionar a opção central de indiferente ou sem opinião, ao contrário de escalas com quatro itens, o que obriga o inquirido a uma escolha positiva ou negativa, uma vez que a opção central não existe.

O presente estudo contará com escalas de 5 pontos e com escalas de 4.

4.4. Estrutura do inquérito

O questionário é composto por um conjunto de questões fechadas das quais fazem parte, questões de escolha múltipla e escalas de avaliação em que o inquirido será confrontado com diferentes alternativas de resposta devendo apenas escolher uma das que lhe são apresentadas.

A estrutura do inquérito é constituída por um total de 11 questões, sendo que as 3 primeiras dizem respeito à caracterização dos inquiridos relativamente à função que desempenham na empresa assim como o tempo de permanência na mesma, sendo que esta última questão será determinante e influenciará a ordem do preenchimento dos questionários. Isto porque de acordo com o tempo de permanência na empresa, o inquirido pode ou não ter acompanhado o processo de implementação das ISO, o que é determinante para a questão seguinte onde é possível separar os colaboradores que acompanharam dos demais.

Assim seguem-se 3 questões, que apenas podem ser respondidas pelos inquiridos que acompanharam o processo, onde o objetivo é o de averiguar a importância que a auditoria interna teve no processo, se serviu como uma preparação à intervenção externa e foi eficiente

e como se sentiriam os colaboradores se tal auditoria não tivesse sido realizada. Por último, neste grupo de questões é avaliado o papel da auditoria externa que conduziu á certificação.

De seguida, são apresentadas 2 questões de escalas de avaliação, onde todos os inquiridos podem dar o seu contributo, uma vez que à medida que vão entrando na empresa, é feito no acolhimento ao novo colaborador, uma breve apresentação de todas as mudanças pelo qual a empresa passou. Desta forma e estando todos familiarizados com as normas em questão, o objetivo é saber quais os benefícios e limitações que podem ser observados no decorrer do dia a dia.

Posteriormente, é colocada uma questão que permite averiguar se na opinião do inquirido, todo este processo que levou à certificação garantiu à empresa um maior reconhecimento. A escala de Likert adotada até aqui, segue uma variação de 5 pontos permitindo aos inquiridos optarem por uma posição mais neutra.

Por fim, as duas últimas questões, permitem classificar se a adoção de procedimentos, políticas, manuais e outros documentos que acompanharam a implementação das ISO, contribuiu para a robustez do controlo interno da organização e questão 11 que encerra o questionário, onde é sintetizado o papel que as auditorias realizadas durante o processo tiveram na organização Ao contrário das questões anteriores, a escala utilizada nestas 2 questões varia entre 1 e 4, de modo a limitar as respostas dos inquiridos, sem a posição de indiferença, uma vez que estas permitirão ir de encontro às questões que guiaram a presente investigação. Deste modo, considerou-se importante, os inquiridos focarem-se numa das respostas que efetivamente leva a conclusões mais robustas.

4.5. Descrição da amostra

A amostra alvo da presente investigação, serão os colaboradores das diversas áreas que compõem a Empresa X com o objetivo de obter uma visão mais alargada dos procedimentos aplicados. As áreas em questão serão, os recursos humanos, a contabilidade em regime insourcing e outsourcing, o finance, o departamento administrativo-financeiro e o tax.

4.6. Procedimento para a recolha de dados e tratamento da informação

O questionário foi realizado via online sendo apresentado o âmbito do estudo a efetuar, seguido de uma breve mensagem de agradecimento pela colaboração prestada, garantindo o anonimato das respostas e a utilização dos dados apenas para fins académicos.

A recolha dos dados teve início no dia 1 de março de 2019 através do envio por correio eletrónico da hiperligação do questionário, para o universo populacional exigível na organização, que conta com cerca de 60 colaboradores.

No dia 26 de abril de 2019, data que estabeleceu o término da recolha de dados, foram obtidas 60 respostas.

Relativamente ao tratamento da informação, a análise estatística proporciona uma maior precisão e rigor, bem como uma maior clareza e confiança na análise dos resultados do estudo. Posto isto, para a análise dos dados recolhidos, utilizou-se as ferramentas disponibilizadas pelo Microsoft Office Excel (tabelas de suporte e gráficos de linhas, barras e circulares) bem como as ferramentas de análise de dados e construção gráfica disponibilizadas pela plataforma na qual os inquéritos foram realizados.

Para verificar a concordância ou não das hipóteses formuladas, a análise das respostas pode ser uni variada ou multivariada. Paes (2010) caracteriza-as da seguinte forma:

- Análise uni variada - em que a variável poderá ser analisada separadamente admitindo que não existe qualquer relação com outra variável;
- Análise multivariada - em que duas ou mais variáveis em estudo poderão ou não apresentar uma relação entre si, originando determinados acontecimentos.

5. Recolha e análise de dados

O capítulo da recolha e análise de dados, será dividido em 2 partes. A primeira, terá como objetivo analisar os dados que resultaram dos questionários, por meio de gráficos e tabelas permitindo verificar as hipóteses anteriormente formuladas, comprovando-as ou não. A segunda parte, contará com a inventariação dos procedimentos e políticas implementadas no decorrer do processo, com o intuito de apresentar as alterações que daí resultaram.

Para uma melhor compreensão e análise dos dados recolhidos, será disponibilizado no Apêndice 1 o questionário realizado, enquanto que as respostas dos inquiridos serão partilhadas no Apêndice 2 que poderão ser repartidas para uma melhor visualização.

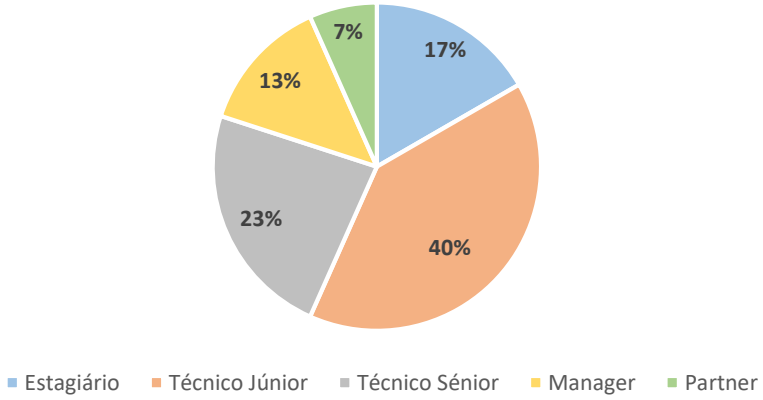
5.1. Caracterização da amostra

Na investigação realizada, a caracterização dos inquiridos será feita tendo por base as primeiras três questões apresentadas no questionário. Esta caracterização assenta nos seguintes critérios:

- Função desempenhada
- Tempo de permanência na empresa
- Se esteve presente na implementação das normas

No que respeita à primeira questão, e como se pode constatar no Gráfico 5.1, 17% exercem a função de estagiário correspondendo a 10 inquiridos, 40% e ocupando assim a maior percentagem dos inquiridos estão os técnicos juniores correspondendo a 24 colaboradores, 23.33% exercem a função de Técnico Sénior num total de 14 colaboradores, 13.33% ocupam a posição de Manager correspondendo a 8 inquiridos e por fim 6.67% dizem respeito a Partners correspondendo a um total de 4 colaboradores.

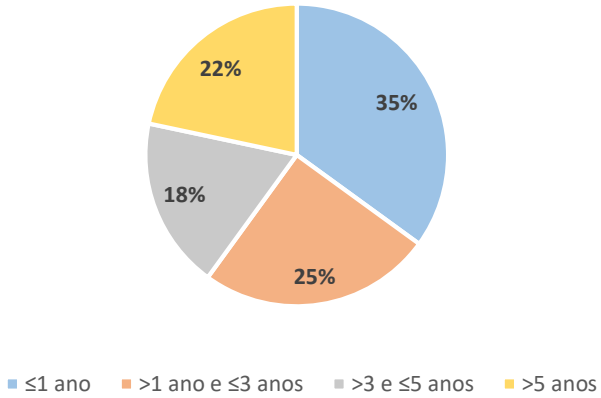
Gráfico 5.1. Distribuição dos inquiridos por função desempenhada



Fonte: Elaboração própria a partir dos dados do inquérito

No que respeita ao tempo de permanência na organização, pode verificar-se no Gráfico 5.2 que a grande maioria dos inquiridos, 21 correspondem a uma percentagem de 35% são colaboradores que estão na empresa há menos de 1 ano. Estes valores podem ser explicados pelo crescimento que empresa tem tido nos últimos tempos. De seguida, observa-se que entre 1 a 3 anos estão 25% que correspondem a um total de 15 inquiridos. Esta percentagem é seguida de perto pelos colaboradores que estão há mais de 5 anos representando 22% da amostra. Por fim, encontram-se os colaboradores cujo tempo de permanência se situa entre os 3 e os 5 anos perfazendo 18%.

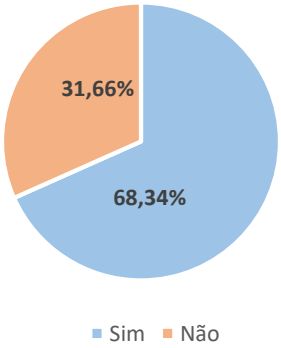
Gráfico 5.2. Distribuição dos inquiridos em função do tempo de permanência na organização



Fonte: Elaboração própria a partir dos dados do inquérito

Por último, e dando início à separação dos colaboradores que acompanharam a implementação das ISO, dos que apenas vêm as consequências da obtenção da certificação no dia a dia, encontra-se o gráfico 5.3, onde é possível observar que maior parte dos inquiridos, representados por 68,34% estiverem presentes desde o início do processo e que os restantes 31,66% não. Estas percentagens, correspondem a 41 e 19 colaboradores respetivamente. Assim sendo e nas 3 próximas questões, apenas foram obtidas respostas dos 41 inquiridos.

Gráfico 5.3. Distribuição dos inquiridos consoante o acompanhamento da implementação



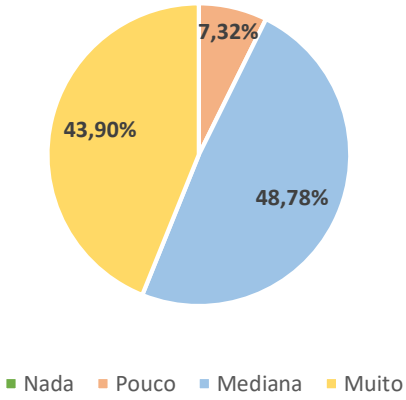
Fonte: Elaboração própria a partir dos dados do inquérito

5.2. Análise dos resultados ao questionário

5.2.1. De uma auditoria interna adequada resultam colaboradores preparados

A questão 4 pretendia avaliar se a auditoria interna realizada como preparação à auditoria externa foi útil e adequada para os colaboradores se sentirem preparados. Como se pode observar no Gráfico 5.4., a maioria dos colaboradores, cerca de 49% respondeu mediana. Seguida de perto pela opção muito com apenas 5% a menos. No que concerne aos colaboradores que consideraram pouco útil e adequada a intervenção interna, representam um total de 3 colaboradores a que corresponde 7%. Por fim, é possível analisar que a opção nada não foi selecionada por nenhum dos inquiridos.

Gráfico 5.4. Distribuição dos inquiridos consoante a importância da auditoria interna



Fonte: Elaboração própria a partir dos dados do inquérito

A equipa de auditoria interna da Empresa X, foi composta por colaboradores independentes das áreas a auditar, após a realização de diversas formações para que reunissem todos os conhecimentos e capacidades para puderem executar os objetivos a que foram propostos.

É possível observar que a maioria da amostra, considera que a atuação da auditoria interna foi relevante para a preparação dos colaboradores face à auditoria externa. Sendo a auditoria interna uma área de análise, verificação das atividades e da eficácia e conformidade das operações é importante que a sua performance seja vista como uma aliada na precursão dos objetivos, neste caso avaliar se as operações desenvolvidas pelas diversas áreas da organização estão em conformidade com o que é suposto. Tendo cerca de 93% confirmado que foi de certa forma útil e adequada, é admissível afirmar que os objetivos propostos inicialmente à auditoria interna foram de alguma forma cumpridos, na visão dos inquiridos.

Assim a maioria dos colaboradores considera que esta auditoria conseguiu avaliar os procedimentos aplicados e a sua conformidade com o que é preconizado nas normas a implementar, a exatidão e segurança não só da informação como a dos restantes ativos, a organização e ação dos auditores para chegarem a toda as áreas com o devido conhecimento.

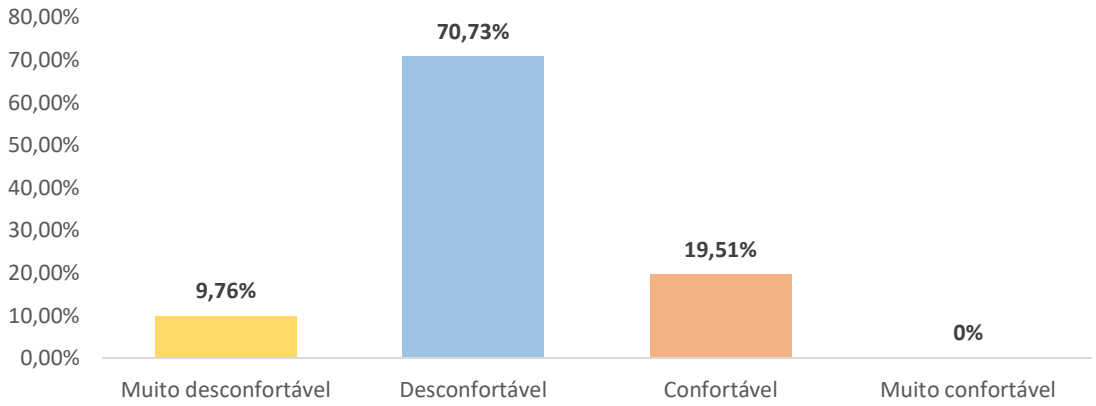
Contudo, 7% dos colaboradores concluiu que a auditoria interna foi pouco importante na preparação dos colaboradores. Uma das razões que podem justificar esta opinião por parte dos inquiridos, são a existência de conflitos de interesse pessoal pelo facto de os auditores serem parte integrante da mesma organização, pondo em causa a transparência que é exigida, assim como a recetividade em ouvir e compreender a execução das atividades dos auditores.

Outra das razões poderá ter sido a extensão da análise às políticas e procedimentos e ainda os recursos disponibilizados para realizar a auditoria interna.

5.2.2. Na ausência de uma auditoria interna derivam colaboradores desconfortáveis

A questão 5, tinha como objetivo determinar o impacto que a ausência da auditoria interna teria nos colaboradores. Pelo Gráfico 5.5., pode concluir-se que nenhum dos inquiridos se sentiria muito confortável para prosseguir para auditoria externa, sem a auditoria interna. De seguida, surge a opção de muito desconfortável com uma percentagem de 9.76% dos inquiridos. A maioria dos colaboradores, num total de 29 dos 41 que responderam, iriam sentir-se desconfortáveis originando 70.73%, enquanto que 19.51% dos inquiridos sentir-se-ia confortável caso a auditoria interna não tivesse intervindo na preparação para o restante processo.

Gráfico 5.5. Distribuição dos inquiridos consoante o impacto perante a ausência da auditoria interna



Fonte: Elaboração própria a partir dos dados do inquérito

Para a auditoria interna, foram selecionados por departamento 2 colaboradores para uma análise mais pormenorizada enquanto que os restantes foram observando e puderam sentir o impacto das conclusões a que os auditores chegaram. Assim sendo, é de esperar que o impacto nos colaboradores que foram selecionados tenha sido maior e por isso na ausência da auditoria interna, sentir-se-iam mais desconfortáveis. A maioria dos restantes

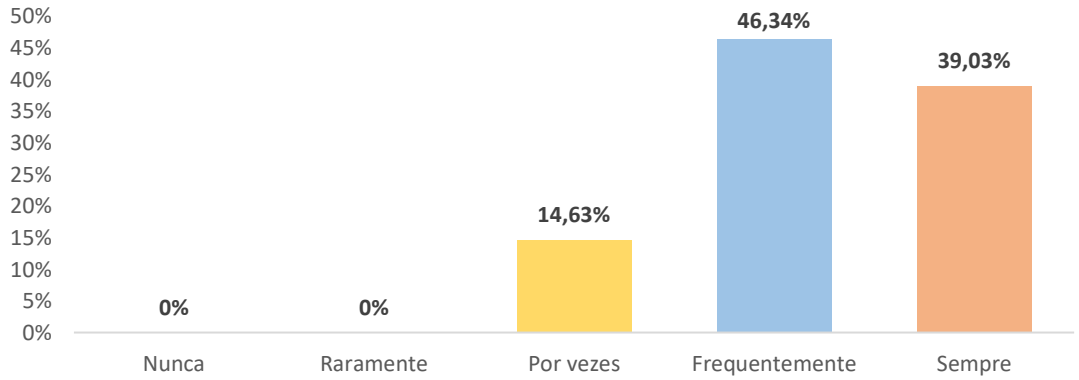
colaboradores, declarou que sem a intervenção dos auditores internos, iriam enfrentar a auditoria externa de forma mais desconfortável na medida que com esta análise inicial foram indicadas quais as não conformidades e quais os aspetos que poderiam ser melhorados de forma a ir de encontro ao estabelecido nas normas ISO.

Por outro lado, os 19.51% que se sentiriam confortáveis sem a auditoria interna, podem em parte remeter para os colaboradores em regime de outsourcing que no decorrer da auditoria não puderam estar presentes aquando a realização da mesma ou ainda e consultando o Apêndice 2 Tabela 1 e 2 para colaboradores com cargos mais elevados e por isso mais preparados para o processo.

5.2.3. A auditoria externa é vista como útil aos processos de implementação das ISO

A questão 6, pretendia determinar se a auditoria externa foi apropriada ao fim em vista, ou seja, avaliar o papel que a mesma teve no processo. Pelo Gráfico 5.6., observa-se que nenhum dos inquiridos que acompanharam a implementação das ISO, considerou que a auditoria externa foi nunca ou raramente inapropriada. Posto isto, as respostas dos inquiridos recaem sobre as restantes 3 opções. Com apenas 14,63%, 6 dos 41 inquiridos sentiu por vezes a necessidade da auditoria externa. De seguida, apresenta-se a opção sempre, que registou uma percentagem de 39,03%, refletindo que uma grande parte dos colaboradores não teve dúvidas quanto ao papel da auditoria externa na persecução dos objetivos. Por fim, a maioria dos colaboradores, afirmou que a atuação dos auditores externos e todas as suas atividades, foram frequentemente importantes assim a sua utilidade no processo.

Gráfico 5.6. Distribuição dos inquiridos consoante a importância da auditoria externa



Fonte: Elaboração própria a partir dos dados do inquérito

A auditoria externa foi realizada por uma empresa de certificação, a EIC. Esta auditoria, como dito anteriormente, tinha como objetivo avaliar a conformidade das operações e atribuir a certificação à empresa no caso de estarem a agir em conformidade com as ISO em questão. A atuação da auditoria externa compreendeu todas as áreas de negócio da empresa e contou com o apoio da auditoria interna, que após a realização das suas atividades, permitiu apresentar uma organização bastante preparada para as suas análises. Daqui se destaca mais uma vez, o papel que a auditoria interna teve, não só na preparação dos colaboradores, como também nos procedimentos e processos implementados, que permitiram aumentar a eficácia e eficiência em toda a organização.

A auditoria externa exerceu as suas atividades durante cerca de uma semana, e decorreu não só nas instalações da empresa como também nas instalações de alguns clientes, sendo estes últimos, clientes em regime de outsourcing, na qual se fizeram acompanhar pelos colaboradores responsáveis por esses mesmos clientes. Desta forma, a extensão dos trabalhos foi maior pois permitiu avaliar os trabalhos desenvolvidos na empresa e ainda os desenvolvidos nas imediações dos clientes.

Realizando todas as etapas do processo, como descrito no subcapítulo da certificação, a empresa conseguiu obter a certificação nos dois sistemas de gestão que pretendia, o da qualidade e o da segurança da informação. Desta forma, ficou claro para todos os envolvidos que a opção nunca e raramente não se aplicou em nenhuma circunstância, ou seja, a auditoria externa foi de alguma forma apropriada e uma fonte de apoio em todo o processo.

De entre as restantes opções, a resposta por vezes foi a que registou uma menor preferência. Embora em menor valor, esta escolha pode ser justificada pelos colaboradores de outsourcing que não foram selecionados para a auditoria e, portanto, não acompanharam os trabalhos dos auditores.

Segue-se a opção sempre que com cerca de 39,03%, demonstra que para estes inquiridos, a auditoria externa foi apropriada e imprescindível neste tipo de implementações, pois sem eles não era possível obter o certificado nem garantir que a organização se encontra de acordo com o que é preconizado nas normas. Esta opção, indica ainda que o apoio prestado pelos auditores foi de encontro ao esperado, assim como os seus objetivos e funções traçadas.

Por último, a maioria dos inquiridos respondeu frequentemente. Embora não seja a opção mais elevada, esta percentagem é bastante motivadora porque retrata que a auditoria externa

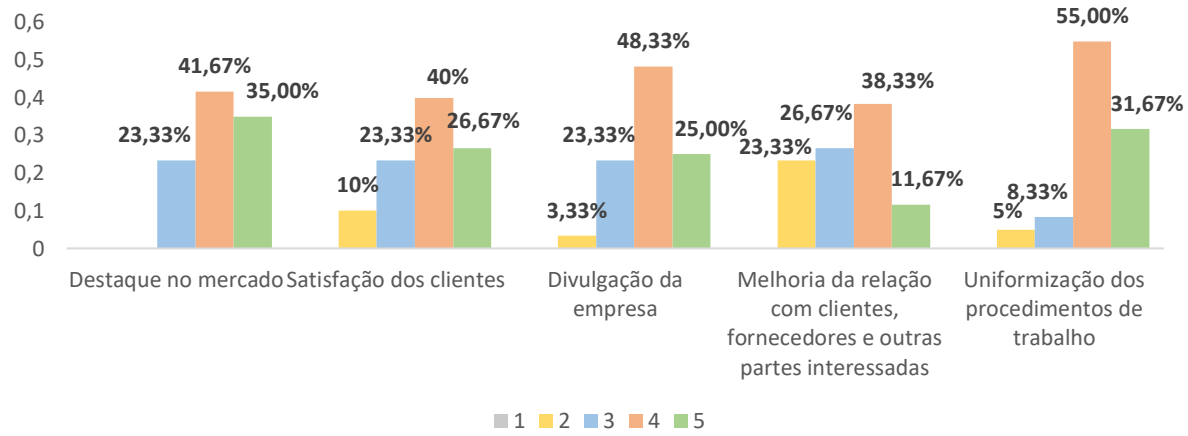
foi útil para a maioria dos colaboradores. No entanto, o que pode ter decretado maior afluência no frequentemente invés da opção sempre, pode prender-se com o distanciamento entre os auditados e os auditores, que pode levar a desconfiança e a uma incorreta interpretação da postura do auditor. Tal como referido anteriormente, o auditor deve ser entendido como um aliado no alcance dos objetivos e não como um mero avaliador. No entanto, é importante referir que o conhecimento e experiência vinda do exterior são sempre uma mais valia que se traduzem não só em novas perspetivas como também em maior credibilidade perante terceiros. Assim sendo, e combinando as duas respostas mais aclamadas, é possível comprovar a H3 na medida em que a auditoria externa foi apropriada e útil no processo de implementação das ISO.

5.2.5. A implementação de sistemas de gestão de qualidade e segurança da informação aporta benefícios para as organizações

De forma a validar ou não a H4, os inquiridos foram confrontados com diversos benefícios que resultam da implementação dos sistemas referidos, com o objetivo de avaliarem segundo a escala de Likert de 1 a 5 mencionada anteriormente, cujos significados são 1 – Discordo totalmente, 2- Discordo, 3 – Sem opinião, 4 – Concordo, 5 – Concordo totalmente. A análise desta hipótese será feita com o tempo de permanência e não com a posição ocupada na entidade porque mesmo que o inquirido ocupe uma posição alta na organização, mas estiver há pouco tempo na organização, pode não ser capaz de identificar os benefícios como outros cuja posição seja inferior, mas que estejam na organização há mais tempo.

Assim, o Gráfico 5.7.1. apresenta a distribuição de inquiridos segundo o primeiro conjunto de benefícios. Como pode ser observado, a opção concordo foi a que registou maior preferência entre os inquiridos, e registou-se uma grande dispersão na maioria dos benefícios retratados. As percentagens dos inquiridos sem opinião também registaram valores significativos, assim como o concordo totalmente. Nenhum dos benefícios aqui apresentados, mereceu discórdia total.

Gráfico 5.7. Distribuição dos inquiridos consoante os benefícios da implementação (I)



Fonte: Elaboração própria a partir dos dados do inquérito

Para melhor compreensão da distribuição acima, segue-se a Tabela 5.1. onde são cruzadas as respostas dadas ao tempo de permanência na empresa com os níveis de 1 a 5 atribuídos a cada benefício apresentado.

Tabela 5.1. Relação entre o tempo de permanência na empresa e os benefícios da implementação (I)

		Destaque no mercado	Satisfação dos clientes	Divulgação da empresa	Melhoria da relação com clientes, fornecedores e outras partes interessadas	Uniformização dos procedimentos de trabalho	Total
≤ 1ano	2	0	1	2	3	0	6
	3	6	5	8	10	2	31
	4	9	9	8	6	13	45
	5	6	6	3	2	6	23
>1 ano e ≤3 anos	2	0	3	0	4	2	9
	3	3	6	4	5	1	19
	4	6	5	6	5	9	31
	5	6	1	5	1	3	16
>3 e ≤5 anos	2	0	2	0	2	0	4
	3	4	3	2	1	2	12
	4	5	3	5	5	5	23
	5	2	3	4	3	4	16
>5 anos	2	0	0	0	5	2	7
	3	1	0	0	0	0	1
	4	5	7	10	7	6	35
	5	7	6	3	1	5	22

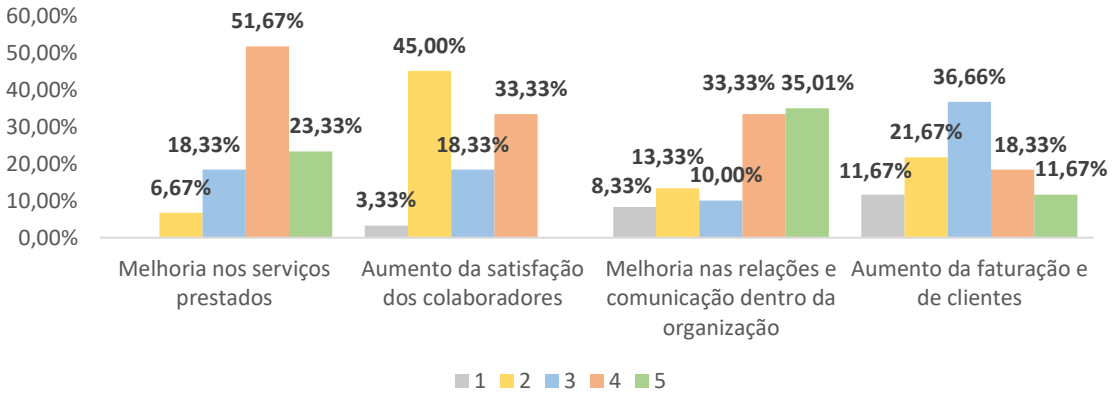
Fonte: Elaboração própria a partir dos dados do inquérito

Conforme se pode observar, para os 4 intervalos de tempo avaliados, a opção mais escolhida foi o nível 4 ou seja o nível de concordância, não registando por isso grandes discrepâncias.

Destes benefícios, resultou a opção 2 em 8.66%, a opção 3 em 21%, a opção 4 em 44,67 % e por último a opção 5 em 25.67%, comprovando que de entre os 5 benefícios apresentados, os inquiridos na sua maioria comprovam que provêm da implementação dos SGQ e SGSI.

O Gráfico 5.7.2. apresenta a distribuição de inquiridos de acordo com o segundo conjunto de benefícios. É possível constatar que os valores mais significantes se deram ao nível do concordo, na melhoria dos serviços e o discordo na satisfação dos colaboradores. Já os últimos dois benefícios, registaram uma maior proximidade de valores, assim como todas as opções foram merecedoras de seleção por parte dos inquiridos.

Gráfico 5.8. Distribuição dos inquiridos consoante os benefícios da implementação (II)



Fonte: Elaboração própria a partir dos dados do inquérito

Para melhor compreensão da distribuição acima, segue-se a Tabela 5.2. onde são cruzadas as respostas dadas ao tempo de permanência na empresa com os níveis de 1 a 5 atribuídos a cada benefício apresentado.

Tabela 5.2. Relação entre o tempo de permanência na empresa e os benefícios da implementação (II)

		Melhoria dos serviços prestados	Aumento da satisfação dos colaboradores	Melhoria nas relações e comunicação dentro da organização	Aumento da faturação e de clientes	Total
≤ 1ano	1	0	1	1	2	4
	2	2	6	2	3	13
	3	4	6	4	14	28
	4	12	8	6	2	28
	5	3	0	8	0	11
>1 ano e ≤3 anos	1	0	0	0	3	3
	2	2	9	6	4	21
	3	3	3	1	6	13
	4	7	3	4	2	16
	5	3	0	4	0	7
>3 e ≤5 anos	1	0	1	0	1	2
	2	0	7	2	4	13
	3	2	1	2	1	6
	4	6	2	4	3	15
	5	3	0	3	2	8
>5 anos	1	0	0	0	1	1
	2	0	5	0	2	7
	3	2	1	1	3	7
	4	6	7	6	4	23
	5	5	0	6	3	14

Fonte: Elaboração própria a partir dos dados do inquérito

Este conjunto de benefícios verificou como se pode constatar, uma maior divergência de opiniões. Os colaboradores cujo tempo se situa nos> 5 anos focaram a sua maioria na opção 4, assim como os colaboradores com >3 e ≤5 seguida de perto pela opção 2. Já os que se situam no tempo < 1 ano igualaram a sua opinião na opção 3 e 4 e os com 1 a 3 anos optaram pelo nível da discórdia.

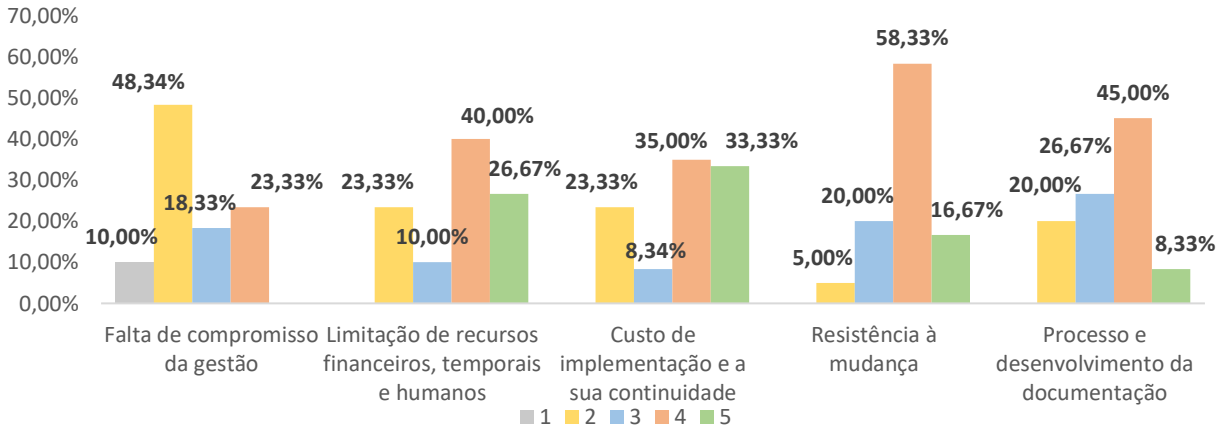
Cruzando esta informação com o Gráfico 5.7.2., o benefício melhoria nos serviços prestados destaca-se pelo nível 4 em todos os tempos de permanência. O aumento da satisfação dos colaboradores tem como maioria o nível 2, em que os maiores contribuidores foram os que estão na empresa há >1 ano e ≤5 anos e, portanto, tem uma clara perceção se tal aumento se verificou, afirmando que não. O benefício melhoria nas relações e comunicação dentro da organização, teve a sua maioria registada no nível 5, sendo que os maiores contribuidores foram os com tempo >5 anos que ocupando maioritariamente posições mais elevadas na organização têm maior capacidade de avaliar as relações e comunicação estabelecida, e os

com ≤ 1ano que à medida que entram, são introduzidos com formações e explicações sobre como funciona a organização.

De acordo com a revisão da literatura, a implementação destes sistemas aporta geralmente benefícios conforme validado acima, mas também limitações. Desta forma, a questão 8 tinha como prepósito averiguar quais as resultam desta mesma implementação.

O Gráfico 5.8.1. apresenta a distribuição de inquiridos segundo as primeiras 5 limitações avaliadas, das quais se pode constatar uma grande variedade nas opções selecionadas, destacando-se o discordo para a falta de compromisso da gestão e o concordo para as restantes.

Gráfico 5.9. Distribuição dos inquiridos consoante as limitações sentidas na implementação (I)



Fonte: Elaboração própria a partir dos dados do inquérito

Para melhor compreensão da distribuição acima, segue-se a Tabela 5.3. onde são cruzadas as respostas dadas ao tempo de permanência na empresa com os níveis atribuídos a cada limitação apresentada.

Tabela 5.3. Relação entre o tempo de permanência na empresa e as limitações da implementação (I)

		Falta de compromisso da gestão	Limitação de recursos financeiros, temporais e humanos	Custo de implementação e a sua continuidade	Resistência à mudança	Processo e desenvolvimento da documentação	Total
≤ 1ano	1	1	0	0	0	0	1
	2	9	3	4	3	4	23
	3	7	3	4	5	10	29
	4	4	8	7	10	5	34
	5	0	7	6	3	2	18
>1 ano e ≤3 anos	1	2	0	0	0	0	2
	2	5	4	5	0	3	17
	3	2	2	0	2	2	8
	4	6	7	3	10	9	35
	5	0	2	7	3	1	13
>3 e ≤5 anos	1	1	0	0	0	0	1
	2	6	4	4	0	2	16
	3	2	1	1	3	4	11
	4	2	4	4	7	5	22
	5	0	2	2	1	0	5
>5 anos	1	2	0	0	0	0	2
	2	9	3	1	0	2	15
	3	0	0	0	2	1	3
	4	2	5	7	8	8	30
	5	0	5	5	3	2	15

Fonte: Elaboração própria a partir dos dados do inquérito

Conforme se pode observar, para os 4 intervalos de tempo avaliados, a opção mais escolhida foi o nível 4. Destas limitações, resultou a opção 1 em 2%, a 2 em 23.67%, a opção 3 em 17%, a opção 4 em 40,33 % e por último a opção 5 em 17%.

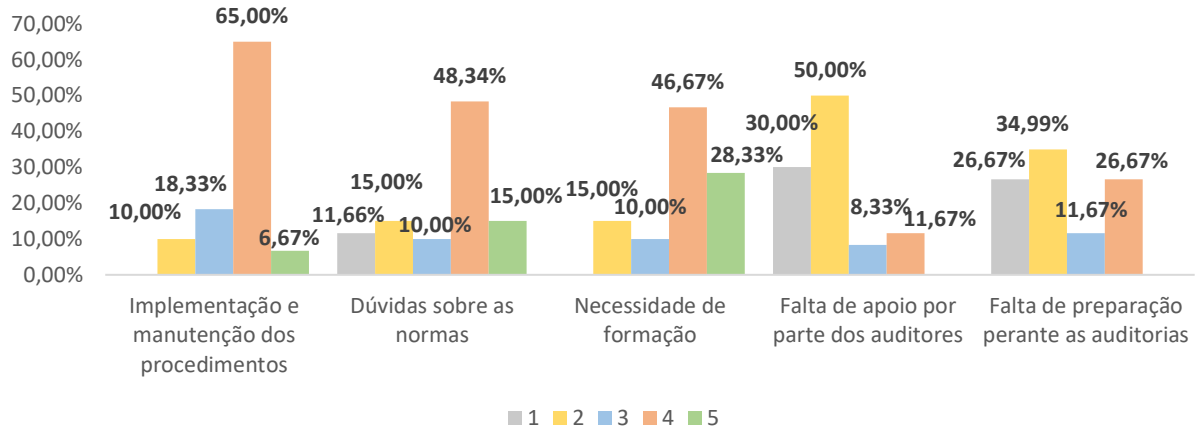
À exceção da falta de compromisso da gestão, as restantes tiveram na sua maioria selecionado o nível de concordância, comprovando a sua origem na implementação dos SGQ e SGSI.

Cruzando esta informação com o Gráfico 5.8.1, a falta de compromisso da gestão levou à discórdia por parte dos inquiridos, sendo a sua maioria colaboradores com tempo ≤ 1ano e >5 anos. As 4 restantes limitações, tiveram resultados semelhantes sendo que os maiores contribuidores, foram aqueles cujo tempo de permanência se encontra compreendido entre ≤1 ano e ≤3 anos.

O Gráfico 5.8.2. apresenta a distribuição de inquiridos perante o segundo conjunto de limitações. Tal com se pode observar, houve maior convergência ao nível do concordo, para

as 3 primeiras limitações apresentadas, enquanto que as últimas duas se centraram no discordo.

Gráfico 5.10. Distribuição dos inquiridos consoante as limitações sentidas na implementação (II)



Fonte: Elaboração própria a partir dos dados do inquérito

Para melhor compreensão da distribuição acima, segue-se a Tabela 5.4. onde são cruzadas as respostas dadas ao tempo de permanência na empresa com os níveis atribuídos a cada limitação apresentada.

Tabela 5.4. Relação entre o tempo de permanência na empresa e as limitações da implementação (II)

		Implementação e manutenção dos procedimentos	Dúvidas sobre as normas	Necessidade de formação	Falta de apoio dos auditore	Falta de preparação perante as auditorias	Total
≤ 1ano	1	0	1	0	6	9	16
	2	4	3	1	8	3	19
	3	6	1	3	5	6	21
	4	9	11	12	2	3	37
	5	2	5	5	0	0	12
>1 ano e ≤3 anos	1	0	3	0	2	1	6
	2	0	3	6	8	6	23
	3	1	2	1	1	1	6
	4	13	7	6	4	7	37
	5	1	0	2	0	0	3
>3 e ≤5 anos	1	0	2	0	4	3	9
	2	1	1	0	6	6	14
	3	2	1	5	0	0	8
	4	8	5	5	1	2	21
	5	0	2	1	0	0	3
>5 anos	1	0	1	0	6	4	11
	2	1	2	3	6	6	18
	3	2	2	4	0	0	8
	4	9	6	5	1	3	24
	5	1	2	1	0	0	4

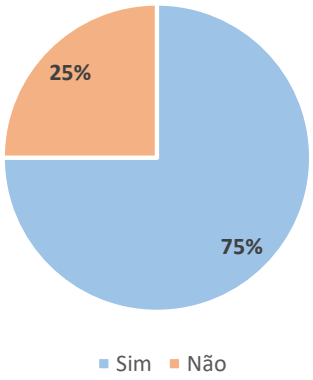
Fonte: Elaboração própria a partir dos dados do inquérito

Conforme se pode observar, para os 4 intervalos de tempos avaliados, a opção mais escolhida foi o nível 4. Cruzando esta informação com o gráfico 5.8.2. obtém-se que a implementação e manutenção dos procedimentos alcançou o nível de concordância, registando maior contribuição dos colaboradores com tempo entre >1 ano e ≤3 anos, que na sua maioria são técnicos juniores e lidam diariamente com os processos que sofreram alteração. As dúvidas sobre as normas advêm na sua maioria pelos colaboradores mais recentes que não se sentem ainda familiarizados com as mesmas assim como a menor frequência de formações quando comparados aos restantes. A falta de apoio dos auditores e dificuldade perante as auditorias não foi na sua maioria sentida, dando por isso origem ao nível 2, não fazendo parte das limitações sentidas na implementação dos sistemas. Estas vão de encontro às questões 4, 5 e 6 do presente questionário, onde ficou comprovado que quer os auditores quer as auditorias realizadas foram essenciais a este processo.

5.2.7. Os processos de certificação garantem maior reconhecimento às empresas

A questão 9 tinha como objetivo validar se a certificação, conferiu ou não maior reconhecimento à empresa. Como se pode observar pelo Gráfico 5.9., 75% representando 45 inquiridos respondeu que a implementação com sucesso destes sistemas, permite hoje em dia um maior reconhecimento do que anteriormente. Pelo contrário, 25% discorda que a adoção das normas e a sua conformidade comprovada pela certificação obtida, confira mais reconhecimento.

Gráfico 5.11. Distribuição dos inquiridos consoante o reconhecimento conseguido após a certificação



Fonte: Elaboração própria a partir dos dados do inquérito

Os valores que constam do gráfico acima, são semelhantes à percentagem de inquiridos que acompanharam todo o processo, 41, dos demais 19, sendo as percentagens de 68,33% e 31,66% respetivamente. Esta relação aqui estabelecida, pode ser evidenciada na Tabela 5.5. abaixo onde são apresentadas as respostas a esta questão de acordo com o acompanhamento feito.

Tabela 5.5. Relação entre o acompanhamento dos inquiridos e a opinião sobre a certificação

Nº. Inquiridos	Sim	Não
41	37	4
19	8	11
60	**45**	**15**

Fonte: Elaboração própria a partir dos dados do inquérito

Desta forma, pode concluir-se que os inquiridos que acompanharam todo o processo, tiveram uma maior tendência para afirmar que a empresa é hoje mais reconhecida e apenas destes, 4 optaram pela resposta não. Estes 4 representam técnicos juniores com tempo de permanência > 1 ano e ≤3 anos.

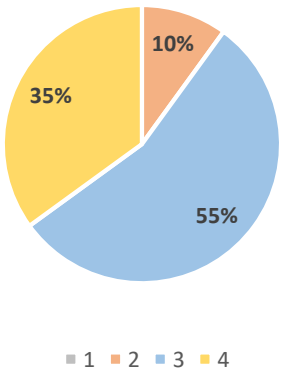
O mesmo se segue para os 19 inquiridos que não acompanharam o processo desde o seu início, em que o não alcançou a maioria e os 8 que afirmaram sim, incluem um manager, técnicos juniores e estagiários.

Assim pode concluir-se que o tempo de permanência e por conseguinte a perceção de todas as alterações e melhorias está implicitamente ligada ao reconhecimento que se considera dado. Para os que não acompanharam todo o processo e, portanto, não puderam assistir às alterações, há um menor valor atribuído a um possível reconhecimento.

5.2.8. A adoção dos requisitos das normas ISO, contribuem para a robustez do controlo interno

Esta questão servia o prepósito de avaliar como a adoção de procedimentos, políticas, manuais e outros documentos decretados pelas ISO, são facilitados pelo controlo interno existente na organização e a sua contribuição para a robustez do mesmo. Através do Gráfico 5.10. é possível observar que numa escala de 1 a 4, cujos significados são 1 – Nada importante, 2- Pouco importante, 3- Importante e 4- Muito importante, a maioria com 55% apontou um 3 como tendência, seguida por 35% que optaram por um 4. Contudo, a resposta 2 foi também selecionada por uma amostra inferior, indicando que as novas implementações foram pouco importantes para a robustez do controlo interno.

Gráfico 5.12. Distribuição dos inquiridos consoante as melhorias no controlo interno



Fonte: Elaboração própria a partir dos dados do inquérito

Aquando a decisão de iniciar o processo de adoção das normas ISO, surgiu a necessidade de elaborar diversos documentos como manuais, políticas, procedimentos entre outros, permitindo uniformizar as tarefas e melhorar a comunicação e funcionamento da empresa indo de encontro aos requisitos das normas.

No que respeitas às políticas, foram introduzidas 4 novas políticas que definem a classificação da informação, a encriptação, o abate de equipamento informático e papel e os backups. Relativamente aos processos adotados, foram incluídos processos sobre a contabilidade, o finance, a gestão administrativa de recursos humanos, o tax, os recursos humanos, a gestão e melhoria, o design e desenvolvimento e o comercial. Já os procedimentos incluíram, o controlo de documentos e registos, o contacto com as autoridades e entidades, a segurança operacional, a gestão de incidentes, não conformidades e ações corretivas, os fornecedores, a auditoria interna, a identificação de requisitos legais e metodologia de avaliação e tratamento de riscos e oportunidades. Por último, foram introduzidos 5 manuais que esclarecem as funções da contabilidade, dos recursos humanos, administrativo e financeiro, as viaturas e as boas práticas.

A distribuição das respostas dadas, pode analisar-se segundo a posição que os colaboradores ocupam na organização. Assim, segundo a Tabela 5.6. é possível esta mesma distribuição.

Tabela 5.6. Relação entre a função desempenhada e a contribuição do controlo interno

	2	**3**	**4**
Estagiário	3	3	4
Técnico Júnior	3	12	9
Técnico Sénior	0	10	4
Manager	0	5	3
Partner	0	3	1

Fonte: Elaboração própria a partir dos dados do inquérito

Como se pode observar, as posições hierárquicas mais elevadas desde o Técnico Sénior ao Partner não classificaram como pouco importante a adoção dos vários procedimentos, processos entre outros documentos no impacto do controlo interno, e focaram a sua preferência no importante. Já os Estagiários e Técnicos Juniores, originaram uma maior dispersão, chegando mesmo a classificar como pouco importante o impacto no controlo

interno, o que pode estar relacionado com o intervalo de permanência na organização ser reduzido. A diferença encontrada entre a escolha do nível 3 para o nível 4, pode ser justificada pelo facto de terem sido selecionados alguns colaboradores de entre as posições mais elevadas para que colaborassem na elaboração dos documentos, atribuindo por isso a máxima importância ou ainda pelo facto de serem alterações recentes e não estarem ainda totalmente operacionais.

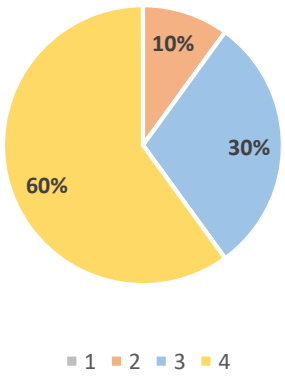
5.2.9. A auditoria é importante para todo o processo de implementação das ISO

A última questão do presente questionário, tinha como objetivo resumir perante todos os inquiridos, e não apenas os acompanharam desde início o processo, qual a importância que as auditorias de implementação e de acompanhamento têm quando se adota as normas ISO. As respostas dadas, incidiram sobre um dos objetivos na qual se centra a presente investigação.

As primeiras auditorias quer a interna, quer a externa realizaram-se em junho de 2018 pelo que nem todos puderam acompanhá-las como dito anteriormente. Contudo, em abril do presente ano deu-se o início da preparação para as auditorias de acompanhamento, pelo que à data de aplicação dos questionários, aqueles que não puderam ver iniciado o processo, puderam observar as auditorias de acompanhamento e por isso classificar a sua importância.

Pelo Gráfico 5.11. é possível constatar que 60% da amostra atribuiu a classificação máxima que se fixa no nível 4, seguida pela opção 3 com valores também muito significativos na ordem dos 30% e apenas 10% à opção com valor 2.

Gráfico 5.13. Distribuição dos inquiridos consoante a importância da auditoria



Fonte: Elaboração própria a partir dos dados do inquérito

Para melhor análise desta questão, reparte-se de seguida na Tabela 5.7, os inquiridos que estão na empresa desde o início das auditorias relacionando as suas respostas à presente questão com as dadas nas questões 5 e 6. Esta relação é possível de estabelecer porque à medida que o nível das opções dadas nas questões 5 e 6 foi aumentando, verificou-se na sua maioria, uma tendência também crescente quanto à opção selecionada na presente questão.

Tabela 5.7. Relação entre as respostas dadas com as das questões 5 e 6

		2	**3**	**4**
Auditoria Interna	Nada	0	0	0
	Pouco	0	2	1
	Mediana	4	6	10
	Muito	1	3	14
Auditoria Externa	Nada	0	0	0
	Raramente	0	0	0
	Por vezes	2	3	1
	Frequentemente	1	3	15
	Sempre	2	5	9

Fonte: Elaboração própria a partir dos dados do inquérito

Relativamente à auditoria interna, conclui-se que se o inquirido determinou que esta era muito importante para o processo, houve uma maior tendência para nesta questão 11, selecionasse o nível mais elevado, neste caso 4. O mesmo se verifica para a opção mediana. Na opção Pouco, em vez de se verificar valores crescentes no número de inquiridos, verificou-se o contrário. Isto porque se o inquirido considerou pouco importante a auditoria interna na questão 5, tem maior probabilidade de no final manter valores mais inferiores perante as auditorias iniciais e as de acompanhamento.

A mesma situação ocorre na auditoria externa, se o inquirido selecionou a opção sempre ou frequentemente tem maior probabilidade de vir agora classificar a questão entre os níveis 3 e 4.

Desta análise, resultam 25 colaboradores com resposta tipo 4, 11 para a opção 3 e por último 5 colaboradores que selecionaram a 2, perfazendo o total de colaboradores que acompanharam o processo desde o início.

Focando agora a atenção para aqueles que apenas estiveram presentes nas auditorias de acompanhamento, segue-se a Tabela 5.8. onde se relacionam as respostas dadas na presente questão com as suas funções na empresa, perfazendo um total de 19 inquiridos.

Tabela 5.8. Relação entre a função desempenhada e a importância da auditoria

	2	**3**	**4**
Estagiário	1	3	4
Técnico Júnior	0	5	4
Técnico Sénior	0	0	1
Manager	0	0	1
Partner	0	0	0

Fonte: Elaboração própria a partir dos dados do inquérito

Como se pode observar quer aqui, quer no Apêndice 2 na tabela 1 e 2, nenhum dos partners está incluído nos 19. O manager e sénior que entraram recentemente, atribuíram às auditorias de acompanhamento a maior classificação permitida. Estas 2 posições, têm mais conhecimentos sobre o processo a desenvolver e mais responsabilidades em manter os sistemas a funcionar adequadamente e a controlar possíveis não conformidades. Estando mais por dentro das atividades e procedimentos, são mais propensos a classificar as auditorias como muito importantes para concluir o processo. Os estagiários e técnicos juniores, embora não estejam tão familiarizados como as posições anteriormente referidas, são incluídos quer nas formações, quer na preparação para as auditorias uma vez que a amostra definida pelos auditores internos e externos é aleatória. Pela análise do gráfico verifica-se que também optaram por as opções compreendidas entre o 3 e o 4, com a exceção de 1 colaborador que optou pela opção 2 ou seja não tao importante como as restantes.

Assim e resumindo a informação recolhida de ambas as partes, é seguro afirmar que a maioria da amostra quer tenha ou não acompanhado desde o início o processo, classifica as auditorias como fundamentais para auxiliarem não só a implementação dos sistemas de gestão abordados como também para colaborarem com a manutenção dos mesmos. No entanto 10% considerou pouco importante o que pode ser justificado com o tempo de permanência na empresa, assim como puderem ser colaboradores em regime de outsourcing que não

foram alvo da amostra dos auditores e por isso não têm uma perceção tão real das auditorias como os restantes.

5.3. Inventariação dos procedimentos e políticas implementadas no âmbito deste processo

No decorrer da implementação das normas, a Empresa X teve que elaborar certas políticas e procedimentos que fossem de encontro ao indicado nas normas e que demonstrassem perante as auditorias como toda a organização se encontrava em conformidade com as normas que desejava implementar. De seguida, são apresentadas algumas das políticas e procedimentos que daí resultaram.

- Política da Classificação da Informação

A Empresa X define informação como qualquer dado que venha a ser posto à disposição dos colaboradores ou sobre a qual estes venham a ter conhecimento ou acesso seja qual for a sua forma. Assim sendo, a classificação da informação pode ser classificada em três níveis, público, interno e confidencial.

- ✓ Público: aplicável a toda a informação, documentos, materiais de domínio público ou cuja divulgação não tem nenhum impacto no negócio da empresa. Dentro deste nível, pode encontrar-se informação pública externa como legislação, normas e regulamentos, newsletters de clientes, fornecedores e correntes ou interna como apresentações da empresa, relatórios e contas anuais, políticas e âmbito do sistema.

- ✓ Interno: aplicável à informação cuja divulgação ou conhecimento por pessoas não autorizadas têm uma probabilidade diminuta de provocar danos ou prejuízos à empresa. Dentro das instalações da empresa, esta informação estará segura através do controlo de acesso físico enquanto que fora das instalações, os equipamentos portáteis transportam a informação de modo encriptado.

- ✓ Confidencial: aplicável à informação cuja divulgação ou conhecimento por pessoas não autorizadas possa ter consequências graves ou muito graves. A sua divulgação para o exterior é proibida, exceto se aprovada pela comissão de Segurança ou pela

Gestão de Topo. Deve ser armazenada nos locais definidos na rede interna e consultada apenas pelos utilizadores autorizados. Sempre que impressa, terá que ser armazenada em locais apropriados e não deve ser exposta nas áreas de trabalho onde todos os colaboradores tenham acesso. A informação confidencial pode ter duas utilidades diferentes, interna como contratos entre a empresa e os seus colaboradores, dados pessoais ou financeiros dos seus colaboradores e clientes ou externa como é o caso de propostas, orçamentos para parceiros ou clientes e contratos entre a empresa e os seus parceiros, fornecedores ou clientes.

- Política de Encriptação

Tendo em conta a importância do SGSI, surge a necessidade de encriptar os equipamentos que contenham informação da empresa através de controlos criptográficos. A Empresa X focaliza a encriptação de discos internos e pen drives através da aplicação BitLocker. A encriptação dos discos internos é da responsabilidade do administrador do sistema, enquanto que a das pen drives que contêm informação da empresa, fica a cargo de cada colaborador. Quando ocorre a encriptação, a aplicação BitLocker cria uma chave de recuperação por equipamento, que deve ser guardada pelo administrador do sistema ou responsável do SIG numa pasta de acesso reservado. Não são autorizados outros métodos de encriptação sem o conhecimento do responsável do SIG.

- Política de Abate de Equipamento ou Papel

Sempre que o colaborador possua um equipamento móvel ou fixo, ou em suporte papel que contenha informação interna ou confidencial da empresa, e pretenda o seu abate, deve seguir certos procedimentos que assegurem a salvaguarda da informação. No caso de ser um equipamento, o suporte informático deve garantir que tal informação é eliminada e só depois o mesmo deve ser enviado para abate ou reutilização. Se a informação estiver em papel, deve ser eliminada nas destruidoras de papel que se encontram nas instalações.

- Política de Backups

Esta política defende que toda a informação disponível na rede informática, na qual estão implementadas cópias de segurança regulares que abrangem toda a estrutura de rede, devem ser salvaguardadas através de backups regulares. A Empresa X realiza backups através de um

servidor que está programado para iniciar as 21:10 de cada dia. O facto de serem feitos diariamente, aumenta a probabilidade de não ser perdida informação crucial.

- Procedimento Segurança Operacional

✓ Inserção de novos utilizadores e posterior eliminação

Quando ocorre a entrada de um novo colaborador, há que criar os acessos ao servidor e pastas de rede. O mesmo acontece com a introdução dos dados biométricos do novo colaborador para que o mesmo possa aceder às instalações da empresa. Quando ocorre a saída de algum colaborador, há que assegurar que os acessos são desativados e o material devolvido, de forma a evitar que no futuro tal colaborador possa desviar ou aceder a informação que não lhe pertence.

✓ Acesso à rede interna

O acesso à rede interna da Empresa X é efetuado via VPN, cuja configuração é da responsabilidade do administrador do sistema. Esta medida serve de combate à invasão por pessoas desconhecidas ou não autorizadas a aceder a tal informação.

✓ Antivírus

A importância de um antivírus eficiente é fundamental para impedir possíveis danificações nos equipamentos. Periodicamente devem ser efetuadas análises a todos os sistemas, para despistar eventuais ameaças sendo despoletados automaticamente pela aplicação antivírus instalada.

- Procedimento das Não Conformidades e Ações Corretivas

Uma não conformidade resulta da não satisfação de um requisito, isto é, de uma necessidade ou expetativa expressa, geralmente implícita ou obrigatória. As não conformidades são tratadas através de ações corretivas, com o objetivo de eliminar as não conformidades, incidentes ou situações indesejáveis.

Após a intervenção das auditorias, é realizada uma reunião onde são apresentadas não conformidades no caso de existirem e onde se debate as possíveis ações corretivas a

implementar pela empresa. De seguida, a auditoria deve verificar se as não conformidades foram corrigidas e se as ações corretivas surtiram efeito na eliminação das mesmas.

- Procedimento da Auditoria Interna

Como referido anteriormente, a auditoria interna serviu como uma preparação à auditoria externa relativamente aos colaboradores, aos trabalhos desenvolvidos e aos procedimentos e políticas que regem a empresa. A equipa de auditoria interna foi selecionada pela Comissão de Segurança do qual fazem parte um gerente, dois managers e a responsável pelo SIG. Para executar esta função, a equipa necessitou de ter formação em auditorias de sistemas de gestão e das normas a auditar, possuir conhecimentos sobre as outras áreas da empresa e ser independente das atividades a auditar. Meramente a título de exemplo, pode afirmar-se que os RH auditaram o DAF, o DAF auditou a contabilidade, e a contabilidade auditou os RH. No fim, a equipa auditora apresenta em reunião um relatório onde são apresentadas as principais conclusões, que após ser enviado para o responsável pelo SIG deverá tomar as medidas necessárias.

- Outras políticas e procedimentos

Como referido anteriormente, o acesso às instalações da Empresa X é feito através de dados biométricos. Todos os restantes visitantes como clientes, fornecedores, parceiros entre outros, são atendidos e reencaminhados para a sala de espera onde aguardam pelo colaborador. Esta medida permite que pessoas exteriores à organização ou à informação em questão, não tenham contacto com a mesma.

As passwords são também formas de proteger o acesso aos diversos sistemas. Por isso a empresa defende um conjunto de regras na sua criação que passam por não pode conter o nome da conta de utilizador, conter no mínimo 6 carateres com letras maiúsculas, minúsculas e números, ser obrigatoriamente, imputado pelo sistema de informação, alterada de 90 em 90 dias, não conter espaços na sua composição e não ser equivalente há palavra-passe definida anteriormente.

Os equipamentos informáticos têm uma política que faz com que o ecrã entre em suspensão após 5 minutos de inatividade, obrigando à introdução da palavra-passe para restabelecer a sessão de forma a impossibilitar o acesso não autorizado. O colaborador deve assegurar que a sua secretária se encontra organizada, ou seja, que toda a informação relevante se encontra devidamente identificada e guardada nos locais apropriados, quando a mesma não seja

necessária. O mesmo deve ocorrer quando abandona o seu posto de trabalho, ao final do dia ou por períodos alargados de tempo. Relativamente ao *software* e demais aplicações, estas só devem ser instaladas após validação e aprovação, garantindo que estas estão em conformidade com as normas legais em vigor.

Face a estas medidas introduzidas na organização, verifica-se um aumento na robustez do controlo interno da organização, pois embora tenham sido adotadas para que a empresa X estivesse em conformidade com o que era exigido, estas políticas, procedimentos e outros documentos permitiram melhorar as ações dos colaboradores e a forma como realizam as suas funções na empresa

Desta forma e uma vez alcançada a certificação comprovando a conformidade da empresa, o controlo interno foi tal como a auditoria um pilar importante neste processo, da qual se puderam observar sinergias.

6. Conclusões

6.1. Síntese e contribuições do estudo

A qualidade e a segurança da informação têm ganho especial importância, com o decorrer dos anos devido às necessidades e exigências do mercado, dos clientes e de outras partes interessadas. Face a tais necessidades, as empresas têm vindo a adotar cada vez mais, sistemas que transmitam a máxima confiança no funcionamento das suas operações. Embora sejam necessárias diversas fases, têm-se verificado aumentos graduais nos certificados emitidos aos SGQ e SGSI, o que demonstra que as empresas vêm reconhecido o valor de possuírem qualidade e segurança nos seus negócios.

Tendo presente o acima exposto, desenvolveu-se a presente investigação com o objetivo de estudar o papel que as auditorias e o controlo interno detêm nestes processos assim como as sinergias resultantes das normas ISO com as componentes do controlo interno. Para tal, foram formuladas diversas hipóteses que através das respostas dadas pelos inquiridos da investigação contribuíram para a fundamentação do estudo.

Relativamente à importância da auditoria, foram abordadas as duas auditorias que incitaram o processo, a auditoria interna e externa, as suas funções e objetivos, os benefícios e as limitações a elas associadas. Sobre a auditoria interna, as suas funções centraram-se na preparação dos colaboradores e na verificação das atividades por eles realizadas de forma a avaliar a eficácia e conformidade das mesmas, identificando sempre que possíveis aspetos a melhorar. A cooperação entre os auditores internos e externos foi visível desde o início, otimizando desta forma os recursos e a informação existente. Concluiu-se, com base nas respostas dos inquiridos que a maioria, de uma forma quase unanime, considerou a auditoria interna útil para preparar os colaboradores, comprovando assim a hipótese formulada.

Quando questionados sobre a hipótese de não ter havido qualquer atuação por parte da equipa de auditoria, a maioria sentir-se-ia desconfortável. Assim sendo, é também destacado como importante o papel desta auditoria, dado todo o trabalho realizado, desde a identificação de não conformidades aos aspetos que poderiam ser melhorados antes da intervenção da auditoria externa.

Concluiu-se que a auditoria externa, executada pela entidade certificadora, foi fundamental para avaliar as áreas da empresa e determinar se esta estava ou não a agir em conformidade

com as normas que desejava adotar. A hipótese que se pretendia validar remetia para a utilidade da intervenção desta auditoria neste tipo de processos.

As respostas dos inquiridos centraram-se nas opções do frequentemente e sempre, deixando claro que nenhum considerou que a auditoria externa foi nunca ou raramente importante. De certo, as atividades exercidas pela auditoria externa, levaram a modificações em toda a estrutura da organização, com a obtenção do certificado nos dois sistemas de pretendidos, o da qualidade e o da segurança da informação, confirmando desta forma o papel desempenhado por esta auditoria na adoção das ISO.

Decorrido aproximadamente um ano, deu-se início à preparação para as auditorias de acompanhamento onde todos os inquiridos puderam classificar a importância das auditorias. A análise que proveio da última hipótese estabelecida desta questão, permitiu concluir que os colaboradores com posições mais elevadas na organização, e, portanto, mais familiarizados com a importância de todas as partes na persecução dos objetivos atribuídos a este processo, destacam as auditorias como muito importantes. Efetivamente, estes detêm mais conhecimentos sobre o processo a desenvolver e mais responsabilidades no que concerne a manter os sistemas a funcionar adequadamente e como ir de encontro ao que é exigido pelos auditores. No que diz respeito aos estagiários e aos técnicos juniores, optaram na sua maioria por atribuir também importância às auditorias realizadas.

Desta forma conclui-se, que quer as auditorias internas e externas iniciais ou as de acompanhamento, são fundamentais para a implementação dos SGQ e SGSI, não só pela preparação dos colaboradores e das alterações nas formas de trabalho no que diz respeito à auditoria interna, como também à auditoria externa que permitiu conduzir a organização no alcance dos objetivos das ISO a adotar, e por fim as de acompanhamento que englobando novamente auditorias internas e externas possibilitaram comprovar que a empresa X se mantém dentro dos parâmetros definidos e por isso conseguiu renovar o certificado emitido pela empresa certificadora.

No que concerne aos benefícios que tais sistemas aportam, e relacionando os retratados na revisão da literatura com os que foram alvo de avaliação no questionário, conclui-se que a uniformização dos procedimentos trabalho e a melhoria dos serviços prestados foram alguns dos benefícios que mereceram maior destaque pelos inquiridos. Este benefício, adicionado à proteção da informação e da qualidade conseguida, permite concluir, por conseguinte, que

os serviços foram de alguma forma melhorados, sendo visível para a maioria dos inquiridos. A uniformização dos procedimentos garantiu que toda a organização operasse com base nos mesmos procedimentos e políticas, eliminando de forma significativa diferenças que existiam entre equipas. Dos benefícios retratados, apenas 2 não foram de encontro a hipótese formulada, sendo eles o aumento na satisfação dos colaboradores e o aumento da faturação, cujos motivos podem estar relacionados com a resistência à mudança e o facto de nem todos terem acesso à faturação da empresa.

Tendo em conta a possibilidade de existirem limitações, estiveram em análise 10 limitações resultantes deste tipo de processo conforme abordado na revisão da literatura e concluiu-se que a resistência à mudança e a implementação e manutenção dos procedimentos a foram algumas das dificuldades que mais registaram preferência pelos inquiridos. As mudanças resultantes deste processo, são visíveis nas tarefas realizadas e na forma de atuar da organização, sendo por isso expectável as percentagens elevadas que se verificaram nos questionários. Já a implementação e manutenção dos procedimentos, dependem não só da gestão, mas também do empenho de todos em aceitar e manter os procedimentos implementados. Das limitações retratadas, 3 não foram consideradas limitações neste processo, como a falta de apoio da gestão, a falta de apoio dos auditores e a falta de preparação para as auditorias.

Relativamente ao reconhecimento da empresa, pela adoção das normas e a sua conformidade comprovada pela certificação obtida, concluiu-se que a maioria dos inquiridos, considera que a empresa é hoje mais reconhecida do que no início do processo. Verificou-se ainda uma relação entre a opinião dada e a presença dos inquiridos nas fases percorridas, onde os inquiridos que acompanharam todo processo têm uma maior inclinação para atribuir reconhecimento à empresa, e os restantes centraram-se de maior forma na não obtenção de maior reconhecimento.

No que concerne ao controlo interno, e tendo por base as sinergias retratadas na revisão teórica entre as diversas componentes do modelo COSO com os diversos requisitos das ISO 9001 e 27001., foi possível observá-las no decorrer do processo. Cada um dos princípios das 5 componentes do controlo interno encontraram correspondência com os requisitos das normas, dando assim resposta a uma das perguntas que guiou esta investigação. De certo, diversas foram as políticas, procedimentos, manuais e outros documentos criados para ir de encontro não só às normas como também para fazer face às exigências dos auditores,

validando assim a robustez do CI e a importância que um SCI tem numa organização e em processos como este.

6.2. Limitações

Uma das limitações que em regra geral costuma ser constatada, é o facto de inquérito por questionário ser enviado com recurso ao correio eletrónico, pois muitos dos destinatários que visualizam a mensagem, não chegam a responder originando reduzidas taxas de resposta. Por forma a contrair esta limitação, foram disparados emails que serviram como lembretes a cada semana com o objetivo de não caírem em esquecimento por parte dos inquiridos. Estes emails surtiram efeito pelo que no período de 2 meses foram recebidos todos os questionários enviados.

O horizonte temporal para recolha de dados pode também representar uma limitação. Isto porque, se o tempo disponível para resposta tivesse sido inferior, os inquiridos poderiam ter-se sentido mais pressionados para que o preenchimento dos questionários fosse feito de imediato. Contudo houve necessidade de delimitar a fase de recolha de dados para um período de 2 meses, na esperança de alcançar com sucesso a totalidade da amostra.

6.3. Sugestões para futuras investigações

Uma sugestão para futuras investigações passa por estender a investigação a outras empresas, por forma a garantir a obtenção de resultados mais aprofundados, recorrendo por exemplo a plataformas como o Linkedin ou ao website de empresas do mesmo setor.

Para além disto, sugere-se ainda, consultar de forma mais pormenorizada os auditores internos, os auditores externos e ainda alguns dos fornecedores e clientes mais importantes de forma a avaliar qual a sua perspetiva sobre todo o processo.

Referências Bibliográficas

António, N.S., Teixeira, A. & Rosa, A. (2016). *Gestão da Qualidade – de Deming ao Modelo de Excelência da EFQM*. Lisboa: Edições Sílabo. ISBN: 978-972-618-854-4

APCER, A. P. (2010). *Guia Interpretativo NP EN ISO 9001:2008*. Porto: APCER. Consultado a 10 de novembro de 2018. Disponível em http://www.esac.pt/noronha/G.Q/apontamentos/Guia_9001_2008_APCER.pdf 11/11

APCER, A. P. (2015). *Guia Interpretativo NP EN ISO 9001:2015*. Porto: APCER. Consultado a 10 de novembro de 2018. Disponível em https://www.apcergroup.com/portugal/images/site/graphics/guias/APCER_GUIA_ISO 9001_2015.pdf

Attie, W. (1992). *Auditoria Interna*. São Paulo: Editora Atlas S.A. ISBN: 85-224-0199-3

Bailey, E. & Becker, J. (2014). *A Comparison of IT Governance and Control Frameworks in Cloud Computing*. Paper apresentado na Twentieth Americas Conference on Information Systems, Savannah. Consultado a 30 de novembro de 2018. Disponível em https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1160&context=amcis2014

Bell, J. (1993). *Como Realizar um Projeto de Investigação – Um Guia para a Pesquisa em Ciências Socias e da Educação* (5ªed). Lisboa: Gradiva. ISBN: 978-972-662-524-7

Boone, H. N. & Boone, D.A. (2012). Analyzing Likert Data. *Journal of Extension*, 2 (50), 2-3. Consultado a 4 de abril de 2019. Disponível em file:///C:/Users/Proprietario/Downloads/JOE_v50_2tt2likertanalysisimp.pdf

Brito, T.F.C. (2015). *Tecnologias de Informação de Suporte à Auditoria* (Dissertação de mestrado, Universidade Autónoma de Lisboa, Lisboa, Portugal. Consultado a 6 de dezembro de 2018. Disponível em

http://repositorio.ual.pt/bitstream/11144/2398/1/Trabalho%20Final%20Mestrado%20-%2002-10-2015%20-%20versaofinal.pdf

Calder, A. (2009) *Information Security based on ISO 27001/ISO 27002 - A Management Guide.* Zaltbommel: Van Haren Publishing. ISBN: 978-908-753-540-7

Canto, A. C. (2010). *Um estudo de caso em jardins públicos da Cidade da Praia* (Trabalho Científico, Universidade de Cabo Verde, Cidade da Praia, Cabo Verde). Consultado a 20 de outubro de 208. Disponível em http://portaldoconhecimento.gov.cv/bitstream/10961/2011/1/final%20cristina.pdf

Carneiro, A. (2004) *Auditoria de Sistemas de Informação* (2ª ed). Lisboa: FCA. ISBN: 978-972-722-436-4

Carneiro, A. (2009). *Auditoria e Controlo de Sistemas de Informação*. Lisboa: FCA. ISBN: 978-972-722-407-4

Carneiro, A. (2016). *Auditoria e Controlo de Sistemas de Informação*. Lisboa: FCA. ISBN: 978-972-722-407-4

Carneiro, S.E.S.M. (2013). *Quais os atributos que um auditor interno deve ter* (Dissertação de Mestrado). Instituto Superior de Contabilidade e Administração do Porto, Porto. Consultado a 15 de dezembro de 2018. Disponível em http://recipp.ipp.pt/bitstream/10400.22/1840/1/DM_SilviaCarneiro_2013.pdf

Casaca, J.A.A. (2010). *Um modelo integrado para a gestão da segurança da informação nas pequenas e médias empresas portuguesas* (Tese de Doutoramento). Universidade Lusíada de Lisboa, Lisboa, Portugal. Consultado a 7 de dezembro de 2018. Disponível em http://repositorio.ulusiada.pt/bitstream/11067/2820/1/dg_joaquim_casaca_tese.pdf

Ciribelli, M. C. (2003). *Como Elaborar uma Dissertação de Mestrado através da pesquisa científica*. Consultado a 20 de outubro de 2018. Retirado de https://books.google.pt/books?id=3haJdQ9KRLEC&pg=PA88&dq=revisao+da+literatura&hl=pt-PT&sa=X&ved=0ahUKEwihw9CFvLDcAhUMElAKHTy-Al0Q6AEINDAD#v=onepage&q=revisao%20da%20literatura&f=false

Correia, C. M. (2016). *Plano de Implementação da Norma ISO/IEC 27001:2013 na organização INEM* (Dissertação de Mestrado). Universidade Nova de Lisboa, Lisboa, Portugal. Consultado a 11 de novembro de 2018. Disponível em https://run.unl.pt/bitstream/10362/19605/1/TGI0069.pdf

COSO (1994). *Internal Control – Integrated Framework*. Consultado a 25 de novembro de 2018. Disponível em http://www.academia.edu/12912529/INTERNAL_CONTROL_INTEGRATED_FRAMEWORK_Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission

COSO (2013). *Internal Control – Integrated Framework*. Consultado a 25 de novembro de 2018. Disponível em https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

Costa, C.B. (2010). *Auditoria Financeira-Teoria & Prática* (9ªed). Lisboa: Letras e Conceitos Lda. ISBN 978-989-830-584-8

Costa, C. B. (2014) *Auditoria Financeira – Teoria & Prática*. Lisboa: Rei dos Livros

Cruz, C.V & Carvalho, O. (1994). *Qualidade – Uma Filosofia de Gestão* (2ªed). Lisboa: Texto Editora. ISBN 978-972-470-391-6

Cruz, C. & Carvalho, Ó. (1998). *Qualidade uma Filosofia de Gestão* (3ªed). Lisboa: Texto Editora

Cunha, L.M.A. (2007). *Modelos Rasch e Escalas de Likert e Thurstone na medição de atitudes* (Dissertação de Mestrado). Faculdade de Ciências e Tecnologia, Lisboa, Portugal. Consultado a 4 de abril de 2019. Disponível em https://repositorio.ul.pt/bitstream/10451/1229/1/18914_ULFC072532_TM.pdf

Druker, P. (1993). *As Fronteiras da Gestão* (2ªed). Lisboa: Editorial Presença

EIC. *Certificação*. Consultado a 16 de dezembro de 2018. Disponível em http://eic.pt/certificacao/

Ernest & Young (2010). *Improving internal controls: the Ernest & Young guide for humanitarian aid organizations*. Consultado a 29 de novembro de 2018. Disponível em https://www.ey.com/Publication/vwLUAssets/ey-improving-internal-controls-overview/$FILE/ey-improving-internal-controls-overview.pdf

Fernandes, D.J. (2016). *Implementação da NP EN ISO 9001:2015 na Indústria da Torrefação* (Dissertação de Mestrado). Faculdade Ciências e Tecnologia, Lisboa, Portugal. Consultado a 15 de novembro de 2018 Disponível em https://run.unl.pt/bitstream/10362/22172/1/Fernandes_2016.pdf

Ferreira, H.A. (2009). *Auditoria de Segurança de Informação*. Consultado a 7 de dezembro de 2018 Disponível em https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14E01F8FC014E02CA0C3626DE

Fonseca, L. (2016). *ISO 9001:2015 & ISO 14001:2015 – Processo de transição*. Consultado a 2 de março de 2019. Disponível em https://www.ipmaia.pt/pt/eventos_/Documents/2016/05-OpenWeekend/Qualidade/Lu%C3%ADs_Fonseca_APQ.pdf

Furtado, D. (2009). *Auditoria Interna e Suas Vantagens*. Consultado a 2 de outubro de 2018 Disponível em http://www.administradores.com.br/informe-se/artigos/auditoriainterna-e-suas-vantagens/30910

Gil, A.L. (1999). *Auditoria da Qualidade* (3ªed). São Paulo: Atlas, S.A. ISBN 85-224-2279-6

Hammar, M. (2015). *First-, Second- & Third-Party Audits, what are the differences?*. Consultado a 30 de novembro de 2018 Disponível em https://advisera.com/9001academy/blog/2015/02/24/first-second-third-party-audits-differences/

Hill, M. M. & Hill, A. (2008). *Investigação por Questionário* (2ª Ed). Lisboa: Edições Sílabo. ISBN: 978-972-618-273-3

Hintzbergen, J., Hintzbergen, K., Smulders, A. & Baars, H. (2010). *Fundamentos de Segurança de Informação*. Consultado a 23 de novembro de 2018 Disponível em https://books.google.pt/books?id=1CVFDwAAQBAJ&printsec=frontcover&dq=iso+27001&hl=pt-PT&sa=X&ved=0ahUKEwi085HHleneAhWMKMAKHf2_BhEQ6AEIKzAA#v=onepage&q=iso%2027001&f=false

Juran, J.M. & Godfrey, A.B. (1998). *Juran's Quality HandBook* (5ªed). New York: McGraw-Hill Education. Consultado a 26 de novembro de 2018. Disponível em http://dump.bitcheese.net/files/yhyjyvy/juran.pdf 8/11

Inácio, H.C. (2014). *Controlo Interno: Enquadramento teórico e aplicação prática*. Lisboa: Escolar Editora. ISBN 978-972-592-454-9

INTEGRITY (s.d.). *ISO 27001 – Sistema de Gestão de Segurança da Informação*. Consultado a 25 de novembro de 2018. Disponível em https://www.27001.pt/index.html

International Navigation Association (1999). *Environmental Management Framework for Ports and Related Industries*. Consultado a 9 de dezembro de 2018 Disponível em https://books.google.pt/books?id=oe6nQVje7QkC&pg=PA35&dq=External+audit+disadvantages&hl=pt-BR&sa=X&ved=0ahUKEwi33v7fu5PfAhUDxxoKHeLkCCUQ6AEIKDAA#v=onepage&q=External%20audit%20disadvantages&f=false

IPAI (2008). Auditoria Interna – Situação e Perspetivas. *III Fórum de Auditoria Interna*, 30, 5-6.

IPAI (2009). *Enquadramento Internacional de Práticas Profissionais de Auditoria Interna*. Consultado a 20 de outubro de 2018. Disponível em http://www.ipai.pt/fotos/gca/ippf_2009_port_normas_0809_1252171596.pdf

IPQ (2013). *NP ISO/IEC 27001: Tecnologia de Informação – Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação*. Caparica: Instituto Português da Qualidade

IPQ (2015). *Norma Portuguesa Sistemas de Gestão da Qualidade Requisitos (ISO 9001:2015)*. Consultado a 15 de outubro de 2018. Disponivel em http://www1.ipq.pt/PT/site/clientes/pages/documentViewer.aspx?ctx=&local=Internet&documentId=IPQINTER-380-156960&tipoSubscricao=1

ISACA. *What is COBIT?*. Consultado a 4 de abril de 2019. Disponível em http://www.isaca.org/COBIT/pages/cobit-5.aspx

ISO (2015). *Quality Management Principles*. Consultado a 10 de novembro de 2018 Disponível em https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/pub100080.pdf

ISO. *ISO 9001 Quality management*. Retirado de https://www.iso.org/iso-9001-quality-management.html

ISO. *ISO/IEC 27001:2013*. Retirado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO. ISO SURVEY. Consultado a 11 de novembro de 2018. Disponível em https://www.iso.org/the-iso-survey.html.

Kerlinger (1973). *Metodologia da Pesquisa em Ciências Sociais*. São Paulo: EPU

Kosutic, D. (2016). *Secure & Simple – A Small Business Guide to Implementing ISO 27001 On Your Own*. Zabreg: EPPS Service Ltd ISBN 978-953-57452-5-9. Consultado a 24 de novembro de 2018. Disponível em https://books.google.pt/books?id=j6Q7DwAAQBAJ&printsec=frontcover&dq=iso+27001&hl=pt-PT&sa=X&ved=0ahUKEwi085HHleneAhWMKMAKHf2_BhEQ6AEIdDAJ#v=onepage&q&f=false

Leal, R. (2016). *Como integrar os frameworks COSO, COBIT e ISO 27001*. Consultado a 29 de novembro de 2018. Disponível em https://advisera.com/27001academy/pt-br/blog/2016/10/11/como-integrar-os-frameworks-coso-cobit-e-iso-27001/

Lopes, A. & Capricho, L. (2007). *Gestão da Qualidade*. Lisboa: Edições Silabo. ISBN 978-972-8871-13-0

Marconi, M. A. & Lakatos, E.M. (2003). *Fundamentos da metodologia científica*. Consultado a 20 de outubro de 2018. Disponível em https://pt.slideshare.net/raianacansianlima/lakatos-marconi-fundamentos-de-metodologia-cientifica-46401881

Marques, M. (1997). *Auditoria e Gestão* (1ªed). Lisboa: Editorial Presença. ISBN :978-972-232-151-8

Marques, D. A. (2013). *Implementação de um sistema de controlo interno numa escola de ensino profissional* (Dissertação de Mestrado). Escola Superior de Gestão de Tomar, Tomar, Portugal. Consultado a 20 de novembro de 2018. Disponível em https://comum.rcaap.pt/bitstream/10400.26/5860/1/Corrigida_Tese.pdf

Marra, E. & Franco, H. (2001). *Auditoria Contábil*. São Paulo: Atlas ISBN 8522429863

Martins, A.P. (2007). ISO 27001 – *Segurança da Informação – Vital para a Competitividade da sua Organização*. Consultado a 18 de novembro de 2018. Disponível em http://cosi.centimfe.com/apresentacoes/DECSIS-ISO27001.pdf

Martins, I. (2013). *Auditoria dos Sistemas de Informação das Instituições Financeiras* (Dissertação de Mestrado). Instituto Superior de Contabilidade e Administração, Lisboa, Portugal. Consultado a 6 de dezembro de 2018. Disponível em https://repositorio.ipl.pt/bitstream/10400.21/3487/1/Disserta%C3%A7%C3%A3oFinal.pdf

Moeller, R. R. (2008). *Sarbanes – Oxley Internal Controls: Effective Auditing with AS5, Cobit and ITIL*. New Jersey: John Wiley & Sons, Inc. ISBN 978-04-470-17092-2

Monteiro, A.M. (2015). *A Avaliação do Sistema de Controlo Interno: o contributo do auditor externo e o seu papel na gestão empresarial* (Relatório de Estágio de Mestrado). Faculdade de Economia do Porto, Porto. Consultado a 27 de novembro de 2018. Disponível em https://repositorio-aberto.up.pt/bitstream/10216/80559/2/36588.pdf

Morais, G. & Martins, I. (2013). *Auditoria Interna Função e Processo*. Lisboa: Áreas Editora ISBN 978-989-8058-81-2

Oliveira, I.T. (2013). *Auditoria Interna e Externa – Uma Perspetiva de Complementaridade* (Trabalho para a obtenção de Licenciatura). Consultado a 30 de novembro de 2018. Disponível em https://www.passeidireto.com/arquivo/44996894/auditoria-interna-e-externa--uma-perspetiva-de-complementaridade

Oliveira, J. A. (2006). *Método de Auditoria a Sistemas de Informação*. Porto: Porto Editora. ISBN 978-972-0-45021-0

Oliveira, R.M. (2015). *Contribuição para a estruturação do sistema integrado de gestão do grupo Cooprofar-Medlog com integração da gestão de segurança da informação* (Dissertação de Mestrado). Universidade Lusiada, Lisboa, Portugal. Consultado a 19 de novembro de 2018. Disponível em http://repositorio.ulusiada.pt/bitstream/11067/2161/2/megi_rui_oliveira_dissertacao.pdf

Osório, P.J. R. (2014). *A relação entre a acreditação/certificação da qualidade e o controlo interno nas organizações* (Dissertação de Mestrado). Instituto Superior de Contabilidade e Administração

do Porto, Porto, Portugal. Consultado a 24 de novembro de 2018. Disponível em https://recipp.ipp.pt/bitstream/10400.22/5153/1/DM_Pedro_Os%C3%B3rio_2014.pdf

Paes, A.T. (2010). *Por dentro da estatística.* Consultada a 20 de fevereiro de 2019. Disponível em http://apps.einstein.br/revista/arquivos/PDF/1595-EC_v8n1p1-2.pdf

Peláez, I. G. (2011). Análisis comparativo de los sistemas de control interno y de calidad, Auditoría y gestión de los fondos públicos. *Auditoria Pública*, n.º 54. pp. 11-31. Consultado a 26 de novembro de 2018 Disponível em http://asocex.es/wp-content/uploads/PDF/Pag11-31%20n%C2%BA%2054.pdf

Perdigão, M.L.B.V. (2016). *Gestão da Qualidade nas Organizações Sociais - Impactos da Implementação da Norma ISO 9001*. Universidade Lusófona de Humanidades e Tecnologias, Lisboa, Portugal. Consultado a 11 de novembro de 2018. Disponível em http://recil.grupolusofona.pt/bitstream/handle/10437/7339/Disserta%C3%A7%C3%A3o%20%20%26%20Apendices.pdf?sequence=1

Pinheiro, J.L. (2008). *Auditoria Interna – Auditoria Operacional - Manuel Prático para Auditores Internos*. Lisboa: Rei dos Livros ISBN: 978-972-51-1137-6

Pires, A.R (2004). *Qualidade* (3ªed). Lisboa: Edições Silabo. ISBN: 978-972-618-333-4

Pires, A.R. (2007). *Qualidade - sistemas de gestão da qualidade* (3ªed). Lisboa: Edições Sílabo.

Pires, A.R. (2016). *Sistemas de Gestão de Qualidade – Ambiente, Segurança, Responsabilidade Social, Industrial e Serviços* (2ªed). Lisboa: Edições Silabo. ISBN: 978-972-618-864-3

Ponte, J. P. (2006). *Estudos de caso em educação matemática*. Consultado a 20 de outubro de 2018. Disponível em http://repositorio.ul.pt/bitstream/10451/3007/1/06-Ponte%28BOLEMA-Estudo%20de%20caso%29.pdf

Quality Management System (2018). *O ciclo PDCA aplicado as normas ISO*. Consultado a 25 de maio de 2019. Disponível em http://www.qmsbrasil.com.br/blog/o-ciclo-pdca-aplicado-normas-iso/

Quivy, R. & Campenhoudt, L. V. (2005). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva. ISBN: 978-972-662-275-8

Ribeiro, S. I. M. C. P. (2012). *Os benefícios e as dificuldades na certificação da qualidade Norma NP EN ISO 9001:2008* (Dissertação de Mestrado). Instituto Superior de Contabilidade e Administração do Porto, Porto, Portugal. Consultado a 7 de novembro de 2018. Disponível em http://recipp.ipp.pt/bitstream/10400.22/638/1/DM-SandraRibeiro_2012.pdf

Rivas, F. G.P. (1989). *Estruturas Organizativas e Informação na Empresa*. Lisboa: Domingos Barreira

Roegiers, X. & Ketele, J. (1998). *Metodologia da Recolha de Dados*. Lisboa: Piaget ISBN: 9789727710744

Sampaio, P. (2008). *Estudo do fenómeno ISO 9000: origens, motivações, consequências e perspetivas* (Tese de Doutoramento). Escola de Engenharia, Universidade do Minho, Portugal. Consultado a 12 de novembro de 2018. Disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/8840/1/Tese_PhD_Set2008.pdf

Sampaio, P. (2017). *Quality in the 21st Century*. Consultado a 24 de novembro de 2018. Disponível em http://siq.se/content/uploads/Sampaio_ASQ-Sweden2017.pdf

Santana, C.L.A. (2014). *Estratégias na Implementação da norma ISO 9001 em IPSS* (Dissertação de Mestrado). Escola Superior de Turismo e Tecnologia do Mar, Peniche, Portugal. Consultado a 6 de novembro de 2018. Disponível em https://www.iconline.ipleiria.pt/bitstream/10400.8/2044/11/Tese%20-%20Estrat%C3%A9gias%20na%20implementa%C3%A7%C3%A3o%20da%20norma%20ISO%209001%20em%20IPSS.pdf

Sequesseque, M.T.M. (2017). *O Impacto da Implementação de Segurança da Informação na Usabilidade dos Sistemas de Informação* (Dissertação de Mestrado). Escola Superior de Ciências Empresariais, Setúbal, Portugal. Consultado a 7 de dezembro de 2018. Disponível em https://comum.rcaap.pt/bitstream/10400.26/18487/1/Disserta%C3%A7%C3%A3o-IMPACTO%20DA%20IMPLEMENTA%C3%87%C3%83O%20DE%20SEGURAN%C3%87A%20DA%20INFORMA%C3%87%C3%83O%20NA%20USABILIDADE%20DOS%20SISTEMAS%20DE%20INFORMA%C3%87%C3%83O.pdf

Serralheiro, A.R. (2017). *A complementaridade do sistema de gestão da qualidade e o controlo interno: estudo comparativo ISO e ICIF-COSO*. Consultado a 25 de novembro de 2018. Disponível em https://www.occ.pt/dtrab/trabalhos/xviicica//finais_site/230.pdf

Silva, J. (2006). *Vale a pena certificar a sua organização na ISO27001 - Segurança da Informação?*. Consultado a 5 de março de 2019. Disponível em https://www.linkedin.com/pulse/vale-pena-certificar-sua-organiza%C3%A7%C3%A3o-na-iso27001-da-julio-c/

Silva, T. M. (2013). *Impacto da auditoria interna na externa – ótica do auditor interno.* (Dissertação de Mestrado). Instituto Superior de Contabilidade e Administração de Aveiro, Aveiro, Portugal. Consultado a 30 de novembro. Disponível em https://ria.ua.pt/bitstream/10773/12107/1/8401.pdf

Silva, S. D. (2014). *Mensuração e Escalas de Verificação: uma Análise Comparativa das Escalas de Likert e Phrase Completion*. Consultado a 4 de abril de 2019. Disponível em http://sistema.semead.com.br/17semead/resultado/trabalhosPDF/1012.pdf

Strategor (1993). *Política Global da Empresa* (2ªed). Lisboa: Dom Quixote

Taborda, D. (2015*). Auditoria - Revisão Legal das Contas e Outras Funções do Revisor Oficial de Contas* (2ª Edição). Lisboa: Edições Sílabo ISBN: 9789726188070

Teixeira, M.F. (2006). *O Contributo da Auditoria Interna para Uma Gestão Eficaz* (Dissertação de mestrado, Universidade Aberta, Coimbra, Portugal. Consultado a 27 de novembro de 2018. Disponível em https://repositorioaberto.uab.pt/handle/10400.2/581

Tribunal de Contas de Portugal (1999). *Manual de Auditoria e de Procedimentos*. Consultado a 27 de novembro de 2018. Disponível em https://www.tcontas.pt/pt/publicacoes/manuais/map/Manual.pdf

THYCOTIC (s.d.). *Mapping to ISO 27001 Controls*. Consultado a 25 de novembro de 2018. Disponível em http://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf

Valente, L. S. P. (2014). *O contributo para um Sistema de Controlo Interno em uma Entidade do Setor Não Lucrativo* (Dissertação de Mestrado). Faculdade da Universidade de Coimbra, Coimbra, Portugal. Consultado a 20 de novembro de 2018. Disponível em https://estudogeral.sib.uc.pt/bitstream/10316/26634/1/Liliana_Valente_Disserta%C3%A7%C3%A3o_MCF-2014.pdf

Vasudevan, V., Mangla, A., Ummer, F., Shetty, S., Pakala, S., & Anbalahan, S. (2015). *Application Security in the ISO 27001:2013* (2ªed). Ely: IT Governance Publishing ISBN 978-1-84928-768-5. Consultado a 23 de novembro de 2018. Disponível em https://books.google.pt/books?id=BEQ3DwAAQBAJ&printsec=frontcover&dq=iso+27001&hl=pt-PT&sa=X&ved=0ahUKEwi085HHleneAhWMKMAKHf2_BhEQ6AEIMjAB#v=onepage&q=iso%2027001&f=false

Vilelas, J. (2009). *Investigação – O Processo de Construção do Conhecimento* (2ª ed). Lisboa: Edições Sílabo. ISBN: 9789726185574

Weindahl, P. (2003). *The Transformable and Reconfigurabe Factory – Strategies and Examples*. Seminário sobre Adaptabilidade Tecnológica, Escola Superior de Tecnologia de Setúbal.

Zorrinho, C. (1991). *Gestão da Informação*. Lisboa: Editorial Presença

Apêndices

Apêndice 1 – Inquérito

Como aluna do mestrado de Auditoria no Instituto Superior de Contabilidade e Administração de Lisboa, venho solicitar a vossa colaboração no preenchimento do presente questionário, com o tema Adoção das ISO pelas organizações – contributos da auditoria e do controlo, o qual tem a duração de aproximadamente 3 minutos, e será distribuído por todos os departamentos da organização, independentemente do nível hierárquico.
O inquérito é anónimo e as respostas serão tratadas com total confidencialidade e serão apenas utilizadas para fins da investigação, sendo analisadas e tratadas de um modo agregado.
Agradeço desde já, a disponibilidade e colaboração neste estudo.

1.Qual a função que desempenha na empresa?

a) Estagiário
b) Técnico Júnior
c) Técnico Sénior
d) Manager
e) Partner
f) Outra

2.Há quanto anos está na empresa?

a) ≤1 ano
b) >1 ano e ≤3 anos
c) >3 e ≤5 anos
d) >5 anos

3. De acordo com a resposta dada anteriormente, acompanhou a implementação das normas ISO 9001 e ISO 27001?

a) Sim
b) Não

(Se a resposta for não, passe para a questão 7)

4. Considera que a auditoria realizada por colaboradores internos e que antecedeu a intervenção externa, foi útil e adequada para preparar os colaboradores?

a) Nada
b) Pouco
c) Mediana
d) Muito

5. Se esta auditoria não tivesse sido realizada, como se sentiria para enfrentar o restante processo?

a) Muito desconfortável
b) Desconfortável
c) Confortável
d) Muito confortável

6. Quanto à auditoria externa, considera que a mesma foi apropriada ao fim em vista e apoiou a empresa no decorrer do processo?

a) Nunca
b) Raramente
c) Por vezes
d) Frequentemente
e) Sempre

7. Que benefícios pensa que a ISO 9001 e ISO 27001 trouxe para a empresa? Tendo como base a escala de valores de 1 a 5 em que:
1 – Discordo totalmente; 2 – Discordo; 3 – Não concordo nem discordo; 4 - Concordo; 5 – Concordo totalmente

	1	2	3	4	5
Destaque no mercado					
Satisfação dos clientes					
Divulgação da empresa					

Melhoria da relação com clientes, fornecedores e outras partes interessadas					
Uniformização dos procedimentos de trabalho					
Melhoria nos produtos/serviços prestados					
Aumento da satisfação dos colaboradores					
Melhoria nas relações e comunicação dentro da organização					
Aumento da faturação e de clientes					

8. Embora existam diversas vantagens associadas, o processo de implementação e toda a continuidade que o mesmo necessita, pode originar algumas dificuldades. Que dificuldades são sentidas perante as normas ISO 9001 e ISO 27001 na empresa? Tendo como base a escala de valores de 1 a 5 em que:

1 – Discordo totalmente; 2 – Discordo; 3 – Não concordo nem discordo; 4 - Concordo; 5 – Concordo totalmente

	1	2	3	4	5
Falta de compromisso da gestão					
Limitação de recursos financeiros,					

temporais e humanos					
Custo de implementação e a sua continuidade					
Resistência à mudança					
Processo e desenvolvimento da documentação					
Implementação e manutenção dos procedimentos					
Dúvidas sobre as normas					
Necessidade de formação					
Falta de apoio por parte dos auditores					
Falta de preparação perante as auditorias					

9. Na sua opinião, a empresa é reconhecida pelas certificações?

a) Sim
b) Não

10. Dada a adoção de procedimentos, políticas, manuais e outros documentos que acompanharam a implementação das ISO, qual considera ter sido a sua importância para a robustez do controlo interno da organização?

Tendo como base a escala de valores de 1 a 4 em que 1 representa nada importante e 4 representa muito importante.

1( ) 2( ) 3( ) 4( )

11. Como classifica o papel das auditorias realizadas durante o processo de implementação das ISO bem como as de acompanhamento que se seguiram?

Tendo como base a escala de valores de 1 a 4 em que 1 representa nada importante e 4 representa muito importante.

1( ) 2( ) 3( ) 4( )

Apêndice 2 – Respostas ao inquérito

Tabela nº1 – Respostas às questões 1, 2,3,4,5,6,9,10,11 do Inquirido 1 ao 30

Inquirido	Q1	Q2	Q3	Q4	Q5	Q6	Q9	Q10	Q11
1	Estagiário	≤ 1ano	Não	-	-	-	Sim	4	3
2	Estagiário	≤ 1ano	Não	-	-	-	Sim	3	3
3	Estagiário	≤ 1ano	Não	-	-	-	Não	4	4
4	Estagiário	≤ 1ano	Sim	Mediana	Desconfortável	Por vezes	Sim	2	3
5	Estagiário	≤ 1ano	Não	-	-	-	Sim	2	2
6	Estagiário	≤ 1ano	Não	-	-	-	Não	4	4
7	Estagiário	≤ 1ano	Não	-	-	-	Sim	3	4
8	Estagiário	≤ 1ano	Não	-	-	-	Não	4	4
9	Estagiário	≤ 1ano	Sim	Mediana	Confortável	Por vezes	Sim	3	2
10	Estagiário	≤ 1ano	Não	-	-	-	Sim	2	3
11	Técnico Júnior	>3 e ≤5 anos	Sim	Mediana	Desconfortável	Sempre	Sim	4	3
12	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Muito Desconfortável	Sempre	Sim	3	4
13	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	4
14	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	2
15	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Confortável	Por vezes	Não	4	2
16	Técnico Júnior	>3 e ≤5 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	4	3
17	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	2	3
18	Técnico Júnior	>3 e ≤5 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	4	4
19	Técnico Júnior	>1 ano e ≤3 anos	Sim	Pouco	Desconfortável	Por vezes	Não	4	3
20	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	3	4
21	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Desconfortável	Sempre	Sim	2	2
22	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	4	4
23	Técnico Júnior	>1 ano e ≤3 anos	Sim	Muito	Desconfortável	Frequentemente	Não	3	3
24	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	4
25	Técnico Júnior	≤ 1ano	Não	-	-	-	Sim	3	3

26	Técnico Júnior	>1 ano e ≤3 anos	Sim	Mediana	Desconfortável	Frequentemente	Não	3	4
27	Técnico Júnior	>3 e ≤5 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	3	4
28	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	3	3
29	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	3	4
30	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	3	3

Tabela nº2 – Respostas às questões 1, 2,3,4,5,6,9,10,11 do Inquirido 31 ao 60

Inquirido	Q1	Q2	Q3	Q4	Q5	Q6	Q9	Q10	Q11
31	Técnico Júnior	≤ 1ano	Não	-	-	-	Sim	4	4
32	Técnico Júnior	>1 ano e ≤3 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	4	4
33	Técnico Júnior	>1 ano e ≤3 anos	Sim	Muito	Desconfortável	Sempre	Sim	2	3
34	Técnico Júnior	≤ 1ano	Não	-	-	-	Não	4	3
35	Técnico Sénior	>3 e ≤5 anos	Sim	Mediana	Confortável	Frequentemente	Sim	4	4
36	Técnico Sénior	>5 anos	Sim	Mediana	Muito Desconfortável	Sempre	Sim	4	3
37	Técnico Sénior	>3 e ≤5 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	4	4
38	Técnico Sénior	>5 anos	Sim	Muito	Desconfortável	Sempre	Sim	3	3
39	Técnico Sénior	>1 ano e ≤3 anos	Sim	Muito	Confortável	Sempre	Sim	3	2
40	Técnico Sénior	>3 e ≤5 anos	Sim	Mediana	Desconfortável	Sempre	Sim	3	3
41	Técnico Sénior	>1 ano e ≤3 anos	Sim	Pouco	Desconfortável	Frequentemente	Sim	3	4
42	Técnico Sénior	>1 ano e ≤3 anos	Sim	Pouco	Desconfortável	Por vezes	Sim	3	3
43	Técnico Sénior	>3 e ≤5 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	3	4
44	Técnico Sénior	>5 anos	Sim	Muito	Desconfortável	Sempre	Sim	3	4
45	Técnico Sénior	≤ 1ano	Não	-	-	-	Não	3	4
46	Técnico Sénior	>5 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	3

47	Técnico Sénior	>3 e ≤5 anos	Sim	Mediana	Confortável	Por vezes	Sim	3	4
48	Técnico Sénior	>5 anos	Sim	Mediana	Desconfortável	Sempre	Sim	4	4
49	Manager	>5 anos	Sim	Muito	Confortável	Sempre	Sim	3	4
50	Manager	>3 e ≤5 anos	Sim	Muito	Muito Desconfortável	Sempre	Sim	4	4
51	Manager	>5 anos	Sim	Muito	Desconfortável	Sempre	Sim	4	4
52	Manager	≤ 1ano	Não	-	-	-	Sim	4	4
53	Manager	>1 ano e ≤3 anos	Sim	Muito	Muito Desconfortável	Sempre	Sim	3	4
54	Manager	>5 anos	Sim	Muito	Desconfortável	Frequentemente	Sim	3	4
55	Manager	>5 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	4
56	Manager	>5 anos	Sim	Muito	Confortável	Frequentemente	Sim	3	4
57	Partner	>5 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	4
58	Partner	>5 anos	Sim	Muito	Confortável	Sempre	Sim	4	4
59	Partner	>5 anos	Sim	Muito	Desconfortável	Sempre	Sim	3	4
60	Partner	>3 e ≤5 anos	Sim	Mediana	Desconfortável	Frequentemente	Sim	3	4

Tabela nº3 –Respostas à questão 7 do Inquirido 1 ao 20

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Destaque no mercado	3	4	3	3	4	4	4	4	3	5	4	3	4	4	5	5	3	4	5	4
Satisfação dos clientes	4	4	3	3	3	4	4	4	3	3	4	2	3	3	3	3	4	3	3	5
Divulgação da empresa	2	4	2	3	4	4	5	4	3	3	3	5	3	3	4	3	4	4	4	4
Melhoria da relação com clientes, fornecedores e outras partes interessadas	3	4	3	4	3	3	3	4	3	3	3	3	3	2	5	5	4	4	2	5
Uniformização dos procedimentos de trabalho	5	4	5	4	5	4	4	5	3	3	5	5	4	4	5	5	4	5	3	4
Melhoria nos produtos/serviços prestados	4	2	2	3	4	4	5	5	3	3	5	4	3	2	4	4	4	4	3	4
Aumento da satisfação dos colaboradores	4	4	2	3	4	3	1	3	3	3	2	2	3	2	3	2	4	3	2	3

Melhoria nas relações e comunicação dentro da organização	4	4	5	3	3	4	1	5	3	3	3	3	2	2	2	2	4	4	5	2
Aumento da faturação e de clientes	3	3	2	3	3	3	3	3	3	3	2	1	3	3	2	1	3	2	3	2
Melhoria a nível da gestão	4	5	5	4	5	4	3	4	3	3	3	3	4	3	3	4	4	4	3	3
Redução de prazos de entrega	4	1	2	3	3	2	1	4	3	3	2	2	3	3	4	4	4	3	2	1
Redução de erros	5	5	2	3	4	3	2	5	3	3	2	2	4	3	4	4	4	4	3	4
Melhoria na definição de responsabilidades e obrigação dos colaboradores	5	5	2	3	3	4	2	5	3	3	3	4	4	4	3	4	4	4	2	3

Tabela nº4 –Respostas à questão 7 do Inquirido 21 ao 40

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Destaque no mercado	3	5	5	4	4	5	3	5	4	4	3	4	5	5	3	3	3	5	4	3
Satisfação dos clientes	2	5	3	4	4	2	2	2	5	5	4	3	4	5	5	4	2	5	4	3
Divulgação da empresa	5	3	3	3	4	5	5	3	3	3	5	4	4	3	5	4	4	4	4	4
Melhoria da relação com clientes, fornecedores e outras partes interessadas	3	5	3	3	4	2	2	3	3	3	4	4	4	2	4	4	4	4	4	4
Uniformização dos procedimentos de trabalho	2	5	5	4	4	4	4	4	4	4	4	4	4	4	4	5	3	5	4	4
Melhoria nos produtos/serviços prestados	2	3	5	4	4	5	3	4	4	4	4	4	4	4	5	5	4	4	4	4
Aumento da satisfação dos colaboradores	3	4	4	2	2	2	2	2	2	4	2	2	2	2	2	2	1	2	4	2
Melhoria nas relações e comunicação dentro da organização	2	5	4	4	5	2	4	2	4	4	5	5	5	5	5	5	2	4	4	5

Aumento da faturação e de clientes	1	2	1	2	3	2	3	1	3	3	1	3	3	3	2	3	2	3	4	4
Melhoria a nível da gestão	5	5	4	3	4	5	4	5	5	4	4	5	5	4	4	4	5	5	4	3
Redução de prazos de entrega	2	3	3	3	3	1	1	4	2	4	2	2	4	2	4	2	2	2	4	2
Redução de erros	3	3	5	3	4	2	4	4	4	4	4	4	4	3	2	2	2	4	4	3
Melhoria na definição de responsabilidades e obrigação dos colaboradores	3	5	5	5	4	2	2	5	4	4	4	5	4	5	5	5	4	5	4	3

Tabela nº5 –Respostas à questão 7 do Inquirido 41 ao 60

	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Destaque no mercado	3	4	4	5	5	4	4	4	4	5	4	5	5	5	5	5	5	4	5	4
Satisfação dos clientes	5	4	4	4	5	4	5	4	4	5	4	5	4	5	5	5	4	4	5	4
Divulgação da empresa	5	4	4	5	4	4	4	4	4	5	4	4	5	4	4	5	5	4	5	5
Melhoria da relação com clientes, fornecedores e outras partes interessadas	4	4	4	2	2	2	2	4	4	5	4	2	2	2	2	2	4	4	5	5
Uniformização dos procedimentos de trabalho	4	2	4	4	4	4	3	4	2	5	5	5	4	4	4	5	4	5	5	4
Melhoria nos produtos/serviços prestados	3	5	4	4	4	4	4	4	3	5	5	5	4	4	3	5	4	5	5	3
Aumento da satisfação dos colaboradores	2	2	2	4	2	4	2	2	4	4	2	4	4	3	4	4	4	4	4	4
Melhoria nas relações e comunicação dentro da organização	5	2	4	5	5	4	3	5	4	5	5	5	4	3	4	5	4	5	4	4
Aumento da faturação e de clientes	3	2	4	4	2	4	5	5	1	4	4	4	4	4	4	5	3	2	5	5
Melhoria a nível da gestão	3	5	4	5	5	5	5	5	5	5	4	4	5	5	5	5	4	5	4	5
Redução de prazos de entrega	2	2	2	4	2	2	2	2	2	1	2	4	4	2	2	1	2	4	3	3
Redução de erros	3	2	2	4	4	4	3	2	3	5	3	4	4	4	3	5	3	4	4	4

Melhoria na definição de responsabilidades e obrigação dos colaboradores	5	3	4	4	4	5	5	3	5	5	5	4	4	4	4	5	4	4	4	4

Tabela nº6 –Respostas à questão 8 do Inquirido 1 ao 20

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Falta de compromisso da gestão	3	3	2	2	2	1	3	3	3	3	1	1	2	4	2	2	4	3	3	4
Limitação de recursos financeiros, temporais e humanos	5	3	2	5	3	2	4	4	5	3	4	5	3	4	4	2	4	5	3	4
Custo de implementação e a sua continuidade	4	4	2	2	4	2	5	4	5	3	2	2	5	5	2	2	4	5	4	4
Resistência à mudança	3	4	2	2	2	3	4	4	3	3	3	3	4	5	4	3	4	5	4	4
Processo e desenvolvimento da documentação	4	3	4	2	3	2	2	3	3	3	3	3	3	4	4	3	5	4	4	4
Implementação e manutenção dos procedimentos	4	3	4	2	4	2	4	2	3	3	2	4	3	4	4	3	4	4	4	4
Dúvidas sobre as normas	3	4	2	5	4	4	2	4	5	5	3	4	3	3	4	5	5	5	4	4
Necessidade de formação	4	4	2	3	4	5	4	5	3	3	4	2	4	2	4	3	5	4	4	4
Falta de apoio por parte dos auditores	3	2	2	3	2	3	2	1	3	2	2	2	2	2	2	2	1	1	2	1	4
Falta de preparação perante as auditorias	3	4	2	3	3	1	3	3	3	2	2	3	2	2	2	1	1	4	4	4

Tabela nº7 –Respostas à questão 8 do Inquirido 21 ao 40

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Falta de compromisso da gestão	3	2	4	2	4	2	4	2	2	2	3	4	1	2	2	1	2	2	4	2
Limitação de recursos financeiros, temporais e humanos	4	5	4	2	4	4	2	4	2	5	4	5	2	5	3	4	5	2	4	4
Custo de implementação e a sua continuidade	5	4	4	5	5	2	2	5	2	3	5	5	5	3	5	4	4	4	4	4

Resistência à mudança	4	5	5	4	4	4	4	5	3	4	4	5	3	5	4	4	4	4	4	4
Processo e desenvolvimento da documentação	4	5	5	4	3	2	4	4	3	3	3	4	2	3	4	3	2	2	4	4
Implementação e manutenção dos procedimentos	4	5	5	4	4	4	4	5	2	3	3	4	4	4	4	3	4	2	4	4
Dúvidas sobre as normas	1	4	1	4	4	4	4	1	2	4	4	1	4	4	1	4	4	2	4	1
Necessidade de formação	5	5	3	5	4	2	3	4	4	4	4	2	2	4	3	3	4	2	4	3
Falta de apoio por parte dos auditores	4	1	3	4	4	2	1	2	2	1	2	1	2	3	2	2	1	1	4	4
Falta de preparação perante as auditorias	1	2	4	4	1	4	2	4	1	1	1	4	2	1	2	2	1	2	4	1

Tabela nº8 –Respostas à questão 8 do Inquirido 41 ao 60

	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Falta de compromisso da gestão	4	4	3	4	2	4	4	4	2	2	2	2	2	2	2	1	2	2	2	2
Limitação de recursos financeiros, temporais e humanos	2	4	4	4	4	4	4	5	2	2	5	5	2	4	5	4	5	2	5	2
Custo de implementação e a sua continuidade	2	5	4	3	4	5	3	4	5	4	4	5	2	2	5	5	4	4	5	2
Resistência à mudança	4	4	4	4	4	3	4	4	5	3	5	4	4	3	4	5	4	4	4	4
Processo e desenvolvimento da documentação	2	4	3	4	4	5	2	4	4	4	4	2	4	2	4	5	4	4	4	3
Implementação e manutenção dos procedimentos	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	5	4	4	4	3
Dúvidas sobre as normas	2	2	4	4	4	1	4	4	2	2	5	5	2	4	4	5	3	4	3	4
Necessidade de formação	4	2	4	4	4	4	4	3	2	3	4	5	4	4	3	5	3	4	3	5
Falta de apoio por parte dos auditores	4	2	2	1	2	1	2	1	4	2	1	1	2	2	1	2	1	2	2	1
Falta de preparação perante as auditorias	4	2	2	1	1	1	4	4	2	2	1	1	2	2	4	1	4	2	2	2