UNIVERSIDADE D
COIMBRA

Alexandre José Henriques Ferreira

IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM CONFORMIDADE COM A ISO/IEC 27001

Relatório de Estágio no âmbito do Mestrado em Gestão orientado pelo Professor Doutor Mário António Gomes Augusto e apresentada à Faculdade de Economia da Universidade de Coimbra

Julho de 2020

Alexandre José Henriques Ferreira

IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM CONFORMIDADE COM A ISO/IEC 27001

Relatório de estágio em Gestão e apresentada à Faculdade de Economia da Universidade de Coimbra para obtenção do grau de Mestre.

Orientador Académico: Professor Doutor Mário António Gomes Augusto

Supervisor Profissional: Doutora Cristina Isabel Roque Ferreira

Entidade de Acolhimento: Pahl Consulting, Lda.

Coimbra, julho de 2020

Agradecimentos

A todos que de alguma maneira contribuíram para a execução deste relatório e deste estágio.

Ao meu orientador académico, o professor doutor Mário Augusto, pela disposição e paciência disponibilizadas ao longo deste período, bem como pelas sábias e imprescindíveis ajudas e orientações.

À minha supervisora de estágio, doutora Cristina Ferreira, por ter acreditado em mim desde o início e ter possibilitado esta experiência incrível.

Aos meus colegas da Pahl Consulting pelo apoio dado ao longo do estágio e pela disponibilidade em colaborar em atividades relativas ao relatório.

À minha família pela paciência ao lidar com este período de mudança e incerteza.

E, em especial, à Sofia pelo apoio, motivação e atenção despendida durante todo este período e em todos as situações mais complicadas relacionadas com este estágio e relatório.

A todos vós, o meu mais sincero obrigado.

Resumo

Este relatório de estágio surge no âmbito do Mestrado em Gestão na Faculdade de Economia da Universidade de Coimbra. O objetivo é apresentar as atividades desenvolvidas durante o estágio curricular, levado a cabo na consultora Pahl Consulting, Lda.

A Pahl Consulting, Lda. foi contratada por uma entidade pública para estabelecer e implementar um sistema de gestão de segurança da informação (SGSI) que cumprisse os requisitos da norma ISO/IEC 27001. Um SGSI pode ajudar a que uma organização reduza os seus custos ao prevenir e tratar de forma eficaz os incidentes de segurança da informação. Ao cumprir os requisitos da norma ISO/IEC 27001, uma organização consegue não só assegurar a confidencialidade, integridade e disponibilidade das suas informações, mas também aperfeiçoar a sua performance operacional e de mercado. Com o auxílio das normas ISO/IEC 27002 e ISO/IEC 27005, é possível estabelecer, implementar e controlar um sistema de gestão do risco e os controlos de segurança da informação propostos pela norma ISO/IEC 27001 para responder aos seus requisitos. Na maior parte das vezes isso acontece através da criação de políticas e procedimentos que deverão ser adotados por toda a organização.

Durante este estágio curricular foi desenvolvido um vasto conjunto de atividades, com particular destaque para a redação dos manuais de procedimentos, que pretendem estabelecer as políticas e os procedimentos que certificam o cumprimento dos controlos de segurança da informação por parte da organização que pretende adotar este SGSI. Para além disso, este relatório retrata, ainda, a metodologia de gestão do risco desenvolvida no âmbito deste projeto.

A preocupação com a segurança da informação tem crescido nos últimos anos e espera-se que continue a aumentar. Assim, este relatório pode tornar-se relevante e útil para quem pensa adotar um SGSI e a certificação ISO/IEC 27001. Por outro lado, este estágio contribuiu para um valioso crescimento pessoal e profissional.

Palavras-Chave: Segurança da Informação, Norma ISO/IEC 27001, Controlos de Segurança, Políticas e Procedimentos.

Abstract

This report comes under the Master's in Management at the Faculty of Economics of the University of Coimbra. The objective is to present the activities developed during the curricular internship, which took place at Pahl Consulting, Lda.

The Pahl Consulting, Lda. was contracted by a public entity to establish and implement an information security management system (ISMS) that complies with the requirements of the ISO/IEC 27001 standard. An ISMS can help an organization to reduce its costs by preventing and effectively handling information security incidents. By meeting the requirements of the ISO/IEC 27001 standard, an organization is able to not only ensure the confidentiality, integrity and availability of its information, but also improve its operational and market performance. With the support of ISO/IEC 27002 and ISO/IEC 27005, it is possible to establish, implement and control a risk management system and the information security controls proposed by ISO/IEC 27001 to meet its requirements. Most of the time this happens through the creation of policies and procedures that must be adopted by the entire organization.

During this curricular internship, a wide range of activities was developed, with particular emphasis on writing the manuals aimed to establish the policies and procedures that certify an organization intending to adopt this ISMS in compliance with information security controls. In addition, this report also portrays the risk management methodology developed within the scope of this project.

Concern about information security has grown in recent years and is expected to continue increasing. Thus, this report can become relevant and useful for anyone concerning of adopting an ISMS and ISO/IEC 27001 certification. On the other hand, this internship has contributed to a valuable personal and professional growth.

Keywords: Information Security, ISO/IEC 27001 standard, Security Controls, Policies and Procedures.

Acrónimos

BS – *British Standard*

CD – *Compact Disk*

COVID 19 – *Coronavirus Disease* 2019

CT – Comissão Técnica

CVSS 3.0 – *Common Vulnerability Scoring System Calculator* 3.0

IEC – *International Electrotechnical Commission*

ISO – *International Organization for Standardization*

itSMF – *IT Service Management Forum*

JTC1 – *Joint Technical Committee* 1

NIST - *National Institute of Standards and Technology*

NP – Norma Portuguesa

PDCA – *Plan-Do-Check-Act*

RBV – *Resource-Based View*

RGPD – Regulamento Geral de Proteção de Dados

ROA – *Return on Assets*

SARS-COV-2 – *Severe Acute Respiratory Syndrome Coronavirus* 2

SGSI – Sistema de Gestão de Segurança da Informação

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

TR – *Technical Report*

USB – *Universal Serial Bus*

Índice geral

Índice de figuras

Índice de tabelas

1. Introdução

A realização de um estágio curricular e elaboração do respetivo relatório é um dos caminhos possíveis para concluir o Mestrado em Gestão. As principais vantagens deste formato são a possibilidade de estar inserido num ambiente e cultura empresarial, permitindo a criação e o desenvolvimento de um diversificado conjunto de competências. Estes fatores estiveram na base da decisão de eleger esta opção para concluir o Mestrado em Gestão da Faculdade de Economia da Universidade de Coimbra. Este estágio decorreu ao longo de, aproximadamente, quatro meses entre 3 de fevereiro e 8 de junho de 2020 na consultora Pahl Consulting, Lda.

Durante este período, a par com outras tarefas, foram elaboradas diversas atividades com o objetivo de conhecer e compreender a norma ISO/IEC 27001 e, posteriormente, auxiliar na criação e implementação dos controlos de segurança da informação propostos por essa norma. A ISO/IEC 27001 é uma norma reconhecida internacionalmente que fornece *standards* para a criação, implementação e monitorização de um sistema de gestão de segurança da informação (SGSI). A informação representa um ativo das organizações de crescente importância, pelo que as medidas que procuram garantir a segurança deste ativo têm-se tornado cada vez mais relevantes e requisitadas pelas organizações em geral e pelas empresas em particular.

Por esse motivo, o objetivo deste relatório de estágio é apresentar a norma ISO/IEC 27001 e um método para implementar um SGSI que responda aos requisitos dessa norma. Nesse sentido, foi analisado o projeto em que a Pahl Consulting, Lda. possui responsabilidades pelo desenvolvimento e implementação de um SGSI na estrutura de uma entidade pública, em conformidade com os *standards* propostos pela norma ISO/IEC 27001.

A adoção de um SGSI permite às empresas reduzirem custos ao prevenirem incidentes de segurança da informação e melhorarem os processos de tratamento desses incidentes. Se adicionalmente, for obtida a certificação ISO/IEC 27001, a organização poderá alcançar uma vantagem competitiva devido à imagem transmitida de preocupação com a segurança das suas informações, dos seus clientes, dos seus fornecedores e de outros *stakeholders*. Para além disso, a ISO/IEC 27001 exige que sejam adotados *standards* que visam o aperfeiçoamento da organização interna das entidades que a adquirem e a melhoria contínua dos sistemas de gestão de segurança da informação. Isto significa que as

organizações ao adotarem os *standards* da ISO/IEC 27001 para um SGSI, para além de protegerem um ativo essencial, podem ainda alcançar benefícios operacionais e de mercado, como por exemplo uma melhoria na relação com os clientes e na organização e competências dos recursos internos.

Para além desta introdução, este relatório compreende mais cinco capítulos: apresentação da entidade de acolhimento, abordagem concetual, estágio, análise crítica e conclusões e considerações finais.

A seguir a esta introdução será apresentada a entidade de acolhimento deste estágio, a Pahl Consulting, Lda. Será descrita a sua curta história e a sua filosofia, assinaladas as áreas onde atua e compreendida a sua estrutura.

No terceiro capítulo, abordagem concetual, será desenvolvida uma análise dos conteúdos relevantes através de uma revisão de literatura que procurou, inicialmente, enquadrar os conceitos relacionados com um SGSI e as normas da família ISO/IEC 27000, com especial atenção para a norma ISO/IEC 27001, e, em seguida, compreender o processo de implementação deste SGSI e os impactos que a certificação ISO/IEC 27001 pode causar na performance das organizações.

No quarto capítulo, serão descritas as atividades desenvolvidas ao longo deste estágio. Serão abordados os vários projetos integrados durante este período e, em seguida, será dado destaque ao projeto referente à implementação de um SGSI que cumprisse os requisitos da norma ISO/IEC 27001. Serão retratadas as atividades desenvolvidas ao longo deste período de estágio, mas também será desenvolvida uma visão retrospetiva sobre o que já tinha sido feito antes deste período e uma visão prospetiva relativa ao que ainda terá de ser executado no futuro.

Por fim, antes das conclusões e considerações finais, será, ainda, dedicado um capítulo à elaboração de uma análise crítica tanto à atuação da entidade de acolhimento como às atividades desenvolvidas durante este estágio curricular.

2. Entidade de acolhimento

A Pahl Consulting, Lda. é uma consultora de gestão que surgiu em abril de 2018, em Lisboa, como uma ramificação da Pahldata, S.A. A Pahldata, S.A. é uma empresa fundada em 1987 cujos fundadores são de origem espanhola, mas está sediada em Lisboa com escritórios partilhados com a Pahl Consulting, Lda. Esta entidade é especializada no fornecimento de soluções de telecomunicações para operadores e empresas, criando e implementando soluções de Tecnologia de Informação e Comunicações (TIC). Assim, a Pahl Consulting, Lda. surgiu para fornecer um novo e diversificado conjunto de serviços, nomeadamente nas áreas de:

- **Estratégia:** com oferta de serviços de planeamento estratégico, estudos de mercado, estudos e análises económicas, diagnóstico organizacional, reorganização empresarial, modelos de *governance, business audit*, gestão da inovação, análises económico-financeira e transformação digital.
- **Operações:** com capacidade de executar a implementação de gestão por processos, a reengenharia e otimização de processos, a implementação de processos de qualidade, a transformação da estrutura de custos, a definição de modelo de serviços partilhados, a gestão de projetos, a elaboração e gestão de candidaturas a fundos comunitários e o *procurement* de oportunidades de financiamento.
- **Risco e *Compliance*:** com serviços focados em modelos integrados de controlo interno, modelos de gestão de risco operacional, modelos de combate à fraude e ao branqueamento de capitais, códigos de conduta e conflito de interesses, planos de continuidade de negócio e sistemas em conformidade com o regulamento geral de proteção de dados (RGPD).
- **Marketing e Comercial**: com capacidade de desenvolver planos de reorganização da rede comercial, de modelos de eficácia comercial, planos de reestruturação comercial, planos de *gamification*, planos de marketing, estratégia de marketing digital e *branding strategy*.
- **Organização e Pessoas:** com capacidade para desenvolver planos de gestão da mudança, modelos de funções e competências, modelos de avaliação de desempenho, modelos de compensação e benefícios, *assessment* de competências, liderança e gestão de talentos, planos de formação, transformação organizacional e programas de *onboarding*.

- ***IT Advisory*:** com oferta de planos estratégicos de sistemas de informação, definição e implementação de modelos de segurança de informação, apoio na implementação de modelos de gestão de serviço, desenho e implementação de soluções, elaboração de cadernos de encargos, gestão de portfólio de TI (Tecnologias de Informação) e gestão de portfólio de projetos.[1]

Atualmente, com um mundo globalizado, fornecer respostas céleres, mas eficazes, à transformação dos negócios é certamente, para além de uma preocupação, um objetivo, principalmente para uma consultora de gestão, onde efetivamente se pode comprovar que o sucesso dos seus clientes é o seu sucesso. Nesse sentido, a Pahl Consulting, Lda tem como propósito "desenvolver e capacitar clientes, colaboradores e parceiros no caminho da excelência"[2] e ambiciona "ser o parceiro de referência para a concretização de iniciativas que traduzam a estratégia em ação"[3] sempre com o compromisso de, juntamente com os seus clientes, construir as soluções que melhor respondam às necessidades atuais, mantendo a sua utilidade futura em perspetiva. Para além disso, esta entidade procura, em todas as atividades em que se encontra envolvida, agir conforme quatro valores fundamentais:

- **Integridade:** agir sempre com honestidade e transparência;
- **Inovação:** procurar incessantemente soluções para os desafios dos seus clientes;
- **Qualidade:** dedicar uma equipa de consultores à prestação de um serviço de qualidade;
- **Ambição:** trabalhar para ser o parceiro de referência das organizações no seu desenvolvimento.[4]

Presentemente, a Pahl Consulting, Lda conta com 25 colaboradores e apresenta vontade de continuar a fazer crescer a organização celeremente. A sua estrutura é composta por elementos que ocupam cargos desde *Analyst*, que têm uma responsabilidade mais reduzida, até ao cargo de maior responsabilidade de *Associated Partner*. Ordenados pelo nível da responsabilidade, as restantes posições são: *Consultant*, *Senior Consultant*, *Manager/Expert* e *Senior Manager/SM Expert*. Para além de um *Managing Partner*, a entidade possui ainda dois *partners* como membros de alta gestão e acionistas da

[1] Informação recolhida na apresentação corporativa da Pahl Consulting
[2] Missão. Informação recolhida em http://www.pahlconsulting.pt/ (Consultado em 19-05-2020)
[3] Visão. Informação recolhida em http://www.pahlconsulting.pt/ (Consultado em 19-05-2020)
[4] Informação recolhida em http://www.pahlconsulting.pt/ (Consultado em 19-05-20120)

organização: um responsável pela coordenação de projetos na área de estratégia e gestão e outro mais vocacionado para projetos da área de TI. Contudo, como se pode confirmar na Figura 1, o maior acionista é a Pahldata, S.A.

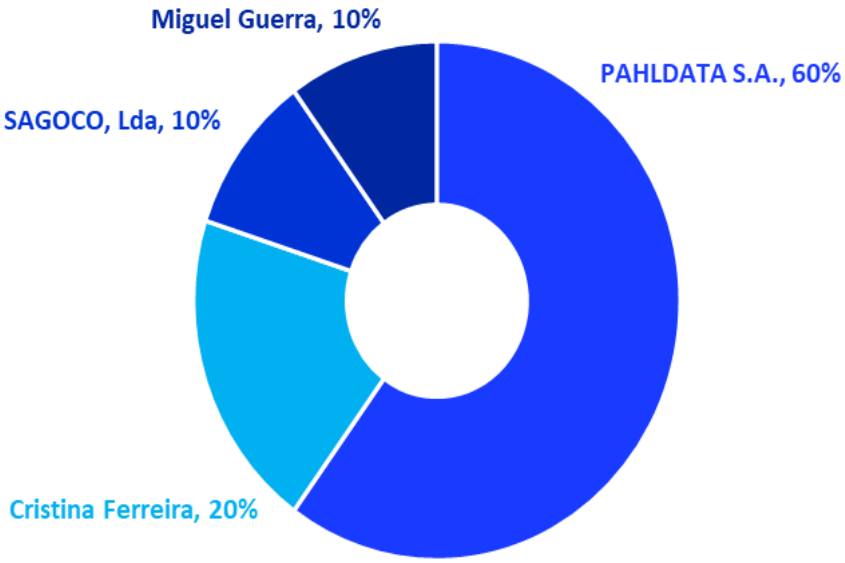
Como se pode ver no organograma da entidade, representado na Figura 2, a estrutura organizacional da Pahl Consulting, Lda. é composta por um conselho de administração que se desagrega em: uma direção comercial partilhada com a Pahldata, S.A.; uma direção administrativa e financeira; e uma direção responsável pelos serviços fornecidos.

A Pahl Consulting, Lda. também se empenha em escolher os seus parceiros estrategicamente com o intuito de conseguir desenvolver e fornecer uma maior quantidade e qualidade de soluções para cada projeto. Grande parte dos clientes da Pahl Consulting, Lda. pertence ao setor público e está presente nas mais diversas áreas. Apesar de grande maioria dos projetos que a Pahl Consulting, Lda. representa atualmente estarem a decorrer em Portugal, o seu maior projeto encontra-se a ser desenvolvido em território angolano.

Para além das "*Big Four*" (PWC, Deloitte, EY e KPMG) que dominam o mercado de consultoria, não só a nível nacional, mas também a nível mundial, existem ainda inúmeras pequenas consultoras capazes de cobrir parte dos serviços oferecidos pela Pahl Consulting, Lda. A atividade da Pahl Consulting, Lda. pode ser dividida em duas categorias principais: uma direcionada para a consultoria nas áreas de estratégia e gestão e outra para a consultoria nas áreas de TI. De acordo com a Central de Balanços do *Banco de Portugal*, em 2018, existiam em Portugal 13 004 empresas a atuar em consultoria para negócios e gestão, onde 52,8% das empresas estão sediadas em Lisboa e 99,84% são micro, pequenas ou médias empresas[5]. Quanto a consultoria em informática, existem 3 446 empresas em Portugal a atuar nessa atividade, sendo que 99,33% destas são micro, pequenas ou médias empresas e 60,2% estão localizadas em Lisboa[6].

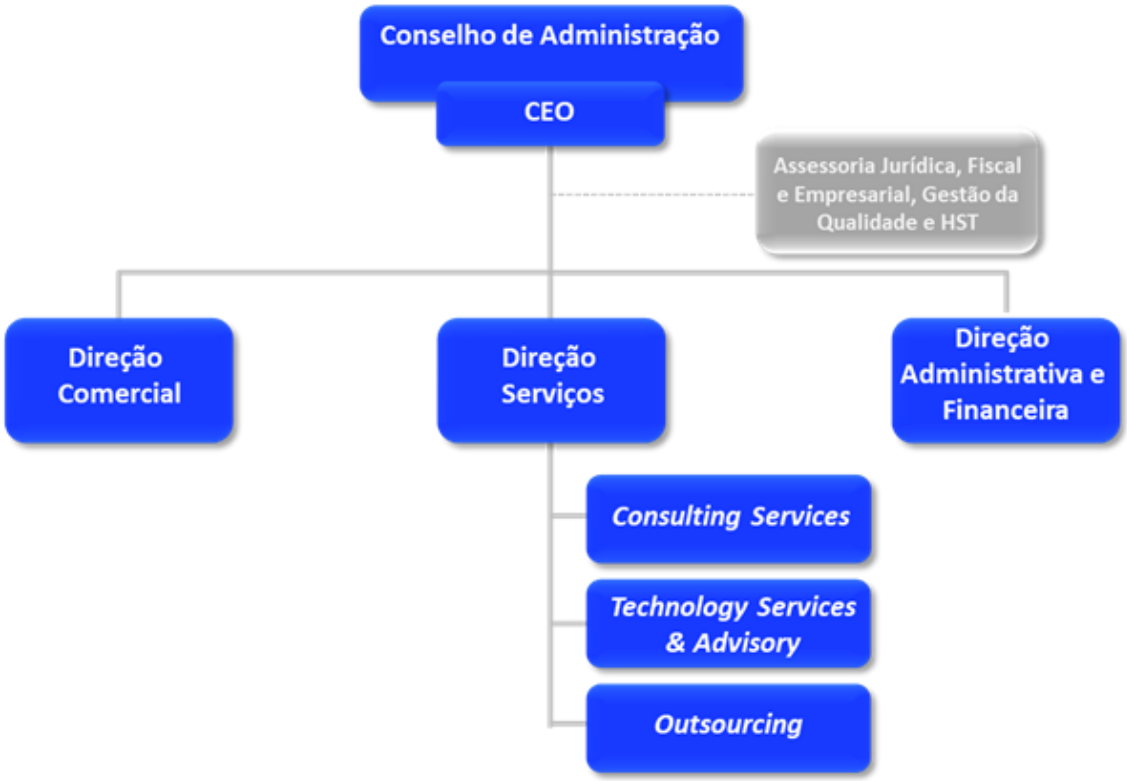
[5] Informação recolhida em https://www.bportugal.pt/QS/qsweb/Dashboards (Consultado em 29-06-2020). Categoria 70220 - Outras atividades de consultoria para os negócios e a gestão.
[6] Informação recolhida em https://www.bportugal.pt/QS/qsweb/Dashboards (Consultado em 29-06-2020). Categoria 62020 - Atividades de consultoria em informática.

Figura 1 - Estrutura acionista.



Fonte: Apresentação Corporativa Pahl Consulting

Figura 2 - Estrutura organizacional.



Fonte: Apresentação Corporativa Pahl Consulting

3. Abordagem concetual

Ataques informáticos a sistemas de informação acontecem frequentemente. Em Portugal, todos os anos aumentam, os números de tentativas de aceder e intercetar informação de forma ilegal[7]. Já por diversas vezes, casos desta natureza ganharam enorme relevo na comunicação social portuguesa, como é o caso "*e-toupeira*" referente à interceção de emails da SAD do Benfica ou, ainda, o caso "*Luanda Leaks*", onde foram divulgadas informações confidenciais sobre supostos esquemas de enriquecimento de uma empresária angolana. No entanto, nem todos estes ataques têm como objetivo denunciar atividades ilícitas. De acordo com um estudo promovido pelo jornal *Visual Capitalist*, o principal motivo destes ataques é o dinheiro, correspondendo a 41% dos mesmos[8]. As informações acedidas são utilizadas em planos de chantagem ou extorsão. Os ataques motivados ideologicamente representam uma baixa percentagem destas investidas. Mas foi um ataque massivo em 1998 ao principal centro de investigação nuclear de Índia, *Bhabha Atomic Research Centre*, iniciado por razões ideológicas, que desencadeou em diversas entidades de grande relevo mundial, uma crescente preocupação com a segurança da informação (Farn, Lin, & Fung, 2004). Este ataque foi possível devido a deficientes políticas de palavras-passe e de retenção de informação, que atualmente são cobertas minuciosamente pelas normas de segurança de informação disponíveis, incluindo a norma ISO/IEC 27001:2013.

Neste capítulo, será desenvolvida uma revisão de literatura com vista a enquadrar concetualmente as temáticas mais importantes para compreender a implementação de um sistema de gestão da segurança da informação em conformidade com a norma ISO/IEC 27001. Nesse sentido, será: i) abordado o conceito de sistema de gestão da segurança da informação, ii) elaborado um enquadramento sobre a família de normas ISO/IEC 27000, iii) explicada a norma ISO/IEC 27001, iv) discutido o processo de implementação da norma e v) expostos os impactos que esta pode acarretar para a performance de uma organização.

3.1 Sistema de Gestão da Segurança da Informação

A informação é um ativo essencial para as organizações, e tal como todos os ativos importantes pode ser alvo de roubo ou acesso indevido (Syreyshchikova, Pimenov,

[7] Informação recolhida em https://ionline.sapo.pt/artigo/641503/ciberseguranca-ataques-informaticos-quase-duplicaram-desde-o-inicio-da-decada-?seccao=Portugal (Consultado em 23-05-2020)
[8] https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/ (Consultado em 23-05-2020)

Mikolajczyk, & Moldovan, 2019). Por causa da sua importância e vulnerabilidade deve ser apropriadamente protegida (Doughty, 2003 apud Casaca & Correia, 2010). Atualmente, todas as organizações, independentemente do tipo ou tamanho, coletam, processam, armazenam e transmitem informação (ISO/IEC 27000:2018). Desta forma, é necessário que reconheçam os riscos associados a este ativo e ajam de forma a garantir a sua segurança. A solução fornecida pela família de normas ISO/IEC 27000 é a aplicação de um "conjunto de elementos inter-relacionados para estabelecer objetivos, políticas e processos" (ISO/IEC 27000:2018, p. 6), que visem alcançar a segurança de informação.

Um sistema de gestão da segurança da informação (SGSI), de acordo com a norma ISO/IEC 27000:2018, "consiste nas políticas, procedimentos, diretrizes e nos recursos e atividades associadas, geridos coletivamente por uma organização, com o intuito de proteger os seus ativos de informação. É uma abordagem sistemática para estabelecer, implementar, operar, monitorar, rever, manter e melhorar a segurança das informações de uma organização para atingir os objetivos de negócios." (ISO/IEC 27000:2018, p. 11-12)

A mesma norma, ISO/IEC 27000:2018, define, ainda, a segurança da informação como a preservação da confidencialidade, integridade e disponibilidade da informação. Num ambiente altamente digitalizado com que as organizações lidam constantemente, cada vez mais é necessário apenas um processo simples de raciocínio para entender a importância que é manter a informação segura. A abundância de dados e sistemas informatizados com detalhes, tanto sobre os processos produtivos como administrativos das organizações, tornam fundamental manter estas informações sensíveis longe das mãos de pessoas mal-intencionadas que poderiam utilizar ou modificar essa informação para responder a interesses pessoais, potenciando, desta forma, enormes prejuízos para as organizações. Por outro lado, a partilha de informação em tempo real cada vez mais exigente e imprescindível, para responder aos objetivos das organizações e dos seus gestores (Correia, 2016), faz com que a sua disponibilidade e integridade adquiram uma importância acrescida.

A informação e, consequentemente, os sistemas de informação são ativos extremamente importantes para as organizações. Desta forma, manter estes ativos seguros passará, cada vez mais, a ser um dos principais objetivos das equipas de gestão das organizações. Com isto em mente, as normas da família ISO/IEC 27000 fornecem orientações para que a proteção dos ativos de informação seja garantida.

3.2 Família ISO/IEC 27000

A *International Organization for Standardization* (ISO) é uma entidade fundada em 1947, com sede na Suíça, responsável pelo desenvolvimento de *standards* a nível mundial nas mais diversas áreas[9]. Em 1987, uniu-se com a *International Electrotechnical Comission* (IEC), uma entidade criada em 1906, também na Suíça, e que desenvolve *standards* e sistemas de avaliação nas áreas de produtos, serviços e sistemas elétricos e eletrónicos[10]. Em conjunto, criaram uma comissão técnica, ISO/IEC JTC1, com o objetivo de desenvolver *standards* relacionados com as Tecnologias de Informação e Comunicação (TIC), e desde então. já publicaram 3 249 *standards* na área[11].

Em 2005, com base no *standard* britânico BS 7799:2, esta comissão técnica conjunta inicia a série de *standards* 27000 direcionada aos sistemas de gestão de segurança da informação. É importante compreender que os *standards* são conjuntos de políticas, processos e procedimentos desenvolvidos por especialistas de cada área, que permitem implementar e controlar determinado projeto que vá ao encontro dos objetivos específicos de quem adota estes *standards*. No caso das normas da família ISO/IEC 27000, o objetivo é "proporcionar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (NP ISO/IEC 27001:2013, p. 5). Contudo, isto não significa que todas as organizações interessadas em adotar um SGSI vão percorrer exatamente o mesmo caminho. É expectável que a adoção de um SGSI seja uma decisão estratégica da organização e esteja completamente integrada com as necessidades dessa mesma organização (ISO/IEC 27000:2018). Isto é, este conjunto de normas fornece um variado número de *standards* com requisitos e instruções para estabelecer, implementar, manter e melhorar o SGSI, tendo cada organização de compreender a sua realidade e de que forma pode alcançar a conformidade com estes requisitos dentro do seu ambiente específico. Resumidamente, os *standards* desta família de normas oferecem o seguinte:

- Definição dos requisitos para o SGSI e a sua certificação;
- Diretrizes detalhadas de como estabelecer, implementar, manter e melhorar o SGSI;
- Orientações para a auditoria e a avaliação da conformidade com os requisitos;

[9] Informação recolhida em https://www.iso.org/about-us.html#12 (Consultado em 24-05-2020)
[10] Informação recolhida em https://www.iec.ch/about/profile/ (Consultado em 24-05-2020)
[11] Informação recolhida em https://www.iso.org/isoiec-jtc-1.html (Consultado em 24-05-2020)

- Diretrizes específicas do setor (ISO/IEC 27000:2018).

Atualmente, as normas que fazem parte desta família são as que se encontram esquematizadas na Figura 3. O propósito de cada uma delas é o seguinte:

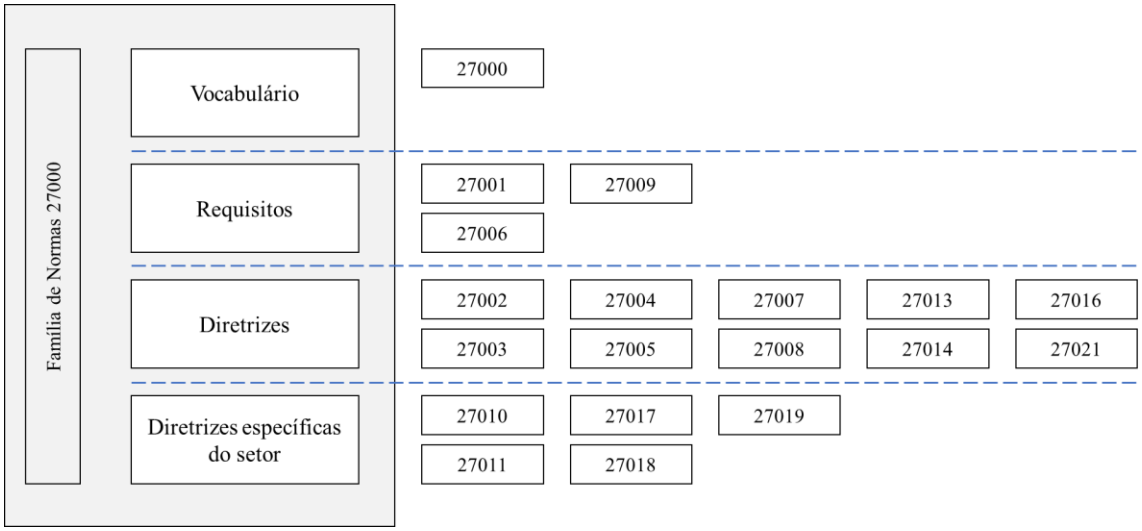
- **ISO/IEC 27000 – *Information technology – Security techniques – Information security management system – Overview and vocabulary*:** fornece uma visão geral da família de normas relativas ao SGSI e a definição de todos os termos relacionados com o SGSI, que são utilizados nas restantes normas;
- **ISO/IEC 27001 – *Information technology – Security techniques – Information security management system – Requirements*:** especifica os requisitos para estabelecer, implementar, manter e melhorar o SGSI. É importante salientar que esta é a única norma passível de certificação tornando-se, por isso, na norma que ganhou mais relevo dentro desta família. Se uma organização desejar que o seu SGSI seja certificado, terá de cumprir, cumulativamente, todos os requisitos especificados nesta norma. Esta propõe, ainda, uma lista de controlos de segurança de informação que as organizações podem adotar para cobrirem os requisitos exigidos;
- **ISO/IEC 27002 – *Information technology – Security techniques – Code of practice for information security controls*:** fornece diretrizes para a implementação dos controlos de segurança de informação cedidos na norma ISO/IEC 27001;
- **ISO/IEC 27003 – *Information technology – Security techniques – Information security management – Guidance*:** oferece explicações e instruções sobre os requisitos impostos pela norma ISO/IEC 27001;
- **ISO/IEC 27004 – *Informatin technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*:** define um plano que permite que seja feita uma avaliação da eficácia do SGSI através de uma medição e análise da conformidade com a norma ISO/IEC 27001;
- **ISO/IEC 27005 – *Information technology – Security techniques – Information security risk management*:** fornece diretrizes para a implementação de um processo de gestão do risco da segurança da informação;
- **ISO/IEC 27006 – *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security systems*:** especifica os requerimentos e fornece diretrizes para as entidades que executam a auditoria e podem certificar a conformidade com a ISO/IEC 27001;

- **ISO/IEC 27007 – *Information technology – Security techniques – Guidelines for information security management systems auditing*:** oferece diretrizes de como as entidades competentes devem conduzir as auditorias ao SGSI;
- **ISO/IEC TR 27008 – *Information technology – Security techniques – Guidelines for auditors on information security controls*:** fornece uma metodologia aos auditores para a avaliação tanto da implementação e da operação dos controlos de segurança de informação, como da conformidade com os *standards* de segurança de informação adotados;
- **ISO/IEC 27009 – *Information technology – Security techniques – Sector-specific application of ISO/IEC 27001*:** define os requisitos para utilizar a ISO/IEC 27001 em qualquer setor específico;
- **ISO/IEC 27010 – *Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications*:** fornece diretrizes para ajudar a manter a segurança da informação quando esta tem de ser partilhada com outras organizações ou setores;
- **ISO/IEC 27011 – *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*:** fornece suporte na implementação dos controlos de segurança em organizações na área das telecomunicações;
- **ISO/IEC 27013 – *Information technology – Security techniques – Guidance on integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*:** oferece apoio na integração dos *standards* dos sistemas de gestão da norma ISO/IEC 27001 com os sistemas de gestão de outras normas;
- **ISO/IEC 27014 – *Information technology – Security techniques – Governance of information security*:** fornece diretrizes para a gestão e controlo da segurança da informação;
- **ISO/IEC TR 27016 – *Information technology – Security techniques – Information security management – Organizational economics*:** fornece uma metodologia que permite que as organizações compreendam como valorizar os seus ativos de informação, numa perspetiva económica;
- **ISO/IEC 27017 – *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*:**

fornece suporte na implementação dos controlos de segurança no provisionamento e utilização de serviços de nuvem;

- **ISO/IEC 27018 – *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public cloud acting as PII processors*:** define os controlos e as diretrizes que devem ser adotadas na proteção da informação de identificação pessoal;
- **ISO/IEC 27019 – *Information technology – Security techniques – Information security controls for the energy utility industry*:** fornece suporte na implementação dos controlos de segurança na indústria de energia;
- **ISO/IEC 27021 – *Information technology – Securtiy techniques – Information security management – Competence requirements for information security management systems professionals*:** especifica os requisitos da competência dos profissionais que estão envolvidos no estabelecimento, implementação, manutenção ou melhoria do SGSI. (ISO/IEC 27000:2018)

Figura 3 - Família de normas do SGSI.



Fonte: Adaptado de ISO/IEC 27000:2018

3.3 ISO/IEC 27001

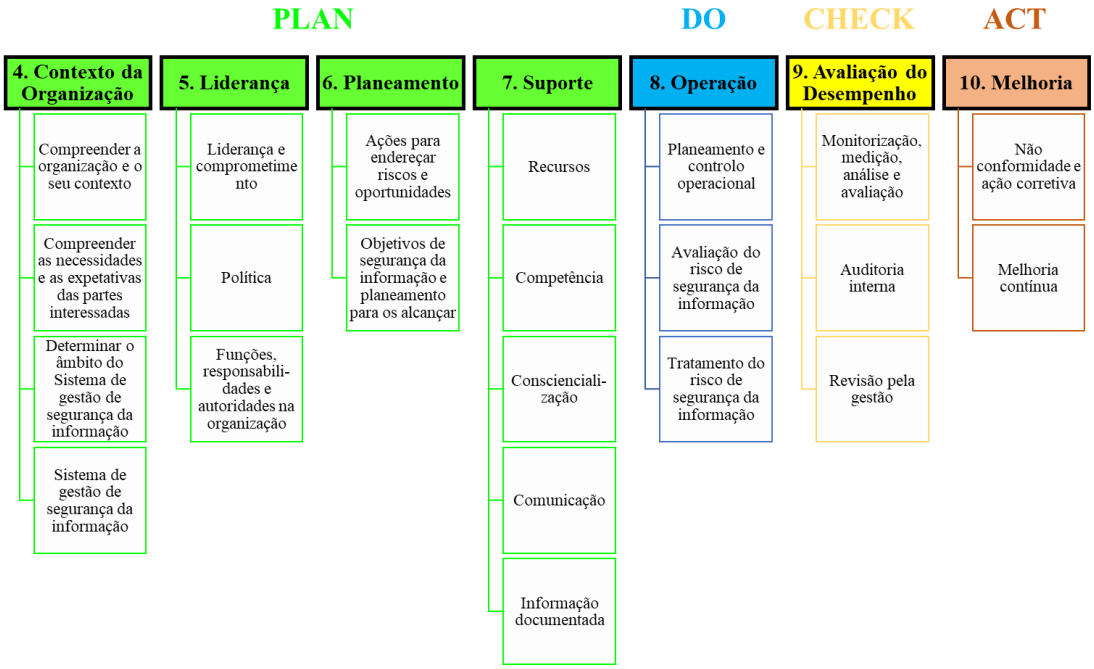
A norma ISO/IEC 27001 é a única da família apresentada que tem uma versão portuguesa. Foi a primeira norma para um SGSI em Portugal e foi preparada pela Comissão Técnica de Normalização CT 163, que é coordenada pelo Organismo de Normalização Sectorial, itSMF Portugal – Associação Portuguesa de Gestores de Serviços de Tecnologias

da Informação. Este é o organismo de normalização para a área das tecnologias da informação nomeado pelo Instituto Português de Qualidade.

Como referido, a norma ISO/IEC 27001 apresenta especial relevância pelo facto de ser a única passível de certificação dentro das normas da família 27000 e fornecer os requisitos para o SGSI. A seguir às secções introdutórias (secções 1, 2 e 3), esta norma apresenta as cláusulas (secções 4 a 10) com as especificações dos requisitos do SGSI, que permitem que as organizações estabeleçam, implementem, mantenham e melhorem o sistema que garante a confidencialidade, integridade e disponibilidade da informação. No final, expõe ainda dois anexos, A e B. O Anexo A lista os controlos de segurança que a organização pode realizar para alcançar a conformidade com os requisitos anteriores. Já o Anexo B é meramente informativo.

Esta norma nem sempre apresentou o mesmo formato. As principais mudanças da norma elaborada em 2005 para a retificada em 2013 têm o intuito de a tornar mais compatível com outras normas, alinhando, desta forma, as suas estruturas e definições. Os requisitos para o SGSI foram tornados mais claros e houve alguns controlos removidos e outros adicionados. No entanto, a filosofia permanece a mesma: concede bastante importância aos processos de avaliação e tratamento dos riscos (devem ser a base do estabelecimento e implementação do SGSI) e baseia a sua dinâmica e implementação no ciclo PDCA (*plan-do-check-act*). Enquanto que na versão de 2005 este ciclo estava explícito na norma e a estrutura estava construída à volta dele, na versão de 2013 não há referência ao ciclo, mas este está implícito. Este ciclo é um método iterativo de controlo e de melhoria contínua. O objetivo é que as organizações melhorem os seus processos de forma contínua e consigam, assim, identificar e corrigir falhas e aperfeiçoar a sua performance. Na Figura 4 encontram-se esquematizadas todas as cláusulas da norma e a sua relação com o ciclo PDCA.

Figura 4 - Estrutura da norma ISO/IEC 27001:2013 e relação com o ciclo PDCA.



Fonte: Adaptado da página web "Trace International"[12]

Dentro da cláusula número 6: Planeamento, no âmbito das ações para endereçar riscos e oportunidades, é pedido que as organizações elaborem um processo de avaliação dos riscos e outro de tratamento desses riscos. Um dos requisitos para elaborar esse processo de tratamento dos riscos é que sejam selecionados e aplicados os controlos de segurança apropriados e, em seguida, sejam comparados com os controlos de segurança do Anexo A de forma a verificar se não foram omitidos alguns controlos necessários (NP ISO/IEC 27001:2013). Este anexo expõe os controlos e os objetivos de controlo. Como é evidenciado na Tabela 1, existe um total de 114 controlos organizados em 14 secções. Cada secção possui um ou mais objetivos de controlo e cada objetivo de controlo pode ser alcançado por um ou mais controlos.

Uma ideia errada sobre a norma ISO/IEC 27001 para um SGSI, é que esta se direciona exclusivamente para a área das Tecnologias de Informação (TI). No entanto, conforme se verifica na Figura 4 e na Tabela 1, a grande maioria das cláusulas e dos controlos são direcionados à gestão organizacional. De acordo com a entrevista de Everett (2011), Mike Gillespie, diretor da consultoria em segurança da informação na consultora *Advent-*

[12] Disponível em https://isoconsultantkuwait.com/2019/07/20/2392/ (Consultado em 02-06-2020)

IM, afirmou mesmo que uma organização "pode realmente obter a certificação do *standard* sem ter um único computador no negócio" (Everett, 2011, p. 6).

Tabela 1 - Secções, objetivos de controlo e controlos.

Secções	Nº Objetivos de Controlo	Nº Controlos
A.5 Políticas de segurança da informação	1	2
A.6 Organização de segurança da informação	2	7
A.7 Segurança na gestão de recursos humanos	3	6
A.8 Gestão de ativos	3	10
A.9 Controlo de acesso	4	14
A.10 Criptografia	1	2
A.11 Segurança física e ambiental	2	15
A.12 Segurança de operações	7	14
A.13 Segurança de comunicações	2	7
A.14 Aquisição, desenvolvimento e manutenção de sistemas	3	13
A.15 Relações com fornecedores	2	5
A.16 Gestão de incidentes de segurança da informação	1	7
A.17 Aspetos de segurança da informação na gestão de continuidade do negócio	2	4
A.18 Conformidade	2	8
14 SECÇÕES		114 CONTROLOS

Fonte: Adaptado de Correia, 2016

Embora o objetivo da norma seja garantir a segurança da informação, os *standards* que ela apresenta são para estabelecer, implementar, manter e melhorar um sistema de gestão. Por esse motivo, garantir que a gestão da organização está comprometida em obter a conformidade com estes *standards* e não deposita todas as responsabilidades para o departamento de TI, é um fator crucial para que a organização alcance a certificação ISO/IEC 27001 e os objetivos estabelecidos para o SGSI (Casaca & Correia, 2010; Everett, 2011; Hsu, Wang, & Lu, 2016; Ifinedo, 2011; Koskosas & Paul, 2004; Martins & Santos, 2005; Syreyshchikova et al., 2019; Wessel & Vries, 2013).

3.4 Implementação

No processo de desenvolver e implementar um SGSI são aplicados os *standards* requeridos, neste caso pela norma ISO/IEC 27001. De acordo com esta norma, "o estabelecimento e implementação de um sistema de gestão de segurança da informação de uma organização são influenciados pelas necessidades e objetivos da organização, pelos requisitos de segurança, pelos processos organizacionais utilizados e pela dimensão e estrutura da organização" (NP ISO/IEC 27001:2013, p. 5). Neste sentido, a organização,

antes de iniciar este processo, deve realizar uma introspeção para compreender o que faz sentido e o que não faz no seu contexto específico. Nesta fase inicial, a organização deve definir:

- a política de segurança de informação que descreva as recomendações, as regras, as responsabilidades e as práticas de segurança;
- o âmbito do SGSI, incluindo a identificação dos ativos que serão abrangidos pelo SGSI;
- todo o processo de gestão do risco (Martins & Santos, 2005; Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2019).

Desta forma, a organização é capaz de avançar para o passo seguinte e selecionar e aplicar os controlos apropriados.

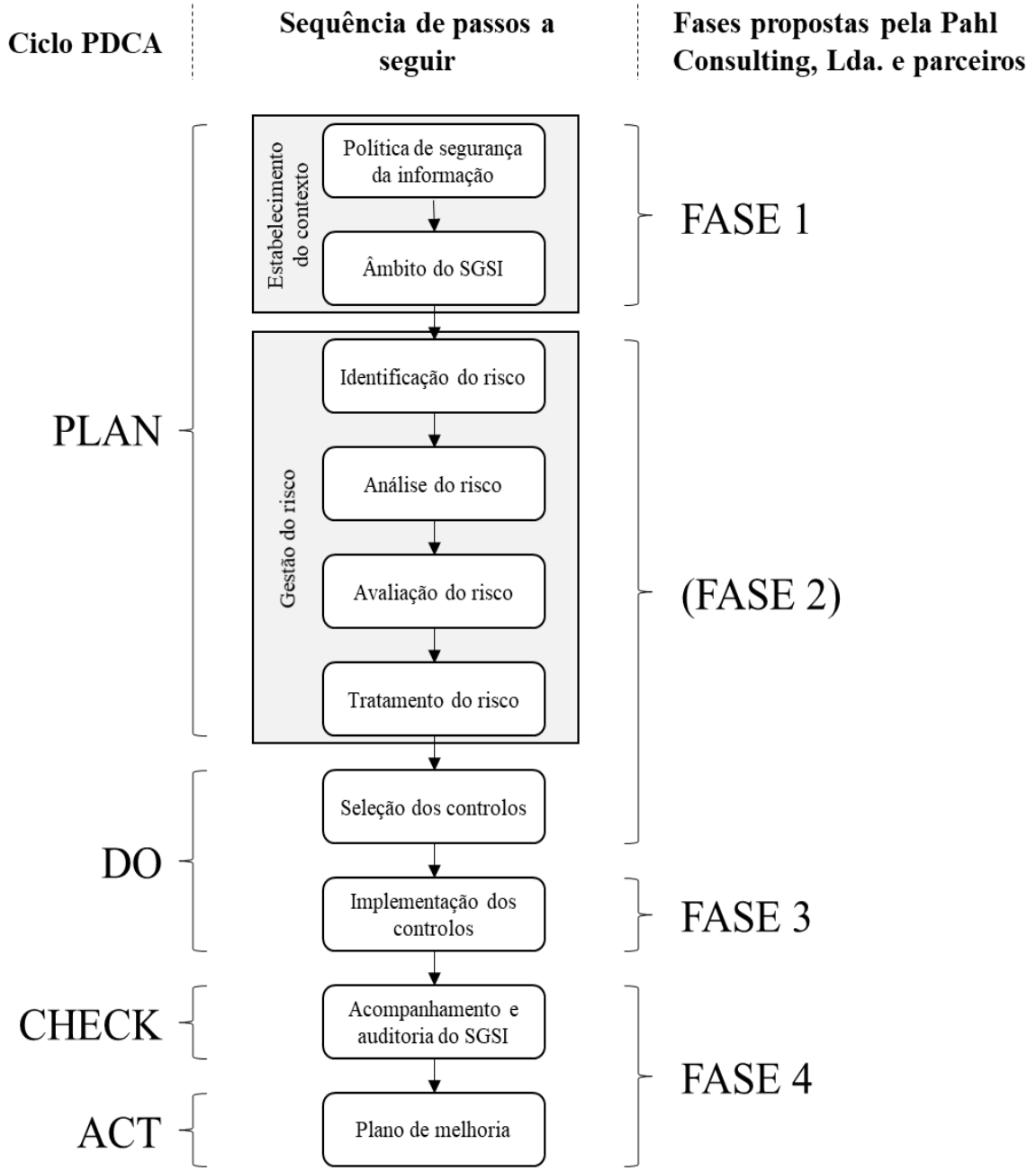
A norma ISO/IEC 27001 não indica a ordem pela qual os requisitos devem ser implementados. No entanto, a forma mais eficaz de implementar um SGSI é de forma faseada. A divisão implícita na norma, e a mais usualmente aceite, é a divisão pelas fases do ciclo PDCA supramencionado. Assim, a organização deve dividir este processo de estabelecer, implementar, manter e melhorar o SGSI nestas quatro fases. Na fase inicial do ciclo, *Plan*, a organização deve estabelecer, desenvolver e definir todo o processo através da análise introspetiva explicada acima. Na segunda fase do ciclo, *Do*, a organização irá, então, selecionar e implementar os controlos apropriados de acordo com as análises feitas anteriormente. Muitas vezes, estas duas fases acabam por ser divididas em três. Como na prática a implementação dos controlos é uma etapa exigente e demorada, as organizações podem optar por dedicar uma fase exclusivamente a este tópico.

Efetivamente, a implementação está concluída após estas duas fases do ciclo PDCA, *Plan* e *Do* (Martins & Santos, 2005). Contudo, o SGSI ainda não está completo. Ainda não foi alcançada a conformidade com a norma ISO/IEC 27001, porque esta exige outros requisitos que garantam que os critérios definidos nas primeiras fases são de facto adequados ao contexto da organização, de que esta está de facto a agir em conformidade com esses critérios e que existe um plano para a organização ir verificando e atualizando esses critérios regularmente. Estes requisitos traduzem-se nas duas últimas fases do ciclo PDCA, *Check* e *Act*. Porém, frequentemente estas fases são agregadas numa só.

Todo este processo está esquematizado na Figura 5. Esta figura mostra, ainda, a diferença entre as fases do ciclo PDCA e as fases propostas pela entidade de acolhimento do

estágio associado a este relatório em conjunto com os respetivos parceiros. Em seguida, serão abordadas mais detalhadamente estas diferentes etapas do processo de implementação de um SGSI. As fases estudadas serão: o estabelecimento do contexto, a gestão do risco, a seleção e implementação de controlos e a manutenção e melhoria contínua.

Figura 5 - Processo de implementação de um SGSI.



Fonte: Adaptado de Martins e Santos, 2005 e ISO/IEC 27005:2018

3.4.1 Estabelecimento do contexto

Após uma organização tomar, efetivamente, a decisão de adotar uma norma e implementar um SGSI, terá de efetuar algumas preparações iniciais, com o intuito de planear e delinear esse projeto e garantir que dispõe das condições e recursos necessários. Após ser executada esta fase inicial, a entidade deverá dispor de um plano de ações que deverá iniciar na fase de estabelecer o contexto da organização. Nesta fase deve ser estudada a situação interna e externa em que a organização se encontra, nomeadamente, em relação aos seus sistemas de gestão da segurança e do risco da informação. Para isso, devem ser definidos tanto os critérios básicos da segurança da informação da organização e do sistema de gestão do risco, como o âmbito e os limites do SGSI e do sistema de gestão do risco (ISO/IEC 27005:2018). Desta forma, a organização pode identificar quais os ativos que deverão ser abrangidos no SGSI e comparar os critérios estabelecidos como necessários para garantir a segurança destes ativos, com os critérios já respondidos pela organização.

Resumidamente, nesta fase de estabelecimento do contexto, a organização deve em primeiro lugar elaborar uma política de segurança da informação onde descreva todos os critérios essenciais, como as recomendações, as regras, as responsabilidades e as práticas de segurança e, em seguida, definir qual o âmbito e os limites desta política (Martins & Santos, 2005). Esta política de segurança de informação vai permitir que a organização realize uma *gap analysis* entre a sua situação corrente e a situação idealizada para o SGSI. Já a definição do âmbito e dos limites permite à organização identificar quais os ativos que devem não só ser alvo da *gap analysis*, como também devem estar na base do processo de identificação dos riscos.

A política de segurança da informação deve ser adaptada por cada organização de acordo com os seus objetivos e situação específica. Como já referido, a política deverá descrever os critérios de segurança. No entanto, deve também apresentar outras características, tais como:

- Ter em conta a classificação das informações e as necessidades e os objetivos de segurança;
- Definir as responsabilidades gerais e específicas;
- Ser aprovada pela equipa de gestão;
- Ser apropriadamente divulgada pela organização;
- Ser revista periodicamente e, se necessário, atualizada;

- Estar em conformidade com a legislação aplicável;
- Explicitar as consequências do não cumprimento (Martins & Santos, 2005).

O âmbito deve definir quais os ativos que são abrangidos no SGSI, tais como: equipamentos, sistemas, informações, pessoas, infraestruturas, serviços, entre outros (Martins & Santos, 2005). Ao estabelecer o âmbito e os limites, tanto do sistema de gestão dos riscos como do SGSI, devem ser consideradas algumas informações sobre a organização, onde se inclui:

- A política de segurança da informação;
- Os objetivos estratégicos, estratégias e políticas da organização;
- A estrutura da organização;
- O sistema de gestão do risco da organização;
- Os ativos de informação;
- A localização e características geográficas da organização;
- As expetativas dos *stakeholders*;
- O ambiente sociocultural (ISO/IEC 27005:2018).

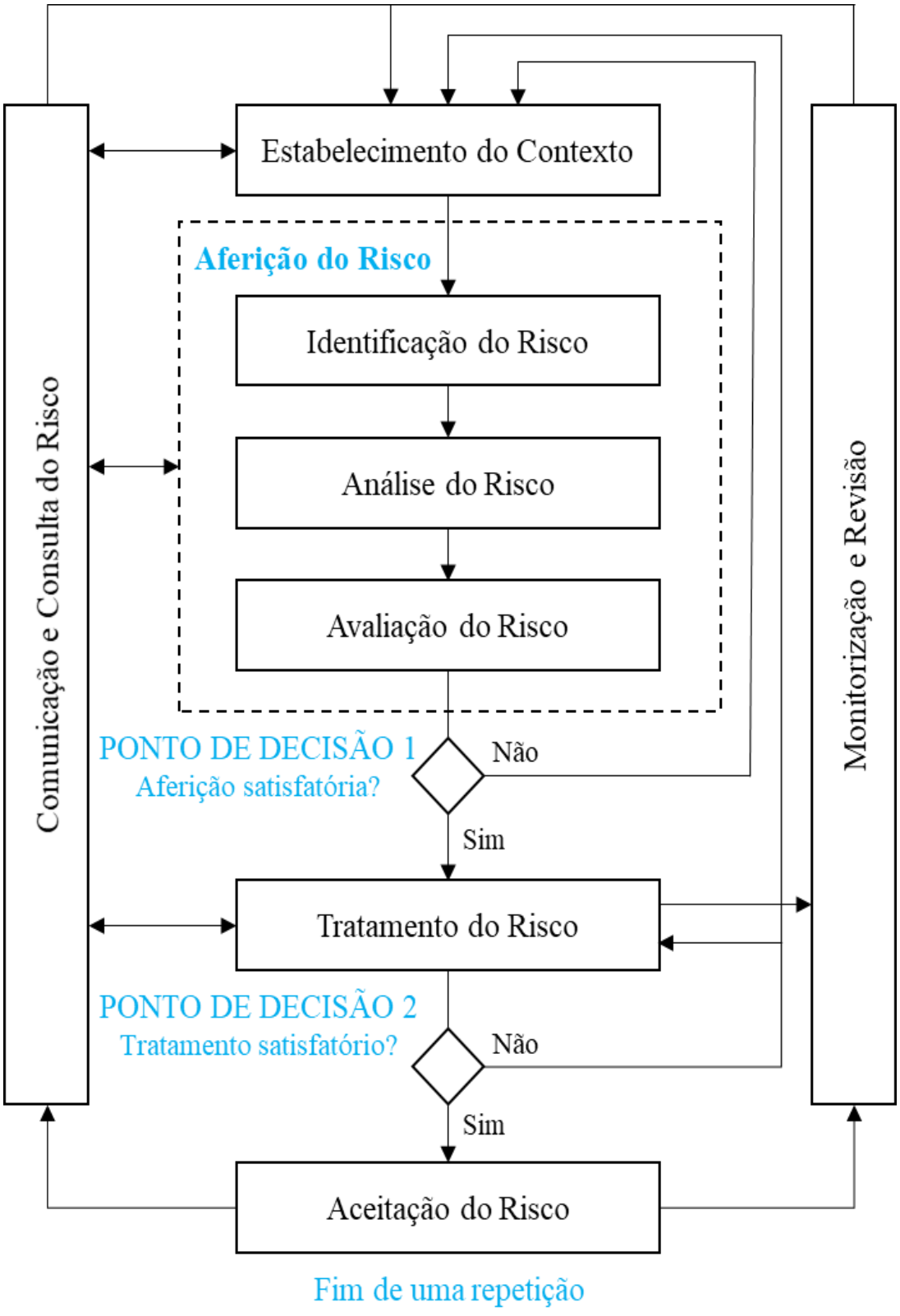
3.4.2 Gestão do risco de segurança da informação

A gestão do risco da segurança da informação é uma parte vital de qualquer SGSI, pois garante que os riscos de segurança da informação são sistematicamente identificados, analisados e tratados de acordo com a política de gestão de risco das organizações (Brunner et al., 2020). A norma ISO/IEC 27005 fornece diretrizes para a implementação de um processo de gestão do risco de segurança de informação em conformidade com os requisitos da norma ISO/IEC 27001. Após o estabelecimento do contexto, a norma ISO/IEC 27005 divide o processo de gestão do risco da segurança da informação em duas etapas principais: a aferição e o tratamento do risco. A primeira consiste nos processos de identificação, análise e avaliação dos riscos. Já a segunda abrange o processo de tratamento destes riscos e a sua consequente aceitação ou rejeição. Este é um processo iterativo que fornece particular importância à comunicação dos riscos e exige uma monitorização e revisão contínua, como é observado na Figura 6.

O estabelecimento do contexto foi a etapa abordada na secção anterior. Todo o contexto interno e externo relativo à segurança da informação necessita de ser estabelecido. Esta fase, no âmbito do processo de gestão do risco, exige também que sejam identificados

ou estabelecidos os critérios de gestão do risco, como os critérios para a avaliação e para a aceitação do risco.

Figura 6 - Processo de gestão do risco da segurança da informação.



Fonte: Adaptado de ISO/IEC 27005:2018

Segue-se a etapa de aferição do risco. O objetivo desta fase é determinar o valor dos ativos de informação, identificar possíveis ameaças e vulnerabilidades à segurança da informação, identificar as possíveis consequências das ameaças detetadas e, desta forma, classificar os riscos identificados de acordo com os critérios de avaliação estabelecidos no passo anterior (ISO/IEC 27005:2018). Como esquematizado na Figura 6, esta etapa divide-se em três passos consecutivos: identificação, análise e avaliação do risco.

O processo de identificação dos riscos atua sobre o âmbito e os limites definidos na fase de estabelecimento do contexto. O objetivo é determinar os eventos que poderão causar perdas para a organização e compreender o modo e as razões pela qual esta perda pode acontecer (ISO/IEC 27005:2018). Para isso, a ISO/IEC 27005 propõe que, após serem identificados os ativos que fazem parte do âmbito e estão dentro dos limites do processo de gestão do risco da segurança da informação, sejam identificadas as ameaças e as suas origens. Estas ameaças podem ser de origem humana, ambiental ou tecnológica; podendo ser motivadas por comportamentos maliciosos ou não maliciosos e podem, ainda, ser intencionais ou acidentais (Jouini, Ben, Rabai, & Ben, 2014). Em seguida, é importante identificar os controlos existentes que podem ser adereçados a estas ameaças. Com esta informação é possível identificar as vulnerabilidades existentes que podem ser exploradas pelas ameaças identificadas e, por fim, serem determinadas as consequências que as possíveis perdas resultantes dessas ameaças terão nos ativos da organização (ISO/IEC 27005:2018).

Existem diversos métodos de análise do risco. A ISO/IEC 27005 fornece duas metodologias para este processo: qualitativa e quantitativa. O método qualitativo utiliza escalas de atributos (por exemplo: baixa, média ou alta) para classificar as potenciais consequências e a probabilidade de estas ocorrerem. Já a abordagem quantitativa usa uma escala numérica para estes atributos, normalmente calculada através de fontes de dados estatísticos. No geral, os métodos qualitativos são mais adotados (Brunner et al., 2020). No entanto, a norma ISO/IEC 27005 não dá preferência a nenhuma das metodologias. Refere apenas que a abordagem adotada deve ser consistente com os critérios de avaliação do risco definidos na primeira fase deste processo. Após serem analisadas e classificadas as consequências e a probabilidade dessas ocorrerem, é então estimado o nível de risco de todos os cenários de incidentes identificados.

Para concluir a etapa de aferição do risco, são avaliados os potenciais incidentes identificados através de uma comparação entre o nível de risco estimado e o critério de

avaliação definido na etapa de estabelecimento do contexto do processo de gestão do risco da segurança da informação. Deste modo, obtém-se uma lista com os riscos prioritários para o passo seguinte de tratamento dos riscos (ISO/IEC 27005:2018).

Ao terminar a aferição do risco surge um ponto de decisão que pretende confirmar se as informações reunidas até ao momento são suficientes para determinar quais as ações necessárias para reduzir os riscos a um nível aceitável. Se as informações forem suficientes, o processo segue para a etapa de tratamento dos riscos, mas se forem insuficientes é necessário rever o contexto estabelecido e repetir novamente esta etapa de aferição do risco (ISO/IEC 27005:2018).

Se for decidido que as informações são suficientes, o processo entra então na etapa de tratamento dos riscos. O intuito é selecionar os controlos apropriados para combater os riscos e definir um plano de tratamento dos mesmos. A ISO/IEC 27005 fornece quatro opções para transformar os riscos aferidos em riscos residuais: modificar, reter, evitar ou partilhar os riscos. A modificação do risco refere-se à introdução, remoção ou alteração dos controlos de segurança para que os riscos sejam reavaliados como aceitáveis. A retenção dos riscos pode ser utilizada quando não são identificados controlos para os riscos aferidos ou quando o custo desses controlos é superior ao valor das possíveis perdas e, por esse motivo, não é executada nenhuma ação adicional. A opção de evitar os riscos consiste em evitar a execução das atividades e condições que fazem do risco identificado uma potencial ameaça. Finalmente, a partilha dos riscos pretende distribuir o risco por terceiros, por exemplo ao contratar um seguro que cubra as potenciais consequências. Não existe um método melhor que os outros, cada opção deve ser selecionada de acordo com os resultados da avaliação dos riscos (ISO/IEC 27005:2018).

Do tratamento dos riscos resultam os riscos residuais, porém estes podem ainda não se encontrar num nível aceitável de acordo com os critérios de aceitação do risco estabelecidos na fase de estabelecimento do contexto. O segundo ponto de decisão, representado na Figura 6, pretende indicar que, se os riscos residuais estiverem num nível aceitável então são aceites, mas se não se posicionarem num nível aceitável é necessário refazer todo o processo revendo o contexto estabelecido, repetindo a aferição dos riscos e, se necessário, desenvolvendo um novo plano de tratamento dos riscos (ISO/IEC 27005:2018).

Quando os riscos são aceites é concluída a primeira iteração do processo. Contudo, o processo e os seus resultados precisam de ser monitorados e revistos de forma contínua, com a finalidade de garantir que estes se mantêm atualizados e corretos. Para além de tudo isto, é importante garantir que, durante todo o processo de gestão do risco da segurança da informação, os riscos e os resultados obtidos em cada etapa são devidamente comunicados e disponibilizados aos gestores e colaboradores apropriados (ISO/IEC 27005:2018).

3.4.3 Seleção e implementação de controlos

Para efeitos de melhor compreensão teórica, a seleção de controlos é considerada separadamente do processo de gestão do risco, apesar de na prática se pretender fazer na mesma etapa que a gestão do risco pelo facto de esta estar correlacionada com o processo de tratamento do risco.

O processo de gestão do risco vai evidenciar quais são as medidas corretivas que deverão ser aplicadas na organização com o intuito de reduzir os riscos identificados a um nível aceitável (Martins & Santos, 2005). O Anexo A da norma ISO/IEC 27001 fornece um extenso conjunto de controlos que uma organização pode adotar para cobrir esses riscos. Todavia, a organização pode adotar mais controlos que os propostos na norma se achar que são necessários para mitigar os riscos identificados. Mas também não é necessário adotar todos os controlos expostos na norma. Para além de existir uma possibilidade de estarem a ser alocados recursos à implementação de controlos desnecessários, Wessel e Vries (2013) deduziram, ainda, que optar por uma implementação cega de todos os controlos sem efetuar uma análise dos riscos, influencia negativamente a atitude dos colaboradores em relação à adoção destes *standards* por parte da organização. Tal possui efeitos negativos na performance da organização (este assunto voltará a ser abordado mais adiante). Portanto, a seleção dos controlos a implementar deve ter por base uma comparação com os controlos já existentes no contexto da organização e uma avaliação dos riscos que são necessários gerir. A norma ISO/IEC 27001 exige a criação de uma declaração de aplicabilidade para completar esta etapa. Esta declaração consiste num documento onde deverão estar listados todos os controlos do Anexo A e outros, se forem necessários, com uma justificação para a decisão de implementar ou não cada controlo.

O processo de implementação dos controlos selecionados constitui um processo quase exclusivamente prático. Esta etapa consiste, muitas vezes, apenas na criação de padrões, normas e políticas internas a serem obedecidas (Martins & Santos, 2005), com o

intuito de alcançar o objetivo de segurança da informação visado por cada controlo específico. Porém, esta implementação pode exigir a aquisição de novos ativos, como equipamentos, infraestruturas, tecnologias, *softwares* ou *hardwares*, pessoas, entre outros.

3.4.4 Manutenção e melhoria contínua

O ambiente de segurança e as condições internas de uma organização variam ao longo do tempo. Por esse motivo, é necessário monitorar e melhorar os elementos do SGSI de forma contínua ao longo do tempo (Szczepaniuk et al., 2019). Para monitorar os controlos implementados pode ser estabelecido um conjunto de indicadores que permitam observar as condições de funcionamento e desempenho dos elementos específicos analisados (Martins & Santos, 2005). Para além de manter estes critérios indicativos é importante que a organização desenvolva auditorias internas com o propósito de confirmar se os controlos implementados estão a responder ao que era pretendido com a sua implementação e verificar se a organização está a agir, internamente, de acordo com os padrões, normas e políticas estabelecidas. A organização necessita estabelecer um plano para realizar estas auditorias periodicamente. Para além disso, é importante que estas auditorias considerem, não só o contexto da organização no momento da implementação do SGSI, como também a evolução no contexto e ambiente da mesma. Todo o processo de implementação do SGSI deve ser revisto e, caso se detete alguma incoerência, a organização deve estar preparada para adotar as medidas corretivas necessárias para voltar a atuar em conformidade com o SGSI proposto. Desta forma, é possível manter o SGSI controlado, permitindo que este seja aprimorado regularmente.

3.5 Impacto da certificação ISO/IEC 27001 na performance da organização

Antes da implementação é necessário que os decisores e investidores estejam confiantes de que os benefícios operacionais e de negócio vão, de facto, compensar todos os inconvenientes. Garantir este comprometimento pode ser complicado e, por esse motivo, ter uma noção concreta das vantagens e dos inconvenientes de implementar este género de *standards* é de extrema relevância para quem é responsável por tomar a decisão de investir ou não nessa implementação.

As principais contrariedades rapidamente identificadas são as quantidades elevadas de recursos financeiros, esforço e tempo que são necessárias. A norma ISO/IEC 27001 tem,

ainda, a particularidade de exigir um grande número de requisitos, o que também pode afastar algumas organizações, levando estas a adiar a decisão de adotar um SGSI ou a optar por fazê-lo, mas através de outras normas mais leves (Everett, 2011).

Quanto aos pontos favoráveis à adoção desta norma destacam-se duas categorias de benefícios: internos e externos. Os primeiros dizem respeito a melhorias nos procedimentos, que se podem traduzir em reduções nos custos derivados tanto da simplificação de processos, como da redução do número de incidentes relacionados com a segurança da informação. Os benefícios externos referem-se a melhorias de mercado e nas relações com os clientes, que são o resultado da imagem transmitida de que a organização está preocupada com a segurança das informações (Hsu et al., 2016).

Apesar da escassez de estudos referentes ao impacto da certificação ISO/IEC 27001 na performance das organizações, é possível encontrar resultados contraditórios. Por exemplo, Wessel e Vries (2013), ao estudarem organizações que obtiveram essa certificação, verificaram que elas conseguem alcançar a maior parte dos seus objetivos. Eles identificaram, ainda, quatro perspetivas em que é possível verificar esse impacto positivo:

- **Financeira:** confirmaram-se que alguns custos subiram, mas, no geral, estes *standards* trouxeram benefícios financeiros às organizações que os adotaram;
- **Dos clientes:** a demonstração de credibilidade e confiança na proteção das informações dos clientes fez aumentar a satisfação destes;
- **Interna:** verificaram-se melhorias em diversos processos de extrema importância para as organizações, como os de gestão de alterações, gestão de incidentes, gestão de ativos, entre outros;
- **De crescimento e aprendizagem:** não só se confirmou a possibilidade de haver um aumento das oportunidades das organizações com esta certificação, como também permitiu aliviar o trabalho dos funcionários através da utilização de procedimentos e métodos pré-definidos e compreendidos.

Por outro lado, Hsu et al. (2016) constataram que a certificação ISO/IEC 27001 não resulta numa melhor performance financeira. Ao estudarem indicadores financeiros como o ROA (*return-on-assets*) e o total de ativos de diversas organizações, concluíram que o impacto da certificação nestes indicadores não é significativo.

Uma justificação para estes resultados divergentes pode ser encontrada no estudo de Hudson e Orviska (2013), onde foi verificado que existem diversos fatores externos capazes

de aumentar ou diminuir a probabilidade destes *standards* terem um impacto positivo na performance da organização. Por exemplo, organizações exportadoras ou sediadas em grandes cidades tendem a obter melhores resultados do que as não exportadoras ou localizadas em zonas rurais (Hudson & Orviska, 2013).

Posto isto, retira-se desta informação que o impacto da certificação ISO/IEC 27001 na performance pode assumir diferentes formas de acordo com variáveis não controladas pela organização, mas mesmo que não apresente um impacto significativo na performance financeira das organizações, estas tendem a sentir-se satisfeitas noutros campos, como por exemplo a nível interno ou na relação com os clientes.

Em seguida, serão aprofundados três temas que são cruciais para compreender o impacto que a certificação ISO/IEC 27001 pode ter na performance de uma organização: a vantagem competitiva, o comportamento dos funcionários e a integração com outros standards ISO.

3.5.1 Vantagem Competitiva

Obter vantagens competitivas é, certamente, um dos principais objetivos das organizações ao adotar este género de *standards*. Contudo, existem fatores que se não forem considerados vão impedir que as organizações alcancem este objetivo.

Apesar de não se tratar de estudos referentes à certificação ISO/IEC 27001, é importante notar as observações de Su et al. (2015), de que o momento da adoção destes *standards* é um fator decisivo na aquisição de uma vantagem competitiva. Uma organização que decida adotar esta norma mais precocemente estará em vantagem em relação a uma organização que tome esta decisão mais tarde. Esta importância é ainda agravada pelo facto destas normas trazerem alguma padronização nos sistemas de gestão destas organizações, o que faz com que se reduza a heterogeneidade dos recursos que poderiam gerar uma vantagem competitiva (Su et al., 2015). Esta ideia é ainda corroborada por Benner e Veloso (2010) que concluíram, também, que há uma vantagem competitiva para quem adota estes *standards* primeiro, mas que essa vantagem se dissipa à medida que outras organizações vão alcançando conformidade com esses *standards*. Estes resultados vão ao encontro da teoria baseada nos recursos (*resource-based view* - RBV) que afirma que, para uma fonte de vantagem competitiva ser sustentável para além de acrescentar valor, esta tem de ser rara e difícil de imitar e substituir.

Estes estudos referem-se à certificação de outras normas, nomeadamente a ISO 9001 relativa a um sistema de gestão da qualidade e à ISO 14001 referente a um sistema de gestão do ambiente. Porém, são todos *standards* para um sistema de gestão, assentam nas mesmas ideologias de gestão como a continuidade do negócio ou melhoria contínua do sistema e os processos de certificação são, também, semelhantes. Devido a estas similaridades seria imprudente não considerar estes estudos, o que não descarta a necessidade de atentar devidamente nas diferenças entre os *standards*.

Assim, obter esta certificação antes dos concorrentes, será certamente crucial para que a organização consiga alcançar uma vantagem competitiva, mesmo que esta seja apenas temporária. E, devido à crescente relevância que esta norma está a adquirir em diversos setores, esta certificação passará a ser um requisito muito procurado (como já acontece com a norma ISO 9001). Nesta situação, a certificação ISO/IEC 27001 deixará de representar uma vantagem para quem a possui, mas sim uma desvantagem para quem ainda não a conseguiu obter.

3.5.2 Comportamento dos funcionários

O comportamento dos funcionários de uma organização pode também ser um fator determinante para que a implementação da norma ISO/IEC 27001 tenha um impacto positivo ou negativo na organização. A resistência dos funcionários à mudança está na origem do insucesso de muitos projetos. Nesse sentido, Merhi e Ahluwaia (2018) estudaram como é que a resistência dos funcionários à adoção de um sistema de informação é indiretamente afetada pela punição e pela certeza de deteção dos atos dos funcionários que vão contra as políticas de segurança da informação. O impacto direto da punição destes atos na resistência dos funcionários à mudança é inconsistente de caso para caso. Por esse motivo, estes autores estudaram o impacto indireto através de crenças, padrões e valores. Os resultados obtidos evidenciam que a punição de atos de inconformidade com as políticas de segurança da informação possui efeitos nas crenças e que estas crenças e padrões, por sua vez, afetam negativamente a resistência dos funcionários à adoção de novos *standards*. (Merhi & Ahluwalia, 2018). Estes resultados completam e vão ao encontro dos resultados obtidos anteriormente por Ifinedo (2011). Este, com base nas teorias de comportamento planeado e de proteção da motivação, demonstrou que as mesmas normas subjetivas avaliadas por Merhi e Ahluwalia apresentam um impacto positivo na intenção dos colaboradores em agir em conformidade com as políticas de segurança da informação. Para além das normas subjetivas, concluíram que a atitude dos colaboradores face à conformidade, o controlo

comportamental percecionado pelos colaboradores ou autoeficácia, a noção de que os colaboradores têm as competências necessárias para agir em conformidade e a perceção destes para a existência de vulnerabilidades eminentes, são todos fatores que influenciam positivamente a intenção destes colaboradores em agir em conformidade com as políticas de segurança de um sistema de informação (Ifinedo, 2011).

Já Koskosas e Paul (2004) destacaram a importância de haver uma forte confiança e cultura dentro da organização para que esta consiga uma performance positiva. Identificaram, ainda, a importância de haver uma eficaz comunicação dos riscos de segurança. Estes indicadores comportamentais têm como principal propósito alinhar os objetivos entre a organização e os seus membros. Desta forma seria possível aumentar o comprometimento e o esforço alocado pelos funcionários à adoção dos novos *standards*.

Todos estes resultados corroboram a ideia inicial de que existem fatores psicológicos que afetam a forma de agir dos colaboradores de uma organização no momento de adotarem novos *standards* para a segurança da informação. Este comportamento foi identificado por diversos autores como uma das principais ameaças ao sucesso do SGSI (e.g., Ifinedo, 2011; Koskosas & Paul, 2004; Merhi & Ahluwalia, 2018). O que se pode concluir é que as organizações não devem abdicar da aplicação de punições e controlos de comportamentos de resistência à mudança de políticas de segurança da informação, mas devem complementar estas medidas com outras que incitem a confiança, a uma atitude positiva e à compreensão da cultura da organização e das ameaças de segurança da informação. Desta forma, espera-se que a resistência dos colaboradores à adoção de novos *standards* diminua, o que influenciará positivamente a performance da organização relativa a estes *standards*.

3.5.3 Integração com outros *standards*

Outro fator que demonstrou ser relevante na análise do impacto que a certificação ISO/IEC 27001 tem na performance das organizações foi a sua integração com outros *standards*. Muitas organizações já possuem conformidade com algumas normas, como a ISO 9001 ou a ISO 14001. Quando estas organizações pretendem adotar outras normas ou quando perspetivam adotar mais do que uma norma, estas podem fazê-lo de forma independente umas das outras, mas isso levará ao dobro ou ao triplo do esforço exigido à organização. Uma solução é desenvolver um sistema de gestão integrado com diversos *standards* de normas diferentes, que permita que o conhecimento acumulado de um *standard* seja aplicado noutro *standard* (Su et al., 2015), não apenas a nível operacional, mas também

na integração de processos de gestão do risco. Barafort et al. (2016) identificaram diversos vetores de similaridades entre diversas normas ISO, incluindo a ISO/IEC 27001, e defendem que o desenvolvimento de processos de gestão do risco integrados e centralizados permitem que as competências organizacionais sejam fortificadas.

Esta solução, de integrar diferentes normas, permite melhorar a competitividade e a performance do sistema de gestão, reduzir a duplicação de tarefas, documentação, funções e estruturas, reduzir inúmeros custos e recursos necessários e aumentar a transparência da organização (Santos et al., 2017).

Resumidamente, se for possível, as organizações devem integrar os *standards* da norma ISO/IEC 27001 com outros *standards* que apresentem um conjunto significativo de semelhanças. Ao fazerem isso irão alcançar uma melhor posição no mercado (Wessel & Vries, 2013) e obter melhores resultados ao nível da performance da organização.

3.5.4 Outras variáveis relevantes

Existem outras variáveis capazes de influenciar o impacto desta certificação. Wessel e Vries (2013) identificaram, através do seu estudo, que a verificação de determinados fatores influenciava positivamente os resultados derivados da adoção da norma ISO/IEC 27001. Alguns deles já foram mencionados anteriormente:

- Participação dos departamentos orientados para os negócios e não apenas para TI, garantindo um alinhamento estratégico e operacional entre os dois setores;
- Compromisso da gestão de topo;
- Envolvimento e atenção dos funcionários durante a implementação;
- Melhoria contínua;
- Definição clara de como atuar em situações que seja necessário agir em não conformidade com os controlos e processos definidos;
- Experiência com outros *standards* de sistemas de gestão, ou ainda, integração de controlos com processos já existentes na organização.

Por outro lado, Casaca e Correia (2010) reuniram um extenso conjunto de fatores essenciais identificados por outros autores. Para além de alguns fatores já identificados, destacam-se:

- Alinhamento da segurança da informação com os objetivos da organização;

- Existência de um órgão responsável pela formulação e implementação das políticas de segurança da informação;
- Programa contínuo de educação e formação em segurança;
- Implementação baseada numa análise de risco adequada e não optar apenas por adotar todos os controlos sem fazer uma análise;
- Compreensão da importância de uma política de segurança da informação e da conformidade e monitorização por parte de todos os membros envolvidos neste processo.

Resumidamente, existem diversos fatores que devem ser estudados e atendidos pelas organizações ao adotarem uma norma para um SGSI, nomeadamente a ISO/IEC 27001, com o intuito de potenciarem o impacto positivo e o sucesso desta norma. Todavia, não se trata de uma receita que se deve seguir à risca para alcançar o sucesso. Como referido, existem fatores externos e intrínsecos capazes de potenciar ou amenizar este impacto positivo, como por exemplo o país, a localização (Hudson & Orviska, 2013) ou o setor e o nível de competitividade em que a organização atua (Su et al., 2015). Por esse motivo é que o primeiro requisito da norma ISO/IEC 27001 exige a compreensão do contexto da organização. Só assim é possível alcançar os objetivos esperados ao adotar esta norma ou outras semelhantes.

4. O estágio

Com base nos conceitos apresentados no capítulo anterior e no contexto proporcionado pela entidade de acolhimento serão explanadas, de seguida, as atividades desenvolvidas ao longo do estágio curricular na Pahl Consulting, Lda.

A posição assumida na Pahl Consulting, Lda. foi a de *Analyst*. O cargo de entrada na empresa é atribuído a quem tem menos de três anos de experiência e implica a execução de atividades de complexidade reduzida, habitualmente com instruções bem definidas, exigindo a aplicação de conhecimentos gerais e capacidades de análise.

Nesse âmbito, foi executado um leque diversificado de atividades durante este estágio. Muitas destas atividades não estavam integradas no projeto que deu origem ao tema e objetivo deste relatório. Por esse motivo, este capítulo será dividido em duas partes distintas: a primeira irá retratar as atividades elaboradas no âmbito do estágio e a segunda pretende abordar, exclusivamente, as atividades e considerações relacionadas com o projeto de implementação de um SGSI.

4.1 Atividades desenvolvidas durante o estágio

A primeira semana de estágio resumiu-se, essencialmente, à apresentação da empresa. Com esse intuito, foram apresentados os colegas de trabalho, as instalações e o contexto e situação atual da entidade. Durante esse período foi fornecida informação formativa, não só para compreender a realidade do que é trabalhar em consultoria e na Pahl Consulting, Lda. em específico, como também para introduzir as tarefas que iriam ser desenvolvidas no futuro.

No final da primeira semana e no princípio da semana seguinte, iniciaram-se as tarefas referentes a um projeto que pretendia analisar a conformidade das despesas imputadas a uma entidade pública com as condições impostas a essa entidade no momento da atribuição de um fundo social europeu. Para o efeito, foram efetuadas verificações administrativas e no local, de acordo com os procedimentos estabelecidos pela organização para estas situações. Nos primeiros dias, preencheram-se documentos que pretendiam relatar a situação verificada no local nas semanas anteriores, através de uma base dados que dispunha as informações necessárias.

No entanto, a gestão da Pahl Consulting, Lda. efetuou uma avaliação à alocação dos seus recursos humanos e apercebeu-se que havia um *Analyst* neste projeto que seria mais útil a realizar outras funções. Por esse motivo, no final da segunda semana e nas semanas seguintes, foram realizadas tarefas de carácter mais administrativo. Foi pedido que se criassem e se estruturassem alguns documentos para mais tarde serem preenchidos, e que se traduzissem outros de inglês para português. Neste período foi estabelecido o primeiro contacto com o projeto de implementação de um SGSI, mas ainda sem ser a título definitivo. Foi também solicitado que se preparassem e completassem candidaturas da entidade a concursos públicos. Estas funções consistiam em apurar os requisitos exigidos pela entidade adjudicante e em completar a candidatura da Pahl Consulting, Lda. a esse concurso, de forma a garantir que os requisitos fossem cumpridos. Por fim, este período compreendeu, ainda, atividades de *benchmark*, em que o objetivo foi comparar diferentes *softwares* de gestão do risco para identificar qual a solução do mercado que respondia de forma mais completa aos requisitos pedidos por um cliente interessado em adotar uma solução informatizada para auxiliar o processo de gestão dos riscos. Nesta atividade foi necessário:

- averiguar os requisitos exigidos pelo cliente para este *software*;
- verificar, de entre um leque de seis fornecedores, quais os requisitos que cada *software* cobria e quais não cobria, através de pesquisa online ou de contacto direto com os fornecedores;
- apurar os preços de cada possível solução;
- participar na elaboração do relatório que iria expor a recomendação final ao cliente.

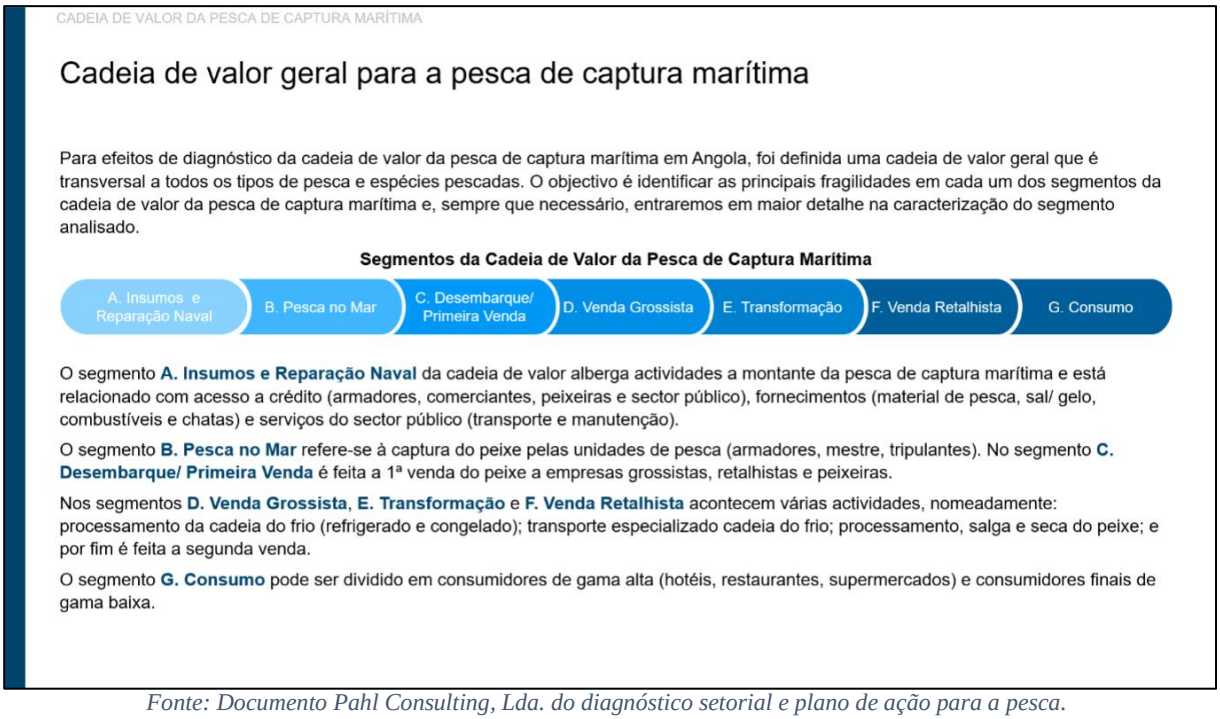
No final do primeiro mês, um dos projetos em que a Pahl Consulting, Lda. se encontrava envolvida sofreu uma atualização repentina e urgente. Por esse motivo foi criada uma *task force* com o intuito de responder às novas exigências em tempo útil. Sumariamente, o objetivo deste projeto era reduzir a dependência de Angola das importações, através de uma melhoria da sua produção interna e de uma diversificação das suas exportações. A urgência referia-se ao facto de o cliente ter antecipado o prazo de algumas entregas.

Este projeto pode dividir-se nos setores da agricultura, da pesca, dos recursos geológicos, do turismo e do têxtil, calçado e vestuário. Para cada setor era necessário elaborar e entregar dois documentos com a mesma informação, mas um seria utilizado como suporte numa exposição oral das informações, enquanto o segundo pretendia-se que fosse um relatório mais detalhado. Estes conteúdos dividem-se em três principais categorias:

- uma visão geral do setor exposta e compreendida através de indicadores macroeconómicos ou outras informações relevantes;
- uma caracterização da cadeia de valor do setor, onde era entendido o processo produtivo referente a esse setor, com o intuito de identificar as principais fragilidades na cadeia de valor desse setor;
- um plano de ação para os próximos anos, onde eram identificadas as principais oportunidades de investimento e expostas tanto as medidas propostas, bem como as recomendações para adotar essas medidas e acompanhar os seus resultados.

As apresentações do setor da pesca e do setor do têxtil, calçado e vestuário foram os documentos cujos prazos foram antecipados. As tarefas referentes a esta atividade consistiam em analisar as informações de cada setor recolhidas no local por outros colaboradores da Pahl Consulting, Lda. em conjunto com especialistas externos em cada uma das áreas e organizá-las de acordo com a estrutura e formatação pretendida. Exemplificando, quando no relatório dos especialistas era descrita a realidade do setor, com base em averiguações locais, era necessário identificar a que passo da cadeia de valor essa realidade correspondia bem como o que representava. Abordando o setor da pesca, apurou-se que este poderia ser dividido em quatro categorias: pesca de captura marítima, pesca de captura continental, aquicultura e sal. Relativamente à pesca de captura marítima, foram identificadas sete etapas na sua cadeia de valor, como está ilustrado na Figura 7. Se, por exemplo, fosse constatado que existia um grande número de peixeiras, nos centros urbanos, a vender peixe de forma informal e com baixo nível de higiene, era necessário identificar esse fator como uma fragilidade do segmento F. Venda Retalhista (Figura 7) da cadeia de valor deste setor e organizar essa informação de acordo com a estrutura pretendida. Todas as atividades desenvolvidas referentes a estes documentos, tanto para estes setores como para os restantes, seguiram sempre esta lógica e estes moldes de atuação.

Figura 7 - Cadeia de valor da pesca de captura marítima.



Fonte: Documento Pahl Consulting, Lda. do diagnóstico setorial e plano de ação para a pesca.

Logo após a conclusão destes dois documentos, a entidade adotou as práticas de teletrabalho em resposta à corrente pandemia provocada pelo coronavírus SARS-COV-2. As indicações, controlos e eventuais esclarecimentos de dúvidas passaram a ser efetuados através de reuniões online regulares. Foi então indicado que deviam ser prosseguidas, a partir de casa, as atividades referentes à elaboração dos restantes documentos necessários para esta fase do projeto em Angola. Assim, aquilo que já tinha sido feito para os setores da pesca e do têxtil, calçado e vestuário foi repetido para os restantes setores. Para além destas apresentações, foram elaborados os seus respetivos relatórios. Neste contexto, as atividades foram semelhantes às já descritas para a elaboração das apresentações. Porém, o nível de detalhe exigido era maior e por vezes não foram recolhidas informações suficientes. Nessas situações era necessário identificar a informação que estaria em falta para enviar aos especialistas e estes tentarem recolher essa informação. Para além disso, os especialistas eram responsáveis por rever os documentos e indicar, se necessário, quais as alterações ou correções que tinham de ser feitas.

Nas sete semanas seguintes, estas tarefas de leitura e análise para posterior reestruturação e organização da informação, foram as atividades desenvolvidas no âmbito do estágio curricular na Pahl Consulting, Lda. Foi então que se iniciaram, a nível definitivo,

as tarefas no âmbito do projeto de implementação de um SGSI, em conformidade com a norma ISO/IEC 27001.

4.2 Implementação de um SGSI

Ainda a partir de casa, as últimas semanas de estágio foram dedicadas a auxiliar a Pahl Consulting, Lda. no seu projeto de implementação de um SGSI. Apesar da entidade de acolhimento deste estágio ser a Pahl Consulting, Lda., a aquisição de um SGSI foi um pedido realizado por parte de um cliente. A Pahl Consulting, Lda. e outras organizações criaram um consórcio com o intuito de desenvolver a melhor solução para este cliente. Devido a um acordo de confidencialidade assinado por todas as partes, não é permitido associar as restantes entidades envolvidas neste projeto com as informações utilizadas para desenvolver este relatório. É possível, no entanto, referir que o cliente, no qual se pretende implementar um SGSI, é uma entidade pública sediada em Lisboa. A solução proposta por este consórcio pretendia cobrir diferentes domínios. Um deles é a ISO/IEC 27001, que ficou ao encargo da Pahl Consulting, Lda.

No âmbito da ISO/IEC 27001, as atividades foram divididas em quatro fases, como explicitado no quadro concetual deste relatório (Figura 5). Todavia, este é um processo demorado, pelo que no período abrangido por este estágio apenas foram desenvolvidas atividades correspondentes à terceira fase do processo, que diz respeito à implementação dos controlos de segurança. As primeiras fases já tinham sido executadas. Por esse motivo, em seguida, serão abordadas de forma distinta as atividades já realizadas, as que estão a decorrer e as que se preveem que sejam executadas no futuro. O objetivo é enquadrar as tarefas desenvolvidas durante este estágio com uma visão retrospetiva do que já tinha sido feito e um quadro prospetivo do que será feito no futuro.

4.2.1 Quadro retrospetivo

No início deste projeto teve de se ter em conta mais considerações do que as explicadas no capítulo anterior. Isso acontece devido ao facto de existirem vários domínios que eram necessários cobrir para além da ISO/IEC 27001. Essa fase preparatória resumiu-se a uma preparação das infraestruturas para possibilitar a aquisição do SGSI por parte do cliente.

No que diz respeito à conformidade com a norma ISO/IEC 27001, o primeiro passo foi realizar uma avaliação da situação inicial da organização. Foi apurado e compreendido o

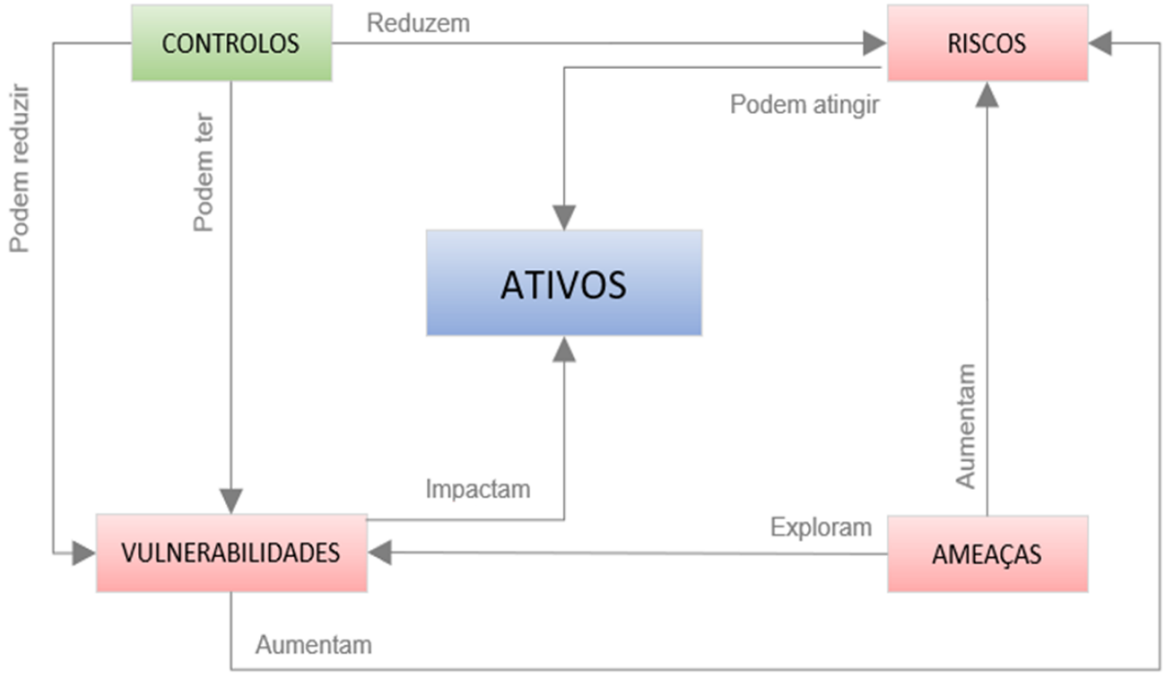
seu contexto e foram verificadas quais as normas, padrões e políticas que já se encontravam em vigor. O objetivo era estabelecer o âmbito e os limites do SGSI e, dessa forma, permitir que fosse desenvolvida uma *gap analysis* entre as condições existentes na organização e as necessárias para atingir os objetivos pretendidos em vários domínios, incluindo a ISO/IEC 27001. Nesta fase foi, ainda, definido o modelo de gestão do risco.

O modelo de gestão do risco adotado segue as recomendações das normas da família ISO/IEC 27000. Assim, este modelo pretende:

- definir quais os órgãos e indivíduos envolvidos no processo e quais as suas responsabilidades;
- identificar as componentes da segurança da informação e compreender como é que estas se relacionam entre si (ilustrado na Figura 8);
- definir a estratégia e a metodologia de gestão dos riscos.

As componentes de segurança da informação são: os ativos, os controlos, as ameaças, as vulnerabilidades e os riscos. Os ativos representam tudo o que tem valor e que requer proteção. Os controlos pretendem mitigar os riscos e reduzir as vulnerabilidades. As ameaças são as causas potenciais de um incidente de segurança da informação. As vulnerabilidades são as fraquezas de um ativo ou controlo, que podem ser exploradas pelas ameaças. Por fim, os riscos são os efeitos de incerteza nos objetivos causados pela exploração de uma vulnerabilidade num ativo por parte de uma ameaça.

Figura 8 - Relacionamento entre as componentes do SGSI.



Fonte: Documento Pahl Consulting, Lda. com o Modelo de Gestão do Risco.

A metodologia de gestão do risco desenvolvida segue o processo proposto pela ISO/IEC 27005, que se encontra esquematizado na Figura 6. Começa por exigir uma inventariação de todos os ativos, uma identificação de todos os controlos já existentes e de todas as ameaças e vulnerabilidades. Em seguida, pretende classificar o impacto de cada ameaça na confidencialidade, na integridade e na disponibilidade de cada ativo através de uma escala de 1 a 5, em que 1 representa um impacto muito baixo e 5 refere-se a um impacto muito alto. O impacto na confidencialidade é medido através da percentagem de clientes afetados, o impacto na integridade através das perdas e o impacto na disponibilidade através do tempo de indisponibilidade. Para avaliar e classificar as vulnerabilidades, esta proposta adotou o modelo *Common Vulnerability Scoring System Calculator* 3.0 (CVSS 3.0) desenvolvido pelo *National Institute of Standards and Technology* (NIST). Resumidamente, este modelo fornece um extenso número de métricas que procura classificar a capacidade de exploração e o impacto da vulnerabilidade, dando ainda a opção de considerar fatores temporais e ambientais. Com estas métricas é possível calcular a gravidade da vulnerabilidade numa escala de 0 a 10, sendo 0 gravidade nula e 10 gravidade crítica. Para além disso, também é classificada a probabilidade dessa vulnerabilidade ocorrer, assumindo esta variável o valor 1 quando ocorre muito raramente e o valor 5 quando ocorre muito

frequentemente (por exemplo uma vez em vinte anos ou uma vez por mês, respetivamente). Por fim, a partir destas classificações será calculado o risco através de uma fórmula predefinida, como é exemplificado na Tabela 2. Assim, se o valor de um risco for menor do que um determinado valor, este será aceite automaticamente, mas se for maior ou igual então terá de ser tomada uma decisão sobre se ele será reduzido, retido, evitado ou partilhado, conforme é descrito no capítulo anterior.

Tabela 2 - Exemplos do modelo de gestão do risco

Ativo	Ameaça	Vulnerabilidade	Impacto			Probab.	Vulnerab. CVSS 0.3	Risco
			Conf.	Int.	Disp.			
Aplicação Informática	Vírus	Antivírus desatualizado	5	5	5	2	3	6
Computador Portátil	Roubo	Portabilidade	3	1	1	3	6	3

Fonte: Adaptado do documento Pahl Consulting, Lda. com o Modelo de Gestão do Risco.

Contudo, na fase inicial de contextualização, foi definido que o âmbito do SGSI iria abranger toda a organização. Para além disso, foi constatada uma grande discrepância entre os controlos existentes na organização e os exigidos pela ISO/IEC 27001. Por estes motivos, a direção decidiu que iriam ser implementados todos os controlos de segurança de informação propostos no Anexo A da ISO/IEC 27001, sem realizar a etapa de análise dos riscos. Assim avançou-se para a implementação de todos os 114 controlos (e outros controlos extra em conformidade com diferentes domínios), mesmo sabendo que essa decisão poderia causar uma reação negativa na performance futura da organização.

4.2.2 Quadro atual

A fase em que este projeto se encontra é a de implementação dos controlos de segurança da informação. O início desta fase coincidiu com o momento de primeiro contacto com este projeto, no âmbito deste estágio curricular. O primeiro pedido foi para verificar se estava planeada a elaboração de todos os documentos obrigatórios no âmbito da norma ISO/IEC 27001. Para uma organização implementar um SGSI em conformidade com a norma ISO/IEC 27001 e possibilitar a sua certificação, existem alguns documentos que têm de ser desenvolvidos obrigatoriamente. A primeira tarefa consistia em analisar o plano de ações do projeto e comparar com a lista de documentos obrigatórios, de forma a garantir que todos eles iriam ser desenvolvidos. Porém, já se sabia que existiam dois documentos em falta

que deviam ter sido elaborados na fase anterior, que foi passada à frente: o plano de tratamento dos riscos e o relatório de avaliação dos riscos.

Outro documento obrigatório é a declaração de aplicabilidade. A criação desta declaração foi a tarefa seguinte. No capítulo anterior explicou-se resumidamente que este documento consiste numa lista de todos os controlos de segurança da informação. Os principais objetivos deste documento são: i) identificar quais os controlos que são aplicáveis ao SGSI em desenvolvimento (neste caso todos), ii) fornecer uma justificação para a aplicabilidade de cada controlo, iii) definir o método de implementação de cada controlo e iv) compreender o seu estado de implementação. Na Tabela 3 é ilustrado um exemplo referente aos controlos da secção A.6 Organização da segurança da informação. Esta secção tem dois objetivos de controlo, sendo que o primeiro possui cinco controlos e o segundo possui apenas dois. Para cada controlo é definida e justificada a sua aplicabilidade e também exposto o seu estado e método de implementação, este último através de um redireccionamento para os documentos específicos de cada controlo. Devido ao facto da norma ISO/IEC 27001 não estar publicamente acessível, os dados apresentados na Tabela 3 representam apenas uma exemplificação do que é pretendido e do que foi feito.

Tabela 3 - Exemplo de parte de uma Declaração de Aplicabilidade

Controlo	Descrição do Controlo	Aplicabilidade (Sim/Não)	Justificação	Método de implementação	Estado
A6	**ORGANIZAÇÃO DA SEGURANÇA DE INFORMAÇÃO**				
A6.1	1º objetivo de controlo -				
A6.1.1	Controlo 3	SIM	Não está atualizado	Conforme descrito no documento: 'SGSI_A6.1.1'	Não implementado
A6.1.2	Controlo 4	SIM	Não está atualizado	Conforme descrito no documento: 'SGSI_A6.1.2'	Parcialmente implementado
A6.1.3	Controlo 5	NÃO	Não está incluído no âmbito do SGSI	-	Não Implementado
A6.1.4	Controlo 6	SIM	Não existe	Conforme descrito no documento: 'SGSI_A6.1.4'	Parcialmente implementado
A6.1.5	Controlo 7	SIM	Obrigações legais	-	Implementado
A6.2	2º objetivo de controlo				
A6.2.1	Controlo 8	SIM	Não existe	Conforme descrito no documento: 'SGSI_A6.2'	Não implementado
A6.2.2	Controlo 9	SIM	Não existe	Conforme descrito no documento: 'SGSI_A6.2'	Não implementado

Fonte: Elaboração própria.

Após a elaboração deste documento, as tarefas deste estágio, relacionadas com este projeto, sofreram uma pausa de sete semanas antes de serem retomadas definitivamente. As atividades desenvolvidas durante este período já foram expostas no subcapítulo 4.1 Atividades desenvolvidas durante o estágio. No regresso ao projeto de implementação de um SGSI, as atividades desenvolvidas foram as de criação de manuais de políticas e procedimentos que deverão ser aprovados ou retificados pelo cliente. Para a implementação dos controlos de segurança ficou definido que para cada controlo, objetivo de controlo e secção deveria ser elaborado uma política, um processo ou um procedimento. A ISO/IEC 27000 define política como "as intenções e direção de uma organização, formalmente aceite pela gestão de topo". Um processo é "um conjunto de atividades inter-relacionadas ou em interação que transforma *inputs* em *outputs*" (ISO/IEC 27000:2018). Já um procedimento define-se como um método específico de executar uma atividade ou processo. Desta forma, serão elaborados documentos para cada controlo de segurança.

Durante este período final de estágio foram elaborados onze procedimentos e seis políticas. Estes documentos podem ser elaborados com o intuito de responder a um controlo, objetivo de controlo ou secção. Um documento pode responder a mais do que um controlo e um controlo pode exigir mais do que um documento. Contudo, neste caso não se verificou nenhuma destas situações. O âmbito de cada procedimento e política está exposto na Tabela 4, juntamente com uma breve descrição do intuito de cada documento.

Os primeiros cinco procedimentos serviram para responder aos cinco controlos de segurança da informação que dizem respeito ao primeiro objetivo de controlo da secção A6 Organização da segurança da informação. O intuito destes procedimentos é definir um modelo de gestão para garantir a implementação e controlo da segurança da informação dentro da organização. Nesse sentido, foram averiguadas as práticas mais comuns de como definir as responsabilidades referentes à segurança da informação, de como garantir a segurança da informação na gestão de projetos e de como e a quem deve ser feita a comunicação dos incidentes de segurança da informação. Para auxiliar a criação destes documentos foram seguidas as diretrizes propostas na norma ISO/IEC 27002. Esta explica qual o intuito de cada controlo e ajuda a definir quais os tópicos que cada controlo deve abranger, de forma a garantir a segurança da informação e a conformidade com a norma ISO/IEC 27001. Por exemplo, para definir um procedimento adequado para contactar com as autoridades competentes em caso de ocorrer um incidente de segurança da informação, a ISO/IEC 27002 propõe que sejam identificadas as autoridades que devem ser contactadas e

seja definida a forma de contactá-las. Nesse sentido, na elaboração do documento que visa responder a este controlo, foi desenvolvida uma pesquisa sobre as práticas mais comuns neste âmbito. Assim, foram identificadas algumas autoridades relevantes, por exemplo: o fornecedor de eletricidade e de abastecimento de água, os fornecedores de serviços de internet e telecomunicações e as agências locais de autoridades como postos de polícia e o corpo de bombeiros. Foram também estabelecidas quais as informações necessárias manter sobre estas autoridades, como o nome da autoridade, a pessoa de contacto na autoridade, o endereço, os números de telefone, entre outros. E, por fim, foi definido que dentro da organização a adotar este procedimento haverá uma pessoa em cada local a quem os funcionários deverão reportar caso detetem algum incidente de segurança da informação. Por sua vez, esta pessoa será responsável por contactar com as autoridades competentes e adequadas e auxiliá-las a lidar com a situação. Este documento, tal como todos os outros, terá de ser apresentado ao cliente para que este aprove, rejeite ou altere parcialmente estes procedimentos.

Tabela 4 - Âmbito dos documentos desenvolvidos.

Âmbito do documento	Descrição do documento	Procedimentos	Políticas
A.6.1.1	Definir e distribuir responsabilidades de segurança da informação	✓	-
A.6.1.2	Segregar responsabilidades conflituantes	✓	-
A.6.1.3	Procedimento para contactar com as autoridades	✓	-
A.6.1.4	Procedimento para contactar com grupos de interesse especial	✓	-
A.6.1.5	Garantir segurança de informação na gestão de projetos	✓	-
A.7.1	Assegurar segurança da informação antes da relação contratual	-	✓
A.7.1.1	Confirmar informações fornecidas pelos candidatos	✓	-
A.7.1.2	Procedimento de rastreio de segurança para os funcionários	✓	-
A.7.2.1	Definir as responsabilidades da gestão	✓	-
A.7.3	Assegurar segurança da informação após a relação contratual	-	✓
A.7.3.1	Definir as responsabilidades na cessão ou alteração de contrato	✓	-
A.11.2.6	Medidas de segurança para ativos fora das instalações	✓	-
A.11.2.8	Medidas de segurança para ativos sem vigilância	✓	-
A.11.2.9	Medidas de segurança para o local e equipamentos de trabalho	-	✓
A.12	Política de segurança de operações	-	✓
A.14	Política de aquisição, desenvolvimento e manutenção de sistemas	-	✓
A.16	Política de gestão de incidentes de segurança da informação	-	✓
	Total	11	6

Fonte: Elaboração própria.

Em relação à secção de controlos A.7 Segurança na gestão de recursos humanos, foram criados quatro procedimentos e duas políticas. Estes procedimentos pretendiam responder a dois controlos do primeiro objetivo de controlo, a um controlo do segundo e a

outro controlo do terceiro objetivo de controlo. O objetivo destes procedimentos é definir o modo como deve ser tratada a informação dos colaboradores (incluindo provedores de serviços, funcionários temporários ou informais, candidatos a vagas de emprego e membros da direção) e, também, como é que a organização deve tratar a informação dos seus colaboradores, antes, durante e após a relação contratual entre os dois. Já as duas políticas desenvolvidas pretendiam dar resposta direta ao primeiro e ao último objetivos de controlo desta secção. São duas políticas de segurança e privacidade de dados que procuram estabelecer as normas pelas quais a organização se deve reger no momento de adquirir, processar ou armazenar informação sobre os seus colaboradores em dois momentos distintos: antes de ser estabelecida uma relação contratual entre a organização e um potencial colaborador e quando a relação contratual com um colaborador terminar ou se alterar. Devido ao carácter destes documentos, é pertinente notar que estes terão de ser disponibilizados e comunicados regularmente a todos os colaboradores da organização, pelo que podem, inclusive, vir a estar publicamente disponíveis. A criação destes procedimentos seguiu também as diretrizes fornecidas pela norma ISO/IEC 27002. Já as políticas foram baseadas numa análise das práticas mais comuns noutras instituições certificadas. Por exemplo, nestas políticas foi definido:

- que informações devem ser recolhidas e armazenadas, como a informação de identificação, de contacto, de experiência profissional e educacional, situação familiar, entre outras;
- como é que as informações devem ser recolhidas, processadas, utilizadas e armazenadas, estabelecendo-se que a informação será recolhida, maioritariamente, através do próprio colaborador ou candidato e que será utilizada para responder às necessidades operacionais e obrigações legais da organização;
- quem tem acesso à informação, nomeadamente, a administração da organização, o departamento dos recursos humanos e próprio dono das informações;
- que responsabilidades tem a organização ao utilizar essas informações, como de implementar medidas de segurança físicas e eletrónicas e de cumprir a legislação aplicável;

- que responsabilidades têm os colaboradores ao acederem a estas informações, como por exemplo assinar acordos de confidencialidade e cumprir as políticas de segurança estabelecidas.

A criação destes manuais não segue a ordem pela qual os controlos surgem nas normas ISO/IEC 27001 e ISO/IEC 27002. Por esse motivo, alguns controlos foram deixados para serem desenvolvidos mais à frente. Assim, os manuais seguintes dizem respeito à secção A.11 Segurança física e ambiental. Para esta secção foram desenvolvidos dois procedimentos e uma política. Estes documentos procuram definir a aplicação de três dos nove controlos do segundo objetivo de controlo desta secção. Através das orientações fornecidas pela norma ISO/IEC 27002 redigiram-se os manuais com o intuito de definir a forma como os colaboradores devem agir para garantir a segurança dos equipamentos da organização e prevenir a perda, dano, furto ou comprometimento de ativos. Foi estabelecido, por exemplo, que: o equipamento fora das instalações deve ser protegido contra acesso indevido (através de uma senha, chave ou cartão de identificação) e ser mantido sempre sob vigilância; quando o equipamento vai ser deixado sem vigilância deve ser bloqueado e, se possível, guardado num compartimento de segurança (como uma gaveta, cacifo, cofre ou armário); e todos os dispositivos com informação sensível (incluindo cadernos, folhas, CDs, unidades USB, entre outros) nunca devem ser deixados em cima da secretária ou noutros locais de fácil acesso e, quando não estão a ser utilizados, devem ser guardados num compartimento de segurança. Os manuais que estipulam estas normas deverão, também, ser partilhados com os colaboradores que utilizam os equipamentos abrangidos por estes procedimentos e políticas.

Por fim, definiram-se três políticas gerais com base nas práticas mais comuns. A primeira, para a secção A.12 Segurança de operações, com o intuito de definir as normas adotadas para proteger, gerir e controlar a segurança das informações durante as operações da organização. Para a secção A.14 Aquisição, desenvolvimento e manutenção de sistemas, com o propósito de estabelecer quais os padrões e requisitos que devem ser exigidos a cada sistema da organização nos momentos de seleção, estabelecimento e controlo do mesmo. Finalmente, uma política para a gestão de incidentes de segurança, secção A.16. O objetivo era definir as normas pelas quais a organização se deve guiar em situações de incidentes de segurança da informação, desde o momento da deteção do incidente até à comunicação e análise pós incidente.

Este último documento foi terminado no último dia de estágio trazendo com ele, não só a conclusão de mais uma política, mas também o fim desta primeira experiência no mercado de trabalho na área de gestão.

4.2.3 Quadro prospetivo

Apesar do estágio curricular ter chegado ao fim, este projeto não terminou. O SGSI ainda não foi implementado, pelo que as atividades irão continuar.

Primeiramente irão continuar a ser produzidos os documentos que definem as políticas, processos e procedimentos a ser adotados pela organização. Em paralelo, à medida que os manuais desenvolvidos vão sendo aprovados, começarão a ser implementados os controlos de segurança. Isto significa que a organização começará a adotar e implementar os métodos e normas propostos nos manuais. Este será um processo demorado visto que existem 114 controlos, 35 objetivos de controlo e 14 secções, só no domínio da norma ISO/IEC 27001. Ficou decidido que para cada controlo, objetivo de controlo e secção deveria ser criado um documento diferente, que muitas vezes terá de sofrer diversas alterações antes de ser aprovado.

Quando todas as políticas, processos e procedimentos forem aprovados poderá então iniciar-se a última fase. Aqui terão de ser definidos indicadores de acompanhamento do SGSI para seguir a conformidade e a performance do mesmo. Para além disso será necessário desenvolver um plano para manter o SGSI. Todos os anos este terá de ser revisto, reavaliado e, se necessário, atualizado. O contexto, tanto da organização como da segurança da informação, não é estático, pelo que é necessário averiguar regularmente se o sistema estabelecido continua a cumprir os requisitos necessários e se os controlos são suficientes para alcançar os objetivos da organização. Assim, este SGSI poderá finalmente ser submetido a certificação e a organização poderá constatar que protege as suas informações de acordo com os padrões mais reconhecidos a nível internacional, transmitindo confiança, credibilidade e preocupação, não só para os seus clientes como para todos os seus colaboradores.

5. Análise Crítica

Nas últimas décadas, houve uma enorme evolução das tecnologias, incluindo as tecnologias de informação (TI). Assim, garantir a qualidade do processamento e da segurança da informação tem-se tornado um fator crítico para a atuação das empresas no geral, mas com uma acrescida influência nas empresas de consultoria. Desta forma, realizar um estágio curricular numa consultora com a possibilidade de atuar simultaneamente na área de gestão e de TI representa, certamente, uma mais valia, tanto a nível profissional como pessoal, para encarar um futuro que se perspetiva com grande evolução e incerteza a nível tecnológico.

Relativamente à entidade de acolhimento deste estágio, a Pahl Consulting, Lda., a apreciação global é muito positiva. Desde o princípio que a entidade e a sua direção se mostraram completamente disponíveis e empenhados em garantir que os seus colaboradores, estagiários incluídos, se sintam bem e confortáveis no seu local de trabalho. Os padrões adotados dão liberdade suficiente para que os colaboradores da Pahl Consulting, Lda. consigam gerir as suas atividades de acordo com as exigências e necessidades específicas de cada um. Para além disso, é notório que o trabalho desenvolvido por cada um é justamente apreciado e valorizado. Desta forma, é possível sentir o enorme ambiente de confiança vivido por todos os membros da organização. O facto de a Pahl Consulting, Lda. ser representada por uma equipa não muito extensa (apenas 25 colaboradores) e relativamente jovem ajuda a promover um ambiente positivo e deveras solidário para um recém-chegado ao mercado de trabalho. Contudo, o facto de se tratar de uma equipa jovem não é sinónimo de inexperiente. Diversos membros apresentam uma experiência extraordinariamente diversificada e relevante, o que faz com que trabalhar com essas pessoas seja não só um teste desafiante, como uma experiência incrivelmente enriquecedora. Porém, as posições e ideias dos trabalhadores com menos experiência não eram discriminadas por isso, havendo sempre disposição e possibilidade para fomentar o espírito crítico de cada um.

Com certeza que o espírito de equipa é um ponto forte da Pahl Consulting, Lda. Contudo, devido à pandemia que se vive atualmente, todos os trabalhos têm sido realizados a partir de casa, o que não promove o desenvolvimento deste espírito coletivo e de entreajuda. Essa tem sido uma das principais preocupações durante todo o período de teletrabalho. Não só manter os níveis de produção, mas também manter uma equipa unida. Nesse sentido, a comunicação da direção para com os trabalhadores surgiu sempre de forma

atempada e pertinente. Todo o processo de lidar com esta nova realidade foi positivo, a entidade adotou medidas de segurança e novos métodos de trabalho, ainda antes de ser declarado o estado de emergência e confinamento obrigatório pelo estado português, fazendo com que todos se sentissem seguros e que não iam estar sujeitos a riscos desnecessários. Para além disso, todas as decisões envolvendo esta situação surgiram sempre no momento em que eram necessárias.

Por estes motivos, a apreciação global da Pahl Consulting, Lda. é francamente positiva. O único ponto de melhoria sugerido seria na comunicação e acompanhamento. Algumas vezes, não sempre, era pedido para se executarem tarefas e não era feito um enquadramento sobre o propósito dessa tarefa ou eram tomadas decisões e não eram explicados os motivos. Isto pode provocar o desenvolvimento de sensações de incerteza quanto às atividades que estão a ser realizadas. Porém, sempre que eram questionados estes objetivos ou motivos, toda a gente mostrou sempre grande disponibilidade e preocupação em explicar os conceitos subjacentes, pelo que era notório que estas situações aconteciam apenas por falta de atenção, causada, muitas vezes, pelas grandes exigências que alguns projetos impunham sobre a entidade e os seus trabalhadores. Desta forma, a proposta de melhoria seria em procurar desenvolver uma comunicação mais completa. A comunicação dentro da entidade é feita de forma aberta entre todos, o que, certamente, representa um ponto positivo. Fazer com que esta comunicação fosse ainda mais completa, possivelmente poderia transformar este ponto positivo num ponto ainda mais positivo.

Em relação às atividades realizadas neste estágio, como em todo o lado, houve algumas atividades mais interessantes que outras. Estas podem dividir-se em três categorias: atividades de análise, atividades de criação e atividades sistemáticas. Porém, é pertinente referir que esta classificação e avaliação deriva, meramente, de uma perspetiva individual. Certamente, esta opinião varia consoante os gostos e perfil de cada indivíduo.

As primeiras, atividades de análise, exigem maiores capacidades de interpretação e de raciocínio. Para executar corretamente estas atividades, muitas vezes é necessário efetuar grandes quantidades de estudo e pesquisa. Estas representam as atividades mais trabalhosas e exigentes, porém permitem a construção e o amadurecimento de capacidade fundamentais de trabalho, para além de que representam um grande desafio intelectual e enriquecimento pessoal. Estas atividades podem revelar-se extremamente interessantes e permitem um grande desenvolvimento do conhecimento nas mais diversas áreas, por parte dos seus executantes.

As atividades de criação exigem outro tipo de capacidades. Ser capaz de organizar e estruturar as informações previamente analisadas, representa, também, uma parte importante do trabalho realizado em diversas áreas, inclusive em consultoria de gestão. Ao contrário dos outros dois tipos de atividade (de análise e sistemático), este, regularmente, é realizado em conjunto, com o intuito de aproveitar as melhores ideias de cada membro do grupo. Tal como as atividades de análise, exige espírito crítico, mas para um âmbito mais criativo do que apreciativo. Representa, por isso, um trabalho mais estimulante.

Quanto às atividades sistemáticas, dizem respeito a tarefas mais disciplinadas que exigem o cumprimento de critérios e regras bem definidas. Não é exigido, especificamente, o desenvolvimento de nenhuma capacidade cognitiva. Retrata um trabalho mais fácil e, normalmente, mais leve. No entanto, pode tornar-se entediante e superficial, criando um ambiente propício à redução do comprometimento e do envolvimento dos indivíduos com a organização.

Estas atividades estiveram sempre interligadas ao longo do estágio. Todos os projetos integrados exigiram a execução de todos os tipos de atividades. Assim, participar na execução de um projeto torna-se um trabalho mais diversificado e leve. Realizar sempre o mesmo tipo de atividades poderia tornar-se um fator de desmotivação. Para além disso, fornece uma experiência holística a todos os colaboradores, o que, consequentemente, contribui para um desenvolvimento pessoal mais completo por parte de todos.

Deste modo, a diferenciação de cada projeto ocorrerá, principalmente, de acordo com a área e o âmbito das atividades exigidas. Abordando os dois principais projetos integrados durante o período de estágio, pode-se afirmar que enquanto alguns colaboradores poderão ter mais experiência e gosto por pesquisar e trabalhar em áreas mais tecnológicas, investigando e estabelecendo as dinâmicas para a implementação de um sistema de gestão de segurança da informação, outros podem apresentar preferências por atuar num ambiente mais direcionado às áreas de estratégia ou economia, procurando diagnosticar e propor medidas para melhorar a atividade em setores importantes da economia.

Através deste estágio foi possível formar e fortalecer um variado conjunto de capacidades que através de aulas teóricas ou práticas muitas vezes se torna complicado. Para além de angariar um diversificado leque de conhecimentos em diversas áreas, foi possível, e necessário, exercitar capacidades pessoais e sociais em contextos diferentes dos presenciados anteriormente. Quando foi tomada a decisão de concluir o mestrado em gestão

através de um estágio curricular, as expetativas eram de que desta forma seria possível estabelecer uma ligação com o meio profissional, para que as competências adquiridas ao longo do restante percurso académico pudessem, finalmente, ser colocadas em prática e totalmente compreendidas. Da mesma forma, esperava-se que as competências pessoais pudessem, por sua vez, ser realmente testadas e aprimoradas num ambiente propício. Chegando ao final do estágio, é possível afirmar que as expetativas não foram apenas correspondidas, como foram superadas. Os conhecimentos adquiridos em disciplinas, tanto na área da informação, como na área de estratégia, mostraram-se, verdadeiramente, relevantes para possibilitar uma consolidação mais rápida e eficaz dos temas abordados ao longo deste estágio curricular. Para além disso, a comunicação, o pensamento crítico, a atitude e a persistência foram competências comportamentais muito requisitadas e, por esse motivo, muito desenvolvidas durante este período.

Contudo, a elaboração deste relatório tornou-se mais complicada por motivos impossíveis de controlar. Primeiramente, a pandemia COVID-19 dificultou a realização de diversas atividades práticas e de contacto com colaboradores dos diversos projetos e, em alguns casos, impediu totalmente. Adicionalmente, os acordos de confidencialidade e os direitos autorais dos materiais envolvidos no projeto base deste relatório, por diversas vezes dificultaram ou impossibilitaram que a exposição dos conceitos e das experiências subjacentes às atividades desenvolvidas fossem expostos de forma totalmente clara.

No entanto, a apreciação global deste estágio curricular é muito positiva. Trabalhar em consultoria pode ser muito exigente, porém demonstrou ser uma atividade extremamente enriquecedora (tanto a nível cognitivo, como a nível social), e que, numa perspetiva pessoal de quem estagiou na Pahl Consulting, Lda., atuando nesta área, sem dúvida que acaba por recompensar todo o esforço investido.

6. Conclusões e considerações finais

A segurança da informação é uma preocupação em crescendo no mundo empresarial. Atualmente vive-se uma revolução industrial que pode ser sentida diariamente. Novas tecnologias surgem a cada instante, incluindo tecnologias de informação. Não é de estranhar, portanto, a importância crescente atribuída à criação e proteção de sistemas de gestão da informação. Numa era dominada pelo setor dos serviços, oferecer um serviço personalizado e diferenciado é um fator de extrema relevância e decisivo para a garantir a satisfação dos clientes e o sucesso de uma empresa. Contudo, tal só é possível se houver um bom processo de recolha e tratamento das informações fornecidas pelos clientes ou potenciais clientes. Em quase todas as páginas da internet é pedido para o utilizador se registar e aceitar a política de *cookies*. Estes dois pedidos visam adquirir e processar informação dos visitantes dessa página. Por esse motivo é que a segurança da informação acumula cada vez mais preocupação por parte dos utilizadores e clientes e, consequentemente, das entidades responsáveis pela informação. A informação é um ativo que se valoriza de dia para dia. Desta forma, é natural que haja um crescente investimento em gerir a informação e em protegê-la contra furtos ou modificação e acesso ilícito.

Devido ao ritmo acelerado a que a tecnologia evolui, é de esperar que a procura por sistemas de gestão de segurança da informação realmente eficazes continue a aumentar à semelhança ou até a um ritmo maior do que o que tem acontecido nos últimos anos. O número de organizações certificadas com a ISO/IEC 27001 anualmente tem crescido 20% todos os anos e, de acordo com Santos et al. (2017), este é o segundo *standard* que as organizações portuguesas mais desejam implementar, a seguir à ISO 45001 para um sistema de gestão da segurança e saúde ocupacional. Assim, é possível deduzir que a relevância desta norma ainda irá crescer nos próximos anos. As empresas querem manter as suas informações seguras de acordo com os padrões mais reconhecidos internacionalmente. Não só pela posição reputacional, mas também para proteger um ativo extremamente importante e prevenir perdas de capital resultantes de incidentes de segurança. Assim, é de esperar que as normas que visam garantir a segurança da informação, como a ISO/IEC 27001, sejam cada vez mais requisitadas e exigidas e, eventualmente, tornando-se obrigatórias.

Outra questão relevante diz respeito aos dados pessoais e à privacidade, questões que muitas vezes deixam as pessoas preocupadas. O facto de não se saber o modo e o propósito da aquisição e tratamento das informações pessoais não é pacificamente aceite pela

população. Dessa forma, existir uma norma que garanta que estas e outras informações são tratadas em conformidade com as melhores práticas a nível internacional e de forma segura, certamente influenciará positivamente o processo de aceitação dos indivíduos mais desconfiados.

Posto isto, a certificação em conformidade com a norma ISO/IEC 27001 seguramente representa uma mais valia para quem a adquire. Porém, futuramente, deixará de representar uma vantagem, mas sim uma desvantagem para quem não a obtiver. Possivelmente, os padrões propostos pela norma poderão adquirir um carácter obrigatório e legislativo, como já acontece com o Regulamento Geral de Proteção de Dados (RGPD). O RGPD é um regulamento europeu sobre a privacidade e proteção de dados pessoais. Talvez, no futuro, o âmbito deste regulamento possa ser alargado para abranger novos domínios.

Desta forma, um relatório de estágio que tem como objetivo estudar a implementação de um SGSI em conformidade com uma norma reconhecida internacionalmente, a ISO/IEC 27001, pode revelar-se interessante e, até, importante para expor e ajudar a compreender as atividades subjacentes a este processo.

As normas da família ISO/IEC 27000 oferecem os *standards* para estabelecer, implementar, manter e melhorar um conjunto de políticas, procedimentos e atividades, que devem ser geridos coletivamente com o intuito de garantir a confidencialidade, integridade e disponibilidade das informações das organizações. As diretrizes fornecidas, especialmente pelas normas ISO/IEC 27002 e ISO/IEC 27005, dão um auxílio crucial para o estabelecimento e implementação de um SGSI em conformidade com os requisitos da norma ISO/IEC 27001. Com a informação desta família de normas pretende-se planear o SGSI com base no contexto da organização, planear o sistema de gestão do risco, avaliar e tratar os riscos para selecionar os controlos que se irão implementar e, ainda, definir um plano para monitorar e melhorar continuamente o SGSI.

Durante o estágio na Pahl Consulting, Lda. foi possível compreender os alicerces da implementação de um SGSI e participar na elaboração das políticas e procedimentos que irão permitir a segurança das informações abrangidas por este sistema. Sabe-se que existem práticas importantes que devem ser consideradas de forma a que os resultados da adoção do SGSI tenham uma maior probabilidade de se tornarem mais positivos. Porém, a entidade que se encontra no processo de adoção deste SGSI nem sempre optou pelas práticas mais aconselhadas, pelo que, no futuro, será interessante acompanhar os resultados obtidos com

a implementação deste SGSI e averiguar se os objetivos pretendidos serão ou não atingidos, mesmo que apenas parcialmente.

Referências Bibliográficas

Barafort, B., Mesquida, A., & Mas, A. (2016). Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives. *Computer Standards & Interfaces*. https://doi.org/10.1016/j.csi.2016.11.010

Benner, M. J., & Veloso, F. M. (2010). ISO 9000 practices and financial performance : A technology coherence perspective. *Journal of Operations Management*, *26*(2008), 611–629. https://doi.org/10.1016/j.jom.2007.10.005

Brunner, M., Sauerwein, C., Felderer, M., Breu, R., Brunner, M., Sauerwein, C., … Breu, R. (2020). Risk Management Practices in Information Security Exploring the Status Quo in the DACH Region. *Computers & Security*, 101776. https://doi.org/10.1016/j.cose.2020.101776

Casaca, J. A., & Correia, M. F. (2010). Porque é necessária a segurança da informação? Da estratégia às políticas de segurança. *Lusiada*, *3*(Política Internacional e Segurança), 88–110.

Correia, C. (2016). *Norma ISO / IEC 27001 no INEM Plano de Implementação da*. NOVA IMS.

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, 5–7. https://doi.org/10.1016/S1361-3723(11)70005-7

Farn, K., Lin, S., & Fung, A. R. (2004). A study on information security management system evaluation — assets, threat and vulnerability. *Computer Standards & Interfaces*, *26*, 501–513. https://doi.org/10.1016/j.csi.2004.03.012

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4842–4848. https://doi.org/10.1109/HICSS.2016.600

Hudson, J., & Orviska, M. (2013). Firms' adoption of international standards: One size fits all? *Journal of Policy Modeling*, *35*(2), 289–306. https://doi.org/10.1016/j.jpolmod.2012.04.001

Ifinedo, P. (2011). Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and Vocabulary. (n.d.).

ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management. (n.d.).

Jouini, M., Ben, L., Rabai, A., & Ben, A. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Koskosas, I. V, & Paul, R. J. (2004). *Information Security Management in the Context of Goal-setting*. *6*(1), 19–29.

Martins, A. B., & Santos, C. A. (2005). Uma metodologia para implantação de um sistema de gestão de segurança da informação. *Journal of Information Systems and Technology Management*, *2*, 121–136.

Merhi, M. I., & Ahluwalia, P. (2018). Examining the Impact of Deterrence Factors and Norms on Resistence to Information System Security. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2018.10.031

Norma Portuguesa ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão de segurança da informação - Requisitos. (n.d.).

Santos, G., Rebelo, M. F., Silva, R., Santos, G., Rebelo, M. F., & Silva, R. (2017). Integrated Management Systems: Trends for Portugal in the 2025 horizon. *Procedia Manufacturing*, *13*, 1191–1198. https://doi.org/10.1016/j.promfg.2017.09.194

Su, H., Dhanorkar, S., & Linderman, K. (2015). A competitive Advantage from the Implementation Timing of ISO Management Standards. *Journal of Operations Management*. https://doi.org/10.1016/j.jom.2015.03.004

Syreyshchikova, N., Pimenov, D., Mikolajczyk, T., & Moldovan, L. (2019). Information Safety Process Development Development According to ISO 27001 for an Industrial Enterprise. *Procedia Manufacturing*, *32*, 278–285. https://doi.org/10.1016/j.promfg.2019.02.215

Szczepaniuk, K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2019). Information Security Assessment in Public Administration. *Computers & Security*. https://doi.org/10.1016/j.cose.2019.101709

Wessel, R. M. Van, & Vries, H. J. De. (2013). Business Impacts of International Standards for Information Security Management . Lessons from Case Companies. *Journal of ICT Standardization*, *1*(1), 25–40. https://doi.org/10.13052/jicts2245-800X