LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

A FUNÇÃO DO CHIEF INFORMATION SECURITY OFFICER NAS ORGANIZAÇÕES

PEDRO MIGUEL CENTÚRIO SOL MONZELO

OUTUBRO - 2018

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

A FUNÇÃO DO CHIEF INFORMATION SECURITY OFFICER NAS ORGANIZAÇÕES

PEDRO MIGUEL CENTÚRIO SOL MONZELO

ORIENTAÇÃO:
PROF. DOUTOR SÉRGIO NUNES (ISEG-UL)

OUTUBRO - 2018

Resumo

Num mundo cada vez mais conectado e digital, a informação é crescentemente vista como potenciador do negócio e fonte de vantagem competitiva sustentável. Desta forma, a segurança de informação torna-se crítica de forma a proteger os ativos de informação, pelo que a preocupação com a estratégia de segurança das organizações tem vindo a alinhar-se com os seus objetivos estratégicos de negócio. Por outro lado, as recentes alterações a nível regulamentar, tais como a Diretiva Segurança das Redes e da Informação (SRI) e o Regulamento Geral de Proteção de Dados (RGPD), vêm regular e impor regras no que diz respeito à privacidade e à segurança da informação, permitindo às organizações um redesenho ou ajuste dos seus processos de forma a garantir que a informação se encontra de facto segura. Neste contexto, o *Chief Information Security Officer* (CISO) vem assumir um papel de destaque na coordenação da confidencialidade, integridade, e disponibilidade da informação na organização.

Este trabalho pretende estudar o ambiente geral da segurança de informação nas organizações, analisar o papel do CISO nas mesmas, e compreender onde este deverá estar integrado na estrutura organizacional. Para tal, foram realizadas entrevistas a consultores especialistas da área e a pessoas com cargos diretivos nas áreas de sistemas de informação e de segurança da informação, que permitiram concluir que ainda é necessário um grande amadurecimento a nível das organizações em Portugal no que diz respeito ao tema, e que tal poderá eventualmente dever-se à ausência de uma cultura de segurança estabelecida no país. Por outro lado, o papel do CISO tem assumido uma maior relevância, sendo que é uma opinião geral que o mesmo deverá ter uma relação próxima com a administração das empresas.

Palavras-Chave: CISO; Segurança da Informação; SGSI; Gestão de Informação; Gestão de Risco; Conselho de Administração; SRI; RGPD

Abstract

In an increasingly connected and digital world, information is seen as a business enabler and a source of sustained competitive advantage. Thus, information security is becoming critical so to protect these information assets, which is why the concern with organizations' security strategy has been aligning with their strategic objectives. On the other hand, recent changes in regulation, as Network and Information Security (NIS) directive and the General Data Protection Regulation (GDPR), come to regulate and create rules when it comes to information security, and allow organizations to redesign or adjust these processes in order to ensure that information is, in fact, safe. In this context, the Chief Information Security Officer (CISO) comes to play an important role in coordinating confidentiality, integrity, and availability of information in the organization.

This paper aims to study organizations' information security environment in general, analyse the CISO's role inside them, and understand where they should be integrated in the corporate structure. To do so, interviews were conducted on experienced information security consultants and information systems and information security directors, which allowed to conclude that organizations in Portugal still need a great amount of maturing when it comes to information security, and that this may eventually be due to the absence of an established security culture in the country. On the other hand, the CISO's role has been increasing in relevance, being a general opinion that their relationship with organizations' boards should be close.

Keywords: CISO; Information Security; ISMS; Information Management; Risk Management; Board of Directors; NIS; GDPR

Índice

1 – INTRODUÇÃO 1

1.1 – MOTIVAÇÃO E QUESTÕES DE INVESTIGAÇÃO 2

2 – REVISÃO DE LITERATURA 4

2.1 – VALOR DA INFORMAÇÃO 4
2.2 – GESTÃO DA SEGURANÇA DE INFORMAÇÃO 5
2.3 – FUNÇÃO DO CISO 7
2.4 – ENQUADRAMENTO LEGAL 10
2.4.1 – RGPD – Regulamento Geral de Proteção de Dados 11
2.4.2 – Diretiva SRI – Segurança das Redes e da Informação 13
2.4.3 – Cybersecurity Disclosure Act of 2017 16
2.5 – NORMATIVOS E *FRAMEWORKS* 17
2.5.1 – ISO 27001 17
2.5.2 – COBIT 19

3 – METODOLOGIA DE INVESTIGAÇÃO 24

3.1 – TIPO DE ESTUDO 24
3.2 – AMOSTRA E RECOLHA DE DADOS 24
3.3 – ANÁLISE DE DADOS 25

4 – APRESENTAÇÃO DOS RESULTADOS 27

4.1 – AMBIENTE GERAL DE SEGURANÇA DE INFORMAÇÃO 27
4.2 – PERFIL E RESPONSABILIDADES DO CISO 29
4.3 – IMPACTO DAS ALTERAÇÕES REGULAMENTARES 31
4.4 – ESTRUTURA HIERÁRQUICA E LINHAS DE REPORTE 33

5 – DISCUSSÃO DOS RESULTADOS 35

6 – CONCLUSÕES 39

6.1 – LIMITAÇÕES DO ESTUDO 40
6.2 – OPORTUNIDADES PARA PESQUISA FUTURA 40

BIBLIOGRAFIA 42

ANEXO I – QUESTÕES DAS ENTREVISTAS 48

ANEXO II – RESULTADOS ANÁLISE DAS ENTREVISTAS 49

Índice de Figuras

Figura I - Ciclo da Informação 4
Figura II – Evolução global de certificações ISO 27001 19

Índice de Tabelas

Tabela I – Tabela RACI – Processo PO9 (Avaliar e Gerir os Riscos de TI) 21
Tabela II – Tabela RACI – Processo DS5 (Garantir a Segurança dos Sistemas) 22
Tabela III – Relação entre os diferentes tipos de atividades de segurança e potenciais stakeholders 23
Tabela IV – Lista de entrevistados 25

Lista de Acrónimos

Acrónimo	*Termo*
BS	British Standard
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNPD	Comissão Nacional de Proteção de Dados
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSIRT	Computer Security Incident Response Team
DPO	Data Protection Officer
DSI	Direção de Sistemas de Informação
UE	União Europeia
EUA	Estados Unidos da América
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NACD	National Association of Corporate Directors
NIS	Network and Information Security
RGPD	Regulamento Geral de Proteção de Dados
SEC	Securities and Exchange Commission
SGSI	Sistema de Gestão de Segurança de Informação
SRI	Segurança das Redes e da Informação
TI	Tecnologia(s) de Informação

1 – Introdução

Atualmente, a informação pode ser vista como um bem essencial, à semelhança da eletricidade, sem a qual muitas organizações simplesmente não conseguem operar (Carr, 2003). No entanto, no mundo cada vez mais interligado em que vivemos, a informação encontra-se muito mais exposta e vulnerável que outros tipos de bens essenciais (Van Niekerk & Von Solms, 2010).

Cada vez mais as organizações reconhecem a informação e respetivas tecnologias como ativos críticos do negócio, que devem ser geridos de forma eficaz (Cadete, 2015). Tal como para qualquer ativo estratégico das organizações, a adequada salvaguarda da informação é essencial para que o sucesso do negócio não seja comprometido (Doughty, 2003), podendo um incidente nos sistemas de informação causar uma interrupção no negócio, comprometer a reputação da organização e, inclusivamente, ter consequências legais, causando assim impacto financeiro para a organização (Allianz, 2016).

Ao longo dos anos, a segurança de informação tem-se tornado uma grande preocupação a nível social e organizacional (Olijnyk, 2015), tendo evoluído de uma orientação maioritariamente tecnológica, para uma orientação mais estratégica das organizações. Com esta evolução, tem-se também verificado a crescente necessidade de alinhar a estratégia de segurança com a estratégia de negócio (Catarino *et al*, 2016). Ainda assim, a segurança de informação ainda é muitas vezes vista como um custo, uma vez que que um projeto de segurança por si não produz aumentos de receitas ou reduções diretas de custos (Fitzgerald, 2007).

Com o crescimento da infraestrutura tecnológica, também a informação se tem tornado mais vulnerável a um vasto conjunto de ameaças (Olijnyk, 2015) e, enquanto várias organizações acreditam que os seus sistemas de informação estão seguros, a verdade é que muitas vezes não o estão (Calder & Watkins, 2012). Segundo o relatório de violações de dados ocorridos durante o ano 2016, realizado pelo Identity Theft Resource Center, os ciber-ataques a organizações continuam a aumentar em frequência e sofisticação. De facto, no ano 2016 verificou-se um aumento de 40% em termos de ataques sucedidos face ao ano anterior (Identity Theft Resource Center, 2016), tendo sido verificado que 2 em cada 3 grandes organizações do Reino Unido foram vítimas de ataques ou falhas de ciber-segurança (Klahr *et al*, 2016).

Neste contexto, com o aumento das violações de segurança de informação, as pressões competitivas e a necessidade de garantir conformidade com as regulamentações governamentais, os conselhos de administração das organizações têm estado mais sensíveis para os riscos de segurança (Nolan & McFarlan, 2005), estando a gestão destes riscos e os maiores requisitos de controlo sobre a informação a ser compreendidos como elementos chave para a governança empresarial (IT Governance Institute, 2007).

Assim, a adoção de um sistema de gestão de segurança de informação é uma decisão estratégica para a organização, devendo a sua definição e implementação ser influenciada pelas necessidades, objetivos e estratégia da organização (International Organization for Standardization, 2013).

A delegação de um CISO (*Chief Information Security Officer*), ou de um responsável pela segurança de informação, demonstra o compromisso da organização com a existência de uma liderança dedicada a responder aos seus compromissos estratégicos (Peltier, 2013).

1.1 – Motivação e questões de investigação

Face à atual complexidade e rápida evolução dos riscos de segurança de informação, as organizações têm vindo a necessitar de alterar a sua abordagem perante este tema. As atuais alterações regulamentares, como o caso da diretiva Segurança das Redes e da Informação (SRI) e do Regulamento Geral de Proteção de Dados (RGPD), têm obrigado as organizações a repensar a sua abordagem e estratégia perante a segurança de informação. Referências de mercado como o COBIT têm vindo igualmente a alterar a sua visão do que é a função e responsabilidades do CISO e da segurança da informação dentro do contexto organizacional, considerando-os cada vez mais como um pilar estratégico nas organizações.

Cada vez mais os administradores estão sensíveis ao facto de a segurança ser um tema crítico para a integridade e continuidade do seu negócio, existindo assim uma necessidade ascendente de estarem mais próximos e alinhados com esta área. Face a este contexto e à crescente relevância que a segurança de informação tem no contexto organizacional, a função do responsável pela mesma tem também evoluído e sido transformada ao longo dos tempos.

Face a este contexto, o presente trabalho visa assim responder às seguintes questões:

Q1: Qual o atual paradigma de segurança de informação nas organizações e como as recentes alterações regulamentares têm alterado o mesmo?

Q2: Quais as competências e responsabilidades chave de um CISO?

Q3: Onde deve o CISO encontrar-se hierarquicamente posicionado dentro da estrutura organizacional?

2 – Revisão de Literatura

No presente capítulo são explorados os pilares principais para o estudo, nomeadamente ao estudar o valor da informação nas organizações, a necessidade da sua adequada gestão e proteção e, consequentemente, na função do CISO no contexto organizacional. São adicionalmente exploradas as atuais alterações regulamentares que impactam diretamente a gestão da segurança da informação organizacional, assim como as evoluções das principais referências do mercado relativamente ao tema.

2.1 – Valor da informação

No contexto organizacional, a informação é um potenciador do negócio. Segundo o ciclo da informação apresentado pelo COBIT 5, apresentado na Figura I, os processos de negócio geram e processam dados, transformam-nos em informação e conhecimento, que por fim são usados para criar valor e direcionar a organização (ISACA, 2012).

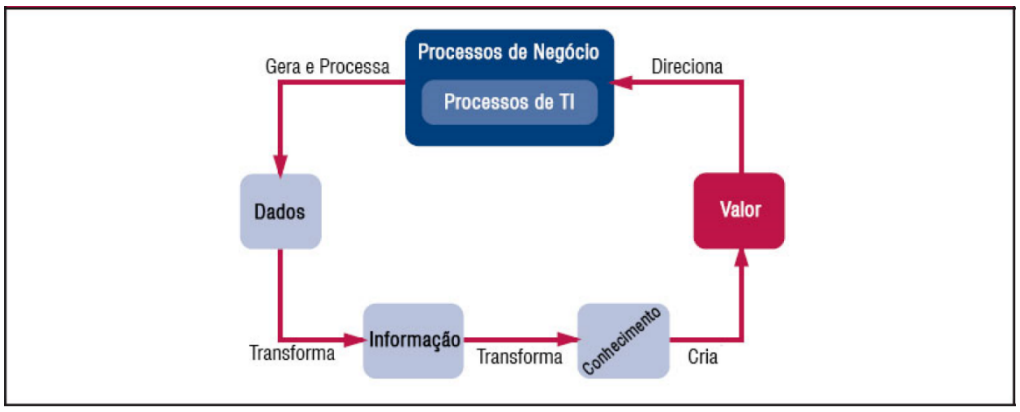

Figura I - Ciclo da Informação
Fonte: ISACA. (2012), p. 84.

O uso proficiente de informação pode ajudar as organizações a atingir vantagem competitiva sobre outras, o que contribui para o aumento do valor do negócio e mantém os *stakeholders* e outros investidores satisfeitos (Posthumus & Von Solms, 2004). Neste sentido, a gestão da informação tem mudado a forma como as organizações conduzem o seu negócio e como competem entre si, sendo fundamental para melhorar a sua vantagem estratégica e competitiva (Saloojee *et al*, 2007).

As organizações tomam decisões explícitas e implícitas sobre a demanda e o uso de informação. Estas decisões são baseadas em estimativas dos custos e benefícios espectáveis da informação, da sua estratégia ou estrutura (Feldman & March, 1981). Neste contexto, a gestão da informação tornou-se uma importante alavanca para a estratégia do negócio. Esta relação torna-se também crítica no planeamento estratégico de sistemas de informação, onde se procura alinhar os investimentos em gestão de informação com a estratégia de negócio, de modo a maximizar a vantagem competitiva da organização (Saloojee *et al*, 2007).

As organizações são consumidoras, gestoras e fornecedoras de informação, sendo a reputação da sua inteligência organizacional construída através da capacidade de assegurar, analisar e recuperar informação de forma atempada e eficiente. Face ao papel crítico que a informação tem nas organizações, é essencial que existam regras formalizadas nos procedimentos operacionais da organização para recolher, armazenar, usar e salvaguardar informação (Feldman & March, 1981).

2.2 – Gestão da segurança de informação

A ISO 27000, *standard* internacional de referência, define a segurança de informação como o processo de "preservar a confidencialidade, integridade e disponibilidade da informação" (International Organization for Standardization, 2014), sendo o seu principal objetivo garantir a continuidade de negócio e a minimização de danos ao limitar o impacto de incidentes de segurança (Von Solms, 1998). Uma gestão da segurança de informação limitada às tecnologias e processos de TI, não é capaz, por si, de garantir uma influência global nas grandes organizações (Sajko *et al*, 2011), uma vez que além de se tratar de um tema técnico, é também um tema cultural e de gestão (Casaca & Florentino, 2014).

À medida que a informação e os sistemas de informação se tornam cada vez mais elementos críticos e estratégicos para as organizações, a sua eficaz gestão torna-se uma preocupação crítica para as suas administrações (Calder & Watkins, 2012). Uma adequada gestão da informação passa também por garantir a sua segurança, pelo que são necessários responsáveis por este tema que tenham uma forte presença na organização e que sejam líderes com visão estratégica (Kark *et al*, 2016).

A governança da segurança organizacional é definida como o processo de definir, estabelecer e manter uma estrutura e processos de gestão que garantam que as estratégias de segurança de informação estão alinhadas e suportam os objetivos de negócio, que sejam consistentes com leis e regulamentações aplicáveis através de uma adoção de políticas e controlos internos, e que atribuam responsabilidades de modo a garantir uma melhor gestão de risco (Bowen *et al*, 2007). O processo de organizar a segurança de informação numa organização deve contemplar fatores como a sua missão, composição, posicionamento na estrutura organizacional, a sua autoridade, responsabilidades, funções e linhas de comunicação e coordenação (Peltier, 2013).

A responsabilidade do CEO (*Chief Executive Officer*) relativamente à segurança de informação não é diferente da sua responsabilidade relativa a qualquer outro tema da organização (Fitzgerald, 2007), e embora em muitas organizações a sensibilização relativamente a questões de segurança por parte da gestão de topo esteja em crescimento, esta atenção ainda é muitas vezes demasiado reativa (Johnson & Goetz, 2007).

Existem duas componentes essenciais na governança da segurança de informação que contribuem para uma estratégia efetiva perante os riscos a que a informação organizacional se encontra exposta: a componente organizacional, que envolve a posição e abordagem da gestão executiva e administração da organização relativamente à definição de uma estratégia e direção de segurança de informação; e a componente de gestão, que está focada em como a estratégia de segurança irá ser implementada e gerida (Posthumus & Von Solms, 2004).

Os processos de governança da segurança devem ser planeados, efetivos e supervisionados. Os riscos devem ser previstos e as funções e responsabilidades devem ser determinadas e delegadas de modo a garantir uma adequada segurança organizacional, de forma a atingir eficazmente os seus objetivos estratégicos (Sajko *et al*, 2011). Na definição de um guia para a gestão de segurança de informação, já em 2001 Basie von Solms apresenta 13 dimensões que, independentemente de como se encontrem definidas, deverão trabalhar em conjunto de modo a criar um ambiente seguro (Von Solms, 2001): (1) Dimensão Estratégica e de Governança Corporativa; (2) Dimensão Organizacional; (3) Dimensão de Política; (4) Dimensão de Melhores Práticas; (5) Dimensão Ética; (6) Dimensão de Certificação; (7) Dimensão Legal; (8) Dimensão de

Seguro; (9) Dimensão Humana; (10) Dimensão de Consciencialização; (11) Dimensão Técnica; (12) Dimensão Métrica; e (13) Dimensão de Auditoria.

Todo e cada indivíduo é responsável pelas diferentes faces da segurança de informação, desde estabelecer e manter uma cultura organizacional que suporte estas atividades, à implementação de projetos de segurança e ao garantir que as operações de segurança estão a ser apropriadamente geridas (Fitzgerald, 2007).

A segurança da informação deve, então, ser compreendida e tratada como uma disciplina multidimensional (Von Solms, 2001), devendo ser endereçada como uma responsabilidade de gestão e governança corporativa, onde devem ser desenvolvidos esforços de gestão de risco, de reporte e de responsabilização da liderança de modo a obter um adequado nível de maturidade de segurança na organização (Posthumus & Von Solms, 2004).

2.3 – Função do CISO

A delegação de um CISO, ou de um responsável pela segurança de informação, aponta a necessidade de uma liderança dedicada aos compromissos e necessidades de segurança de informação de uma qualquer organização (Peltier, 2013). A pessoa que desempenha esta função pode, ou não, ter este título, podendo ainda ser denominado de Diretor de Segurança, Gestor de Segurança ou *Information Security Officer*. No entanto, o seu título não é tão importante como as suas responsabilidades (Fitzgerald, 2007), que envolvem atividades tanto de natureza técnica, como de gestão e liderança (Goodyear *et al*, 2010).

Enquanto as funções do CEO e CIO (*Chief Information Officer*) estão mais claramente definidas devido à maturidade da descrição dos seus postos, a do CISO continua em evolução (Fitzgerald, 2007). No passado, a função do CISO era apenas focada na definição de normas e políticas técnicas de segurança, validando controlos de segurança e garantindo a proteção dos dados pessoais dos clientes. Atualmente as organizações estão conscientes que o ciber-risco está diretamente associado com as suas estratégias de inovação e crescimento (Goodyear *et al*, 2010).

É desejável que o CISO tenha pelo menos as seguintes características (SC Jobs, 2017): (1) capacidades de liderança; (2) competências de planeamento e gestão estratégica; (3) capacidade de tomar decisões no momento certo; (4) excelentes capacidades de comunicação e apresentação; (5) forte orientação para o cliente (interno e externo); (6)

ser flexível e adaptável; (7) capacidades de supervisão; (8) sólidas competências para gerir pessoas; (9) capacidade de adaptação às constantes mudanças das TI e das suas ameaças; e (10) entusiamo por tecnologias e segurança. É esperado que o CISO tenha extensos conhecimentos de segurança e conheça a razão da sua importância para a organização, podendo assim contribuir para a sua visão e missão (Fitzgerald, 2007).

Assim, o CISO tem que ser um mediador, orientador, questionador, analista e, consequentemente, um elemento chave na definição da estratégia de gestão de riscos organizacionais (Médice, 2013), tendo entre as suas principais responsabilidades (SC Jobs, 2017): (1) desenvolver e gerir a operação e implementação diária da estratégia de segurança de informação; (2) orientar uma avaliação contínua das práticas atuais de segurança; (3) executar auditorias de segurança e avaliações de risco; (4) supervisionar a gestão do departamento de segurança de informação, liderando e formando a sua equipa; (5) garantir a conformidade com o ambiente regulamentar; (6) desenvolver e implementar planos de continuidade de negócio; (7) proteger a propriedade intelectual da organização; (8) sensibilizar toda a organização relativamente aos riscos e estratégia de segurança de informação; (9) gerir os orçamentos de ciber-segurança; (10) reportar ao conselho de administração e ser um membro ativo da equipa de gestão de topo.

O posicionamento do CISO na organização influencia a sua capacidade de conseguir comunicar e ter a atenção da gestão de topo. Posto isto, para garantir um nível apropriado de visibilidade, a função de segurança de informação não pode estar no fundo da estrutura organizacional (Peltier, 2013).

Tendencialmente os CISO's reconhecem que podem beneficiar de novas competências, como o maior foco na estratégia da organização e uma maior interação com o conselho administrativo (Kark *et al*, 2016). Segundo um estudo realizado pela Deloitte (2017), mais de 90% dos CISO's esperam melhorar o alinhamento entre a estratégia de segurança e a estratégia da organização. No entanto, 46% temem a incapacidade de realizar este alinhamento.

O CISO tem um cargo executivo na organização, e tem a responsabilidade de estabelecer e manter a visão, estratégia e programa da organização de modo a garantir que a informação está apropriadamente protegida (Goodyear *et al*, 2010). Ao estabelecer a sua visão, o CISO deve criar uma declaração que descreva como ambiciona alcançar a sua missão na organização. Este documento deverá estabelecer referências para avaliar os

serviços de segurança desempenhados, para definir como a sua área irá funcionar, os processos operacionais padrão e medidas para transmitir confiança a clientes internos e externos (Peltier, 2013). Este plano deve incluir as metas e objetivos a serem atingidos num período de tempo relativamente longo, normalmente entre 3 a 5 anos, devendo definir marcos a ser alcançados, bem como estabelecer prioridades e sequências de tarefas a ser desempenhadas. O desenvolvimento deste plano deve ser consistente com a estratégia geral da organização e do TI (Peltier, 2013).

Devido a responsabilidades de cumprimento legal e normativo, as organizações de maiores dimensões deverão considerar a necessidade de ter um CISO independente dos elementos organizacionais afetados pela política de segurança, devendo esta independência ser evidente perante toda a organização (Peltier, 2013). A independência da função de segurança de informação deve também incluir o controlo sobre o seu próprio orçamento e recursos, assim como do seu espaço operacional de modo a permitir uma proteção apropriada dos seus próprios ativos sensíveis (Peltier, 2013).

Apesar dos CEO's e os CIO's terem diferentes interesses no trabalho do CISO – os CEO's esperam o cumprimento com requisitos regulamentares e a resposta a deficiências identificadas em auditorias, enquanto os CIO's esperam um acompanhamento próximo da segurança com as áreas de gestão de TI – os CISO's têm que se conseguir relacionar com estes de modo a compreender os verdadeiros riscos e como o negócio pode ser afetado por eles (Fitzgerald, 2007). Estas relações são bastante importantes, uma vez que o negócio não pode ser separado das necessidades de segurança, portanto é necessário associar os requisitos organizacionais com os requisitos de segurança, assim como os riscos de negócio com os riscos e vulnerabilidades de segurança (Fitzgerald, 2007).

A principal responsabilidade do CISO é coordenar a confidencialidade, integridade e disponibilidade da informação na organização. No entanto o CISO também tem que ser capaz de traduzir os seus problemas e sugestões numa linguagem que o CEO, CIO e restantes partes interessadas compreendam. Esta capacidade é fundamental para que o CISO consiga construir relações de confiança com todos os parceiros de negócio de modo a suportar a missão e visão da organização (Fitzgerald, 2007). Adicionalmente, o CISO tem a responsabilidade de influenciar e melhorar a cultura organizacional de modo a suportar a segurança de informação (Ashenden & Sasse, 2013).

Um dos desafios desta função é mudar o comportamento dos colaboradores. O CISO deve ser visível e ser ouvido de modo a melhorar a cultura organizacional, sendo mandatário usar uma comunicação de duas-vias com os funcionários de modo a reduzir a distância entre estes, aumentando o seu comprometimento com as iniciativas de segurança (Ashenden & Sasse, 2013).

Embora os CISO's possam enfrentar vários desafios nas organizações, eles são fundamentais para o sucesso das companhias. Segundo um estudo realizado pela IT Policy Compliance Group (Kessinger, 2010), a alocação de um CISO traz mais valor para a organização, nomeadamente ao (1) aumentar a retenção de clientes, faturação e/ou lucro; (2) diminuir a exposição financeira derivada de perdas de dados; (3) reduzir as taxas de roubo ou perda de dados; (4) melhorar os níveis de produtividade do negócio; e (5) reduzir custos com auditorias.

Neste sentido, o CISO moderno está intrinsecamente mais alinhado com a administração e gestão da organização, que com a vertente mais técnica de segurança. As organizações idealmente deveriam procurar um CISO que tenha experiência em cargos de gestão de risco e segurança, mas com antecedentes técnicos (Cave, 2017).

Apesar das considerações acima apresentadas, a ISACA e a RSA Conference realizaram um estudo juntamente com gestores e profissionais de ciber-segurança, onde se verificou que para 63% dos entrevistados a função de segurança de informação continua a reportar ao CIO, 14% ao CEO e apenas 8% reporta diretamente ao conselho de administração (ISACA, 2016).

2.4 – Enquadramento legal

A proliferação da crescente complexidade, sofisticação e ameaças globais para a segurança de informação, em combinação com os requisitos de conformidade com regulamentações globais de ciber-segurança e privacidade, está a levar a que as organizações tenham uma visão mais estratégica sobre a segurança de informação (Calder & Watkins, 2012).

O processo de organizar a segurança de informação numa organização, além de ter que estar alinhada com a missão e plano estratégico da organização, deve também incluir fatores associados a diretivas e regulamentos que podem potencialmente direcionar os esforços de segurança de informação (Peltier, 2013). Segundo Myles Bray, vice-

presidente da ForeScout Technologies, “o encorajamento regulamentar irá ajudar os conselhos de administração a garantir que alcançam maior visibilidade e segurança na organização, nos seus recursos e dados”, afirmando que “este encorajamento se trata de uma enorme necessidade e positiva evolução” (Cave, 2017).

É expectável que a adoção de legislação como o Regulamento Geral de Proteção de Dados (RGPD) e a diretiva Segurança das Redes e da Informação (SRI) tenham um impacto substancial nas práticas de segurança dos próximos tempos (Brown, 2017), aumentando a confiança nos sistemas e políticas de segurança nas organizações (Augustinos *et al*, 2016). Estas alterações legislativas criam oportunidade para as organizações melhorarem e reestruturarem a sua estratégia e infraestrutura de segurança, de modo a que a segurança se torne um maior facilitador para o negócio (Brown, 2017).

2.4.1 – RGPD – Regulamento Geral de Proteção de Dados

Trazendo penalizações pelo seu incumprimento, o Regulamento Geral de Proteção de Dados apresenta requisitos específicos relativamente aos direitos dos titulares dos dados, e relativamente às obrigações dos responsáveis pelo seu tratamento (quem determina as finalidades e meios de tratamento de dados pessoais) e respetivos subcontratantes (quem trata os dados pessoais por conta do responsável) (Council of the European Union & European Parliament, 2016).

Está à responsabilidade dos responsáveis pelo tratamento dos dados, a aplicação de medidas técnicas e organizativas que assegurem e comprovem que o tratamento será realizado em conformidade com o Regulamento e que assegurem que os dados apenas sejam processados se necessários para cada finalidade. Poderão ser aplicados códigos de conduta ou procedimentos de certificação, por exemplo a família de normas ISO 27000, como elemento para demonstrar a existência de medidas que contribuam para a salvaguarda da proteção de dados (Council of the European Union & European Parliament, 2016).

Sempre que uma organização sofra de uma violação de dados que seja suscetível de resultar num risco para os direitos e liberdades dos seus titulares, esta tem a obrigação de reportar esta violação à autoridade de controlo (CNPD) e aos seus titulares, no caso desta violação resultar num elevado risco para os seus direitos e liberdades. O Regulamento define como violação de dados qualquer violação de segurança que resulte na destruição,

perda, alteração, divulgação ou acesso não autorizados dos dados pessoais (Council of the European Union & European Parliament, 2016).

As organizações têm que conseguir comprovar o cumprimento dos requisitos do Regulamento, nomeadamente ao exigir que sejam documentadas as decisões de proteção de dados, que seja desenvolvida uma avaliação de impacto para processamentos de maior risco, e adotar uma estratégia de proteção de dados por desenho e por defeito (Allen & Overy, 2017; Council of the European Union & European Parliament, 2016). Estas provisões promovem a responsabilização, governança e transparência da proteção de dados, contribuindo para que sejam minimizados os riscos de violação de dados pessoais (ICO, 2017). O incumprimento das suas obrigações pode levar à aplicação de coimas até 20M € ou até 4% do seu volume de negócios mundial anual, consoante o montante que for mais elevado (Council of the European Union & European Parliament, 2016).

As autoridades ou organismos públicos, entidades que realizem monitorização sistemática e em larga escala de indivíduos, ou que realizem processamentos em larga escala de categorias especiais de dados devem delegar um encarregado pela proteção de dados (DPO – *Data Protection Officer*). Mesmo as entidades que não se encontrem abrangidos nos pontos anteriormente referidos, podem eleger um DPO. O responsável pela proteção de dados tem, pelo menos, as seguintes funções (Council of the European Union & European Parliament, 2016): (1) informar e aconselhar o responsável pelo tratamento de dados ou subcontratante, bem como a quem trata os dados, a respeito das suas obrigações nos termos do Regulamento e de outras disposições de proteção de dados; (2) controlar a conformidade com o presente regulamento, com outras disposições de proteção de dados e com as políticas da entidade; (3) controlar a realização da avaliação de impacto sobre a proteção de dados e prestar aconselhamento sempre que solicitado; e (4) ser o primeiro ponto de contacto com a autoridade de controlo e com os titulares dos dados.

Deve ser garantido que o DPO esteja envolvido atempadamente e de maneira apropriada nas questões relacionadas com a proteção de dados, que seja independente e não seja dispensado ou penalizado por cumprir as suas funções, que a execução das suas responsabilidades não resulte em conflitos de interesse com outras funções ou tarefas que desempenhe, e que reporte diretamente à gestão de topo da organização (Council of the European Union & European Parliament, 2016).

As organizações estão a debater-se relativamente à necessidade de criar uma responsabilidade adicional para o DPO, ou de a fundir com a função do CISO (Ataya, 2017), uma vez que o CISO é responsável pela segurança de informação, o que inclui a proteção de dados pessoais (Approach, 2017). Atendendo aos requisitos de independência definidos para o DPO, não pode ser automaticamente designado o CISO como responsável pelas suas funções (Roland, 2017). O CISO é o melhor aliado para as organizações à procura de iniciar um programa de privacidade de dados, uma vez que é responsável pela gestão dos seus riscos de informação, de incidentes de segurança e gestão de crise, que são também requisitos do RGPD. O CISO deverá também ter um papel fundamental na definição de uma estratégia de segurança que responda aos requisitos do Regulamento (Approach, 2017).

As organizações cuja eleição de um DPO seja mandatária deverão focar-se em garantir que esta eleição seja estabelecida de acordo com os requisitos do Regulamento, não sendo assim recomendada a combinação da função do DPO com a do CISO (Approach, 2017). Por outro lado, as organizações cuja eleição de um DPO não seja obrigatória deverão avaliar a utilidade e valor de delegar uma pessoa para este cargo. Nestes casos, o CISO poderá absorver as tarefas de um DPO, devendo ser garantido que (Approach, 2017) (1) o CISO adquire as funções e competências espectáveis para o DPO; (2) existe um investimento em termos de trabalho e recursos de modo a garantir que esta fusão não resulte em detrimento da segurança de informação; e (3) não exista conflito de interesses entre ambas as funções.

Independentemente de como sejam dispostas estas funções, é essencial que ambas as atividades estejam organizadas de forma a servir de linha de defesa para os riscos de segurança e de proteção de dados das organizações (Ataya, 2017).

2.4.2 – Diretiva SRI – Segurança das Redes e da Informação

A Diretiva 2016/1148 do Parlamento Europeu e do Conselho foi criada em 6 de junho de 2016 com o objetivo de apresentar medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (National Cyber Security Center, 2017; Parlamento Europeu e Conselho da União Europeia, 2016).

A União Europeia reconheceu que qualquer incidente de segurança poderia afetar vários Estados-Membros, tendo em 2013 avançado com esta proposta para aumentar a

maturidade de ciber-segurança da UE. Esta proposta tornou-se efetiva em agosto de 2016, dando aos estados membros 21 meses para transpor esta diretiva para legislação nacional (National Cyber Security Center, 2017; Parlamento Europeu e Conselho da União Europeia, 2016).

Estando a magnitude, frequência e impacto dos incidentes de segurança a aumentar, aumenta também a ameaça para o funcionamento das redes e sistemas de informação. Estes incidentes podem impedir o exercício de atividades económicas, gerar perdas financeiras importantes, danificar a confiança dos utilizadores e causar graves prejuízos à economia da União Europeia (National Cyber Security Center, 2017; Parlamento Europeu e Conselho da União Europeia, 2016). A criação desta diretiva demonstra a estratégia da UE em promover o ciber-espaço como uma área de liberdade e direitos fundamentais, procurando expandir o acesso à Internet como uma ferramenta para promover globalmente a democracia, sem aumentar a censura ou o controlo em massa (Cavelty, 2013).

A fim de garantir uma aplicação eficaz e inclusiva desta diretiva, é indispensável que todos os Estados-Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de segurança das redes e dos sistemas de informação no seu território. Adicionalmente, este normativo estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na UE, a fim de melhorar o funcionamento do mercado interno (National Cyber Security Center, 2017; Parlamento Europeu e Conselho da União Europeia, 2016).

Com o objetivo de cobrir todos os incidentes e riscos relevantes, a diretiva aplica-se a duas diferentes categorias de prestadores de serviços (Bird & Bird, 2016; Parlamento Europeu e Conselho da União Europeia, 2016): (1) operadores de serviços essenciais, tais como: energia, transportes, serviços financeiros, saúde, infraestruturas digitais; e (2) prestadores de serviços digitais.

Os Estados-Membros devem assegurar que estes prestadores de serviços tomem as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos a que as suas redes e sistemas são expostos na execução das suas operações e serviços (Parlamento Europeu e Conselho da União Europeia, 2016). Deverá também ser assegurado que os operadores de serviços essenciais notifiquem as autoridades competentes ou as CSIRT (*Computer Security Incident Response Teams*), sem demora

injustificada, dos incidentes com impacto importante na continuidade dos serviços essenciais por si prestados, devendo estas notificações incluir informação que permita as autoridades competentes determinar o impacto transfronteiriço dos incidentes. A notificação não acarreta responsabilidades acrescidas para a parte do notificante (Parlamento Europeu e Conselho da União Europeia, 2016).

A implementação desta diretiva é alcançada através da implementação de um conjunto de 14 princípios comuns de segurança, descritos em 4 objetivos de alto nível (National Cyber Security Center, 2017): (1) aplicação de apropriadas estruturas organizacionais, políticas e processuais, de modo a compreender, avaliar e gerir sistematicamente riscos de segurança para a rede e sistemas de informação a suportar serviços essenciais; (2) proporcionar medidas de segurança de forma a proteger os serviços essenciais e os seus sistemas de ciber-ataques; (3) capacidade para garantir que os mecanismos de segurança permanecem eficazes e detetam eventos de ciber-segurança que afetem, ou possam afetar, os serviços essenciais; e (4) capacidade de minimizar os impactos de um incidente de segurança na entrega de serviços essenciais, incluindo a capacidade de restaurar os serviços quando necessário.

Será dado suporte para ajudar as organizações a implementar estes princípios, específicos para o seu setor. Este suporte poderá tipicamente ser em forma de orientação ou casos de uso, podendo também incluir serviços com certificações específicas (National Cyber Security Center, 2017). A diretiva requer também que os Estados Membros adotem as suas próprias estratégias de ciber-segurança, definindo os seus objetivos estratégicos, políticas e medidas regulamentares, podendo designar autoridades nacionais que sejam competentes para a monitorização da aplicação da diretiva a nível nacional (Bird & Bird, 2016).

Esta diretiva também irá ajudar os profissionais da segurança de informação a reforçar a importância da ciber-segurança, assim como a incentivar uma abordagem de gestão de risco na elaboração de um plano de segurança de informação (Josi, 2016).

Tem sido demonstrada a importância da presença de cargos de liderança no âmbito da gestão da segurança de informação nas organizações. As linhas a quem o CISO reporta devem ser avaliadas e revistas, nomeadamente em termos do reporte direto ao CEO, visto que estas linhas podem impactar a eficácia do programa de segurança (Augustinos *et al*, 2016).

2.4.3 – Cybersecurity Disclosure Act of 2017

Em março de 2017 o *Cybersecurity Disclosure Act* de 2017 foi introduzido ao Senado dos Estados Unidos da América (Ross, 2017). Num esforço de melhorar a proteção dos clientes, aumentar a transparência para os investidores e garantir que as empresas públicas estão a priorizar a segurança de informação e privacidade de dados (Homeland Security Today, 2017), os senadores Jack Reed, Susan Collins e Mark Warner introduziram este ato, com o objetivo de promover transparência na supervisão dos riscos de ciber-segurança em empresas públicas (Veltsos, 2017).

Este projeto de lei obriga a que, em todos os relatórios anuais para a SEC (*Securities and Exchange Commission*), as organizações divulguem o nível de conhecimento de ciber-segurança nos conselhos de administração, e caso este não exista, que outros passos de ciber-segurança estão a ser adotados pela organização para mitigar esta falta de conhecimentos (Ross, 2017).

Tem sido verificado que vários conselhos de administração não têm os conhecimentos suficientes para compreender adequadamente as suas organizações e as complexidades do ciber-risco, e não têm feito um trabalho eficaz na gestão da exposição das mesmas (Homeland Security Today, 2017). Muitos especialistas consideram que se este regulamento for aprovado, representará um passo bastante positivo em melhorar a comunicação entre a ciber-segurança e o negócio (Ross, 2017), trazendo uma melhor proteção para empresas públicas, os seus clientes, e *stakeholders* (Homeland Security Today, 2017).

De acordo com um inquérito realizado pela *National Association of Corporate Directors* (NACD), concluiu-se que 86% dos entrevistados estão a dedicar mais atenção à supervisão da gestão de risco do que há 2 anos atrás. Destes entrevistados, 59% afirmaram que consideram desafiante supervisionar os riscos de ciber-segurança, e apenas 19% afirmaram que os seus conselhos de administração têm um elevado nível de conhecimentos de ciber-segurança (Homeland Security Today, 2017).

O conselho de administração é responsável por estabelecer a direção, cultura e proteção da organização. Como tal, a administração é responsável por estabelecer a cultura adequada, métricas e orientação para os seus executivos gerirem de forma adequada o ciber-risco ao seu nível de tolerância (Homeland Security Today, 2017).

A ciber-segurança está cada vez mais a transformar-se de um tema técnico para uma questão de gestão de risco, que se encontra alinhada com outros riscos operacionais (Homeland Security Today, 2017). Se este projeto de lei for aprovado, no atual formato ou noutro, deverá existir um esforço para garantir que as organizações estão a levar a sério a ciber-segurança e estão comprometidas em gerir os ciber-riscos. Esta preocupação deve começar no topo da organização, sendo passada até à base, tornando-se uma questão cultural para a organização (Veltsos, 2017).

2.5 – Normativos e *Frameworks*

Existem várias razões pelas quais os normativos e *frameworks* têm um papel bastante relevante na melhoria de abordagens perante a segurança de informação, nomeadamente ao (Hathaway, 2013): (1) melhorar a eficácia e eficiência de processos chave; (2) criar guias de boas práticas de gestão; (3) facilitar a integração e interoperabilidade de sistemas; (4) estruturar a abordagem perante a segurança de informação e modelos de negócio; (5) apoiar na definição de uma estratégia de segurança de informação, e (6) proporcionar crescimento financeiro.

As ferramentas apresentadas neste capítulo visam contribuir para o desenvolvimento da maturidade da segurança de informação organizacional.

2.5.1 – ISO 27001

A ISO 27001 (formalmente conhecida como ISO/IEC 27001) é uma norma internacional publicada em 2005 pela *International Organization for Standardization* e pelo *International Electrotechnical Commission*, emergindo do *standard* britânico BS 7799-2 (Disterer, 2013; Boehmer, 2008).

As normas da família ISO 27000 têm como objetivo endereçar cada atividade considerada necessária para gerir a segurança de informação (Armstrong, 2009), fornecendo requisitos para estabelecer, implementar, manter e melhorar de forma contínua um Sistema de Gestão de Segurança de Informação (SGSI) (International Organization for Standardization, 2013).

Esta norma é neutra em termos tecnológicos e de fornecedores, definindo um conjunto de especificações de melhores práticas para o desenvolvimento de um SGSI, usando uma

abordagem baseada em risco específica para a organização que a implementa e mantém (IT Governance Institute, 2015), sendo uma ferramenta versátil que pode ser aplicada em organizações de todos os sectores e tamanhos (Disterer, 2013).

Um SGSI direciona pessoas, processos e tecnologias, demonstrando que de facto as ameaças de ciber-segurança não são apenas de natureza tecnológica, mas que afetam a organização como um todo (IT Governance Institute, 2015).

Com a ISO 27001, as organizações podem ter o seu SGSI certificado por uma entidade habilitada para tal, podendo demonstrar evidência aos seus clientes das suas medidas de segurança (Disterer, 2013). Esta certificação pode ser utilizada por *stakeholders* internos e externos, para avaliar a habilidade da organização para ir de encontro com os seus requisitos de segurança de informação (International Organization for Standardization, 2013).

Com o objetivo de proteger a informação e sistemas de informação organizacionais, esta norma fornece um conjunto de objetivos de controlos, requisitos e orientações com os quais as organizações podem atingir níveis de segurança de informação adequados (Disterer, 2013).

Resumidamente, esta ferramenta manifesta-se assim como um contributo para o sistema de gestão para riscos empresariais, estabelecendo uma relação direta entre a segurança da informação e a segurança do negócio (Boehmer, 2008). A sua relevância para as organizações tem sido manifestada com o constante aumento de entidades certificadas (Disterer, 2013).

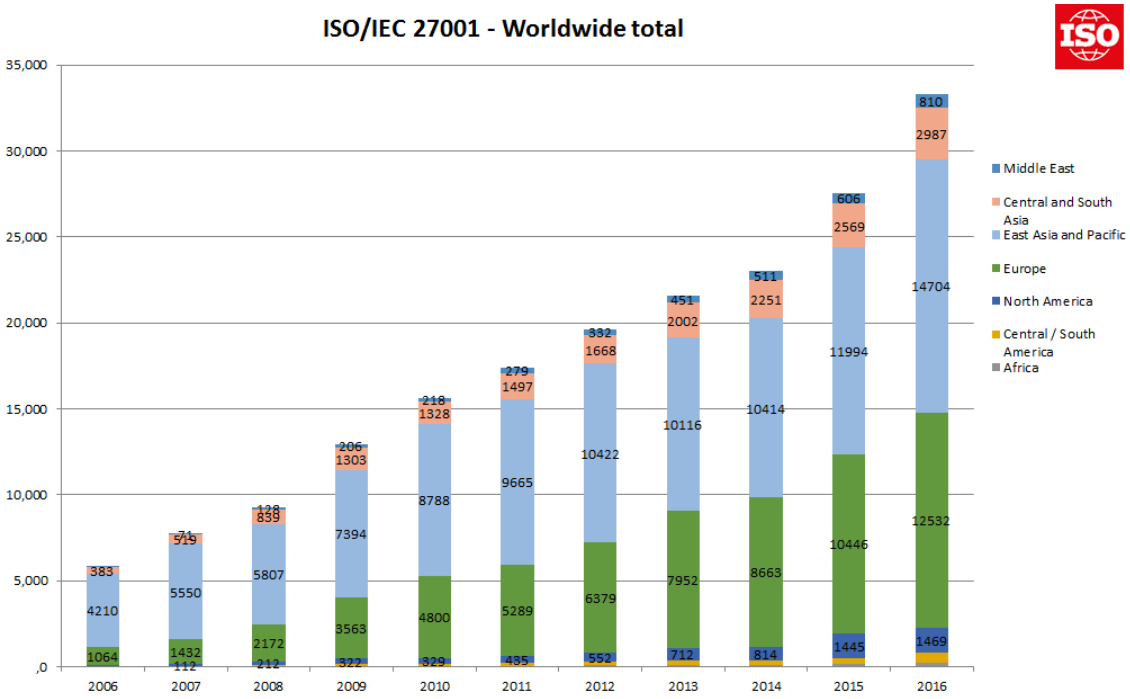

Figura II – Evolução global de certificações ISO 27001
Fonte: International Organization for Standardization (2018)

Tratando-se de uma ferramenta de gestão organizacional, as responsabilidades da gestão de topo em todas as fases do ciclo de melhoria contínua estão definidas (International Organization for Standardization, 2013). A liderança, como em todas as iniciativas chave de negócio, têm que ser dadas do topo, sendo requerido pela norma que este comprometimento seja evidenciado. Idealmente, o CEO deveria garantir o cumprimento do programa e que o seu objetivo se encontra alinhado com o plano de negócio (Calder & Watkins, 2012).

Esta ferramenta reforça a importância de um SGSI ser parte e estar integrado nos processos e estrutura de gestão global da organização, devendo ser considerada no desenho de processos, de sistemas de informação e controlos (International Organization for Standardization, 2013).

2.5.2 – COBIT

O COBIT – inicialmente conhecido como *Control Objectives for Information and Related Technologies* – é uma *framework* de boas práticas criada pela ISACA (Information Systems Audit and Control Association) para a governança de Tecnologias

de Informação, tendo a sua primeira edição sido lançada em 1996 (ISACA, 2012) (Stroud, 2012). Atualmente esta *framework* é globalmente aceite como um modelo no que concerne à gestão do TI empresarial (Anisingaraju, 2013).

Tendo a sua 5ª edição sido publicada em 2012, esta ferramenta fornece à gestão das organizações recomendações de como combinar as operações de negócio com os objetivos de operações de TI, e em como medir estes objetivos. O COBIT também ajuda as organizações a compreender que funções e tarefas estão incluídas nos seus procedimentos de TI (ISACA, 2012).

Nesta *framework*, a gestão e a governança estão separados em áreas diferentes. Os processos de gestão estão categorizados em quatro diferentes domínios: Planear e Organizar (APO), Adquirir e Implementar (BAI), Entregar e Suportar (DSS) e Monitorizar e Avaliar (MAE). Estes domínios são suportados por um total de 34 processos, que incluem diferentes atividades de gestão de TI (ISACA, 2012).

O COBIT é utilizado por muitas empresas, agências governamentais, instituições académicas e outras entidades, ajudando a desenvolver e documentar as estruturas organizacionais apropriadas, processos e ferramentas para uma eficaz gestão do TI de uma maneira compreensiva e integrada. Facilmente se integra e suporta outros *frameworks* e normas de negócio e TI, tal como o COSO, ITIL e ISO 27000, contribuindo assim para melhorar a sua eficácia (Qualified Audit Partners, n.d.).

A última versão desta *framework* tem várias áreas e domínios que estão cobertas pela ISO 27000, descrevendo diversas atividades de segurança e gestão de risco dentro dos processos de cada um dos domínios (ISACA, 2012).

Utilizando este modelo, as partes interessadas, tais como profissionais de segurança, executivos de operações de TI e auditores de TI conseguem ver como o seu trabalho se relaciona com o âmbito global da gestão da organização (Anisingaraju, 2013).

Com o objetivo de fornecer orientações mais concretas para os profissionais de segurança de informação – incluindo o CISO – o COBIT 5 *for Information Security* surge como uma evolução estratégica do COBIT 5, trazendo vários benefícios para as organizações, tais como (ISACA, 2012): (1) reduzir complexidade e aumentar a rentabilidade; (2) aumentar a satisfação dos *stakeholders* nas disposições e resultados de segurança de informação; (3) aprimorar a integração da segurança de informação na organização; (4) informar decisões de risco e garantir a consciencialização para as

mesmas; (5) reduzir incidentes de segurança de informação; e (6) incentivar a inovação e competitividade.

O COBIT 5 *for Information Security* é um guia profissional que se foca num vasto número de facilitadores, tal como funções de segurança, títulos, comités, conselhos, processos e políticas, dando assim orientações para uma eficaz gestão da segurança de informação (ISACA, 2012). Este guia traz uma nova visão da estratégia defendida pelo COBIT relativamente à gestão da segurança de informação. Na sua anterior versão, o COBIT 4.1 defendia que a gestão da segurança de informação deveria ser vista como uma subparte do TI, estando assim a estratégia de segurança de informação dependente da estratégia de TI (Morimoto, 2009).

Como se pode verificar na Tabela I, referente ao processo PO9 – *Avaliar e Gerir os Riscos de TI*, descrito no âmbito do primeiro domínio da *framework* – *Planear e Organizar* – a definição e adoção de uma estratégia de mitigação de riscos é criada a partir de atividades trabalhadas principalmente pelo CIO, conjuntamente com os executivos de negócio, sendo a segurança maioritariamente consultada, ou apenas informada, sobre estas atividades (IT Governance Institute, 2007).

RACI Chart / Activities	CEO	CFO	Business Executive	CIO	Business Senior Mangement	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives, and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives (some events are business-oriented [business is A]; some are IT-oriented [IT is A, business is C]).	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate and select risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Tabela I – Tabela RACI – Processo PO9 (Avaliar e Gerir os Riscos de TI)
Fonte: ISACA. (2012), p. 84.

Do mesmo modo, é possível verificar pela Tabela II, de acordo com o processo DS5 – *Garantir a Segurança dos Sistemas*, no âmbito do domínio *Entregar e Suportar*, que as funções de segurança apenas são vistas como as responsáveis pela execução da estratégia de gestão da segurança de informação, sendo o CIO o principal responsável pela sua concretização (IT Governance Institute, 2007).

RACI Chart — **Functions**

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Tabela II – Tabela RACI – Processo DS5 (Garantir a Segurança dos Sistemas)
Fonte: IT Governance Institute (2007), p. 119.

Neste sentido, o COBIT 5 traz uma nova visão sobre a gestão da segurança de informação e a função do CISO. O COBIT 5 *for Information Security* defende que o CISO é o responsável por desenvolver uma estratégia de segurança de informação empresarial adequada à direção e estratégia de negócio (ISACA, 2012).

Como se pode verificar na Tabela III, o COBIT 5 *for Information Security* estabelece a relação entre as diferentes atividades de segurança e o CISO, tendo este uma responsabilidade mais assente sobre estas atividades, verificando-se um maior alinhamento entre o CISO e o CIO, CFO e CEO. A indicação da natureza da relação entre os *stakeholders* e os tipos de informação é a seguinte (ISACA, 2012): A – Aprovador; O – Originador; I – Informado; e U – Utilizador.

Stakeholder	Information Type									
	Information Security Strategy	Information Security Budget	Information Security Plan	Policies	Information Security Requirements	Awareness Material	Information Security Review Reports	Information Security Service Catalogue	Information Risk Profile	Information Security Dashboard
Internal: Enterprise										
Board	U			I		U	I		A	
Chief executive officer (CEO)	U			A		U	I		U	
Chief financial officer (CFO)		A		U		U			U	
Chief information security officer (CISO)	O	U	O	O	A	A	A	A	U	U
Information security steering committee (ISSC)	A	O	A	U	U	I	U	I	U	U
Business process owner				U	O	U		U	U	
Head of human resources (HR)				U		U				
Internal: IT										
Chief information officer (CIO)/IT manager	U	O	U	U	U	U	I		U	U
Information security manager (ISM)	U	U	U	O	U	O	O	O	O	O

Tabela III – Relação entre os diferentes tipos de atividades de segurança e potenciais stakeholders
Fonte: ISACA (2012), p. 47.

Assim, o COBIT 5 defende que um alinhamento entre o CISO e o negócio desempenha um papel fundamental na eficácia da *framework* de segurança de informação da organização (Wolden *et al*, 2015).

3 – Metodologia de Investigação

No presente capítulo é apresentada a abordagem adotada para o estudo, assim como para a amostragem e recolha de dados e, por fim, o método adotado para a análise de dados.

3.1 – Tipo de estudo

Devido à natureza das questões de investigação, à contemporaneidade do tópico, e à escassez de literatura teórica, este estudo irá adotar uma abordagem indutiva, uma vez que se pretende ganhar uma melhor compreensão do contexto da investigação e do entendimento dos indivíduos em relação aos contextos e acontecimentos. Esta abordagem permite uma estrutura flexível de forma a facilitar alterações do ênfase do estudo à medida que a pesquisa avança (Saunders *et al*, 2009).

De forma a atingir os objetivos da pesquisa, será realizado um estudo exploratório, útil para compreender os acontecimentos, procurar novos entendimentos, fazer perguntas, e avaliar os fenómenos de outra perspetiva (Robson, 2002, citado por Saunders *et al*, 2009). A estratégia consiste numa análise de conteúdo suportada em entrevistas semi-estruturadas com questões direcionadas à pesquisa que se pretende realizar, uma vez que se visa obter um entendimento rico de contexto e agregar dados válidos e fiáveis relevantes para as questões e objetivos da investigação (Saunders *et al*, 2009).

O estudo será transversal, uma vez que se pretendem estudar as evoluções que levaram às circunstâncias atuais, assim como previsões futuras.

3.2 – Amostra e recolha de dados

A amostra é não-probabilística e auto-selecionada, uma vez que a pesquisa é principalmente exploratória e pretende-se que todos os casos tenham as características desejadas (perfis de gestão e administração com vários anos de experiência em temas relacionados com a segurança e sistemas de informação, tais como CISO’s / Diretores de Sistemas de Informação / Diretores Executivos / Consultores e auditores especialistas). Esta amostra providenciará uma análise rica em informação no qual será possível explorar as questões de investigação e obter novos entendimentos teóricos.

A amostra foi obtida através de contacto direto com convite para participar em entrevista, e é composta por 4 (quatro) CISO's, 3 (três) Diretores de Sistemas de Informação, 2 (dois) consultores/auditores especialistas e 1 (um) técnico de segurança informática. Esta amostra é considerada suficiente uma vez que as visões por perfil estão bastante alinhadas, tendo sido considerado que foi atingido o ponto de saturação. O desdobramento da amostra é o seguinte:

Ordem	*Função*	*Setor da Entidade*	*Código*	*Duração*
1	CISO	Energia	E1	~30m
2	Diretor IT e Técnico de Segurança	Farmacêutico	E2	~20m
3	CISO	Banca	E3	~1h10m
4	CISO	Regulador	E4	~35m
5	Consultor especialista	Consultoria e Auditoria	E5	~55m
6	Diretor IT	Farmacêutico	E6	~25m
7	Consultor especialista	Consultoria	E7	~45m
8	CISO	Investigação e Consultoria	E8	~1h15m
9	Diretor IT	Direito	E9	~50m

Tabela IV – Lista de entrevistados

Todas as entrevistas foram realizadas ao longo de 2018 e, à exceção da entrevista com E2 que foi realizada via contacto telefónico, todas as entrevistas foram presenciais. Adicionalmente, as entrevistas com E1 e E2 não foram gravadas, contrariamente a todas as restantes.

Fui adotada uma abordagem de entrevista semiestruturada para a recolha de dados qualitativos, uma vez que as questões são complexas e abertas, será útil explorar as respostas dos entrevistados de forma a desenvolver ou procurar explicação para as mesmas (Saunders *et al*, 2009). As questões do guião podem ser consultadas no Anexo I.

3.3 – Análise de dados

De acordo com Bardin (2010), a análise de conteúdo consiste num "conjunto de técnicas de análise das comunicações visando obter por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/receção (variáveis inferidas) destas mensagens".

Para a realização desta análise, são necessárias as seguintes operações mínimas (Vala, 1986): (1) delimitação dos objetivos e definição de um quadro de referência teórico orientador da pesquisa, (2) constituição de um *corpus*, (3) definição de categorias, (4) definição de unidades de análise, e (5) quantificação.

Considerando que o material a analisar foi obtido através de entrevistas com questões direcionadas à pesquisa que se pretende realizar, o *corpus* da análise é composto por toda a informação obtida, sendo que a categorização visa reduzir a complexidade do material a analisar, organizando-o de forma a potenciar a apreensão e a explicação da informação a reter (Vala, 1986). As categorias são compostas por termos-chave que representam o significado dos conceitos a registar nas mesmas, e deverão ser exaustivas – todas as unidades de registo deverão poder ser categorizadas – e exclusivas – cada unidade de registo só deverá poder ser incluída numa das categorias (Vala, 1986).

Já no que diz respeito às unidades de análise, diz Vala (1986) que estas podem ser divididas em unidades de registo, unidades de contexto, e unidades de enumeração. Uma unidade de registo é o segmento determinado de conteúdo que se categoriza colocando-o numa determinada categoria (Vala, 1986; Carmo & Ferreira, 1998) - para a presente análise, irá ser utilizada uma unidade de registo formal, uma vez que serão incluídas frases ou excertos de intervenções dos entrevistados. Já a unidade de contexto consiste no segmento mais largo de conteúdo que o analista examina quando caracteriza uma unidade de registo (Vala, 1986; Carmo & Ferreira, 1998). Por fim, a unidade de enumeração permite a quantificação e permite, por exemplo, e como é o caso neste estudo, contar a frequência de determinada categoria, sendo que é geralmente estabelecida uma relação entre a frequência de uma categoria e a sua importância no sistema de interesses da fonte (Vala, 1986).

O resultado desta análise pode ser consultado no Anexo II.

4 – Apresentação dos Resultados

O presente capítulo dedica-se à apresentação dos resultados obtidos através das entrevistas, estando a sua organização alinhada com as questões da investigação.

4.1 – Ambiente geral de segurança de informação

Com o objetivo de compreender como a visão e consciencialização perante a segurança de informação tem evoluído ao longo dos tempos, numa fase inicial das entrevistas tentou obter-se um entendimento da evolução, contexto geral e perspetivas futuras relativamente ao ambiente de segurança de informação nas organizações dos entrevistados.

Desta análise, foi possível verificar que a função da segurança de informação nas organizações era inicialmente muito técnica (E1, E3, E4 e E7), embora ainda existam várias organizações maioritariamente focadas na vertente técnica da segurança (E2, E6 e E7) e em que o CISO (ou a pessoa responsável pelos temas de segurança) não se encontra totalmente alocado a responder a estes temas (E5). Nomeadamente, verificou-se que o orçamento para a segurança nas organizações de maior parte dos entrevistados é definido pelo TI (E1, E2, E6 e E9), e apenas os CISO's E3 e E4 afirmam ter um orçamento próprio.

Apesar de ainda existir um grande foco por parte das organizações na vertente técnica da segurança, E7 e E8 concordam que cada vez mais existe a consciência que proteger o perímetro de segurança não é suficiente. Segundo E7 "as fronteiras esbateram-se completamente. Tens parte da infraestrutura *on-premises* e parte da infraestrutura na *cloud* (…), há todo o conjunto de movimentos que dissiparam completamente o que é a noção de perímetro e o que é a noção da segurança da infraestrutura. (…) Na banca, e em alguns outros setores, começa-se a perceber que a segurança é muito mais do que apenas proteger a infraestrutura e proteger sistemas e aplicações.". E8 vê também o caso *Stuxnet* como um contributo para esta mudança, "(…) na minha opinião foi um marco (...). O *Stuxnet* mostrou que é possível entrar numa rede *air gapped*, e por isso não se está seguro simplesmente por se estar isolado do mundo. Isso ajudou à mudança de mentalidade.".

Mesmo com esta mudança de paradigma, existe a visão de que as organizações em Portugal ainda têm uma maturidade de segurança muito reduzida e maioritariamente

reativa (E2, E5, E7 e E9), embora existam organizações que já estão a adotar uma estratégia mais preventiva (E1 e E5), verificando-se inclusivamente organizações que estão a contratar serviços externos de monitorização e deteção de eventos de segurança, para que possam estar mais focados em definir uma estratégia de segurança (E6) e a investir em seguros para incidentes de segurança de modo a encontrarem-se mais salvaguardados (E1 e E6). Segundo E5, verifica-se uma mudança de paradigma, principalmente na banca, que "estão agora a trabalhar muito na ótica da *framework* de cibersegurança e na função de cibersegurança (…) na prática estão a definir uma componente de *governance* de segurança".

E7 apresenta que "a visão que as organizações têm perante este tema não permite coloca-la ao nível de uma questão estratégica, que é onde ela deveria estar", uma vez que os crimes de segurança de informação estão cada vez mais avançados e organizados, devendo haver a mesma organização do lado de quem se está a proteger (E7 e E8).

Foi possível verificar o interesse em investir em *security intelligence* e *intelligence gathering* (E1 e E5) de modo a conseguir tornar a segurança mais inteligente e menos intrusiva (tanto para o negócio como para as pessoas) (E1), no entanto E5 apresenta que face à realidade que conhece, o trabalho nesta área ainda está muito atrasado. E3 apresenta ainda que seguiu um modelo de gestão integrado para a segurança de informação na sua organização, baseado na PAS 99 – *Integrated Management Systems*, que defende como algo muito importante para simplificar e tornar o trabalho mais eficaz, embora, no seu ponto de vista, ainda não exista consciencialização para este tema em Portugal.

E7 e E8 defendem que existe um problema cultural em Portugal no que toca à segurança de informação, sendo este um grande obstáculo para a maturidade da área no país. Portugal tem uma vantagem geográfica e geopolítica que acaba por reduzir a sua exposição para as ameaças vindas de outros países, embora esta vantagem acabe por resultar numa redução da visibilidade e sensibilização para o tema (E7). Segundo E8 "nós precisamos de cultura de segurança de informação em toda a sociedade, não é só nas administrações (...) nós temos que começar a incutir a cultura de segurança de informação na escola, da mesma maneira que nós incutimos a segurança rodoviária. Será um problema ao mesmo nível ou pior".

Existe, no entanto, a visão que as recentes alterações regulamentares, tanto internas (impostas por reguladores nacionais), como externas (como a SRI e o Regulamento Geral de Proteção de Dados), estão a mudar a cultura e consciencialização para os temas da segurança (E1, E2, E5, E7 e E8).

4.2 – Perfil e responsabilidades do CISO

Apesar de se ter verificado que a segurança se está cada vez mais a desprender de uma vertente puramente técnica, existe uma visão geral de que o CISO, apesar de não ter que ser um técnico puro, deve ter também antecedentes técnicos (E1, E3, E4, E5, E7 e E9). É considerado que o CISO deve ter conhecimentos técnicos, uma vez que deve ter uma visão crítica sobre os temas de segurança (E1), ter conhecimento das técnicas existentes (E4), e ter capacidade para comunicar adequadamente com as equipas técnicas responsáveis pelo tema (E5 e E7).

Além deste conhecimento técnico, é visto que o CISO deve também ter uma visão de negócio (E3, E4, E7), de governança (E5, E7) e uma visão estratégica sobre os temas de segurança (E1, E7 e E8).

E1 considera que o CISO deve ser um líder, deve ser capaz de gerir pessoas e ter uma boa capacidade de comunicação, tanto para cima como para baixo (E1, E3, E4 e E6), devendo também ter uma capacidade de reporte de modo a transmitir a mensagem de forma apropriada aos conselhos de administração (E1, E3 e E5). Para conseguir transmitir a mensagem adequadamente, o CISO deve ser capaz de comunicar sobre como os riscos de segurança a que a organização se encontra exposta se podem manifestar em riscos para a operação da mesma, devendo ser capaz de compreender e transmitir não só em termos de riscos financeiros, como também dos riscos sociais e ambientais (E1 e E3). No entanto, segundo E3, ”o COSO atualmente encontra-se na versão de 2018, em que o grande fulcro são riscos ambientais e riscos sociais. Tipicamente a nossa banca está muito focada no COSO 2013 que são riscos financeiros, não temos grande capacidade de evolução rápida nesse sentido. E muitas das vezes é preciso fazer notar a um *board* e a um *top management* que se calhar nem tudo o que fazemos é absolutamente correto e tentar fazer algumas mudanças, porque a mudança será por aí.”.

E3 e E5 afirmam que, para isto, o CISO deve ter uma relação próxima do negócio e não ter uma visão de segurança focada puramente no TI, deve compreender todos os

ativos de informação existentes, e como estes estão relacionados com a operação diária das diferentes áreas da organização. No entanto, o CISO também deve ter uma grande proximidade com as atividades do TI, sendo considerado por E4, E5 e E8 que se existir um acompanhamento da segurança durante todo o processo de desenvolvimento de projetos de sistemas de informação, podem reduzir-se custos em futuras intervenções corretivas, uma vez que este acompanhamento contribui para a maior robustez dos sistemas em termos de segurança desde a sua conceção, "hoje em dia usa-se muito o chavão de '*security by design'*, mas é mesmo uma necessidade porque é muito mais barato mexer num projeto numa fase de requisitos que numa fase de testes", defende E8.

O CISO deve também ter um forte espírito crítico e deve saber lidar com a pressão de modo a assumir riscos calculados (E3), devendo estar focado na melhoria continua das suas atividades e das áreas que se encontram sobre a sua responsabilidade (E3, E4 e E8). "Atualmente tens uma frente de ataque tão grande que acabas por ser desafiado pelas pessoas que te estão a atacar. (…) Há cerca de 1 ano houve um ataque, o *WannaCry* (...) e há coisas muito simples que poderiam ter sido feitas (…) não é como muitas entidades fizeram que foi, identificarem que estavam a ser atacadas, entrar em pânico e desligar as máquinas, causando uma negação de serviço a si próprias.", apresenta E3.

Ao analisar as áreas de intervenção que se encontram sob a responsabilidade do CISO, foi possível identificar 8 principais domínios, nomeadamente: (1) formação e consciencialização dos colaboradores e partes interessadas (E1, E5, E6, E7, E8 e E9); (2) gestão de risco (E1, E4, E5, E7 e E8); (3) gestão da continuidade de negócio (E1, E3, E4, E7 e E9); (4) gestão de incidentes (E4, E5, E8 e E9); (5) definição de um modelo de governo, políticas, processos e procedimentos (E1, E5, E7 e E8); (6) auditoria (E1, E3 e E9); (7) conformidade com boas práticas e regulamentação (E4 e E8); e (8) gestão de utilizadores e acessos (E1 e E2).

No âmbito da execução das suas funções, foram identificados alguns desafios que impactam na estratégia e operação do sistema de gestão de segurança de informação, nomeadamente: (1) conseguir investimentos numa área que não traz retornos financeiros diretos (E4, E5, E6, E7 e E9); (2) alinhar as pessoas com a estratégia de segurança (E1, E5, E7, E8 e E9); (3) comunicar de forma eficaz à administração (E1, E4, E5 e E9); (4) o impacto da segurança e dos controlos nas pessoas (E1, E3, E5 e E9); (5) alinhar a segurança com o contexto organizacional (E3, E5, E8 e E9); (6) o impacto da segurança e

dos controlos na operação diária na organização (E1, E6 e E8); (7) o investimento em pessoas (E4 e E7); e (8) a resistência à mudança (E3 e E9).

4.3 – Impacto das alterações regulamentares

Verificou-se um alinhamento geral relativamente ao impacto positivo que o Regulamento Geral de Proteção de Dados teve nas organizações, nomeadamente ao elevar a consciencialização para os temas de segurança (E1, E2, E7 e E8) e ao potenciar a segurança nas organizações (E1, E2, E4 e E5). "O regulamento tem uma contribuição interessante, que é a contribuição de levar à administração o problema, porque de repente eles são criminalmente responsáveis e a organização é responsável e poderá ter coimas avultadas, o que coloca o tema nos conselhos de administração. E esta foi uma boa contribuição do regulamento.", afirma E8. Segundo E7, "para quem trabalha em segurança, como eu, o RGPD é algo libertador porque de facto vem abrir as mentes das pessoas e as pessoas percebem que isto não é apenas uma questão de se acontece ou não acontece, é mais uma questão cultural, é mais uma questão das próprias organizações entenderem.".

E7 apresenta que "se há uma coisa que o nosso RGPD nos traz é nos aproximar dos *standards* e do nível de maturidade que os EUA acrescentam. Existem regras e leis de privacidade nos EUA há mais de 10 anos ao nível de dados e dados pessoais.". É considerado que o Regulamento é um bom ponto de partida para a segurança, mas não é suficiente, uma vez que para garantir privacidade é necessário existirem medidas de segurança, mas estas medidas não são suficientes para garantir a proteção dos ativos de informação do negócio (E7 e E8) – "Através da privacidade chegámos ao tema da segurança, mas a segurança não chega só para a privacidade, e os conselhos de administração precisam de perceber isso.", afirma E8.

Relativamente ao perfil do DPO, verificou-se que maioria das organizações dos entrevistados que delegaram um DPO, optaram por um perfil de direito (E1, E4, E7 e E9), tendo apenas a organização de E3 delegado alguém da área de segurança. Independentemente do *background* do DPO, existe a visão que para o Regulamento ser implementado com sucesso, deve existir um trabalho conjunto entre a segurança e o direito (E1, E3, E4 e E7). No caso da organização de E9, em que o DPO é uma pessoa de direito e não existe trabalho em conjunto com a segurança, E9 sente que o Regulamento

não foi visto como uma prioridade nem implementado de modo a garantir o seu total cumprimento.

Quanto à diretiva SRI, pelo número de pessoas que foi possível abordar o tema, verificou-se uma muito menor consciencialização para o mesmo. E5 defende que a Diretiva foi abafada pelo Regulamento e E8 acredita que tal possa ser também justificado pelo facto de ser direcionada apenas aos prestadores de serviços essenciais, tendo um impacto muito menos generalizado na sociedade. E7 e E8 defendem que em termos de segurança a Diretiva é muito mais urgente que o Regulamento. "A minha expectativa perante o NIS é que complemente o RGPD, porque tem uma vertente ligeira de direito e muito forte de segurança." apresenta E5.

Relativamente ao Regulamento, E7 e E9 consideram que a falta de compromisso do Estado foi um entrave para o compromisso das organizações e para a cultura de segurança que poderia advir daí. No entanto, E8 defende que a Diretiva poderá ter um impacto bastante positivo na cultura de segurança em Portugal, "a NIS era urgentíssima, principalmente porque a maior parte dos fornecedores de serviços essenciais são estatais ou com algum controlo do estado. (…) Por isso eu acho que a Diretiva NIS foi muito importante para obrigar o estado enquanto operador de serviços essenciais a tomar algum tipo de cuidados que não iria tomar porque não tem recursos e porque não estava na prioridade, e agora terá que ser uma prioridade.".

É apresentado por E5, E7 e E8 que para estas alterações regulamentares serem levadas com a devida seriedade e compromisso, assim como com uma perspetiva de melhoria continua, tem que existir uma fiscalização mais acentuada que a existente até à data. E8 apresenta que "não podíamos continuar no estado em que estávamos com a anterior diretiva (de proteção de dados), em que as comissões nacionais de proteção de dados ou equivalentes não tinham capacidade nenhuma para intervir (...) por isso na realidade a fiscalização era insuficiente. Eu espero que o regulamento ajude.". E7 conclui que "se ninguém fiscaliza e se ninguém faz o trabalho de garantir que está tudo a ser bem feito, vai ter que ser o cidadão. Mas se o cidadão se queixa e depois não existe consequências, o cidadão vai acabar por desistir.".

4.4 – Estrutura hierárquica e linhas de reporte

Relativamente ao posicionamento hierárquico da segurança na organização, verificou-se que, devido à necessidade de alinhar a segurança com a estratégia da organização e de transmitir os riscos de segurança e o seu impacto à administração, existe um alinhamento relativamente à necessidade do CISO fazer um reporte direto aos conselhos de administração (E1, E3, E4, E5 e E8), assim como à necessidade de ser independente (E3 e E4). Os consultores E5 e E7 vão ainda mais longe, ao defender que o CISO deve mesmo fazer parte do próprio conselho de administração, derivado à criticidade da sua função para a estratégia do negócio. "É um *C-level*", afirma E7, defendendo que tendo um cargo de "*Chief*", deve pertencer aos conselhos de administração.

Uma vez que os riscos de sistemas de informação estão sempre no topo da cadeia de riscos para a organização (E4 e E6), e por ser uma função muito mais orientada ao risco que à tecnologia (E8), de modo a não existirem conflitos de interesses, é considerado que o responsável pela segurança não deve estar abaixo nem reportar diretamente ao diretor de TI (E3, E4, E5, E7 e E8) – "Quando há uma reunião com o conselho de administração em que ele (o CISO) esteja lá, e esteja abaixo do *IT Manager*, ele não consegue reportar algo que vá contra aquilo que o *IT Manager* diz, porque é o chefe dele. No limite até pode ser despedido.", afirma E5. Uma vez que se trata de uma função muito focada em risco, E8 considera que em organizações de menor dimensão faria mais sentido o CISO encontrar-se sob a alçada da área de Risco, no entanto, E3 considera que colocar o CISO abaixo desta área pode ser insuficiente para assegurar as necessidades da segurança, uma vez que "(…) às vezes cai muito na tentação de produzir KPI's em excesso, podendo-se perder tão ou mais tempo a mostrar aquilo que fazemos, que em fazer.".

E3 e E4 defendem claramente que o CISO não pode estar no fundo da cadeia hierárquica das organizações, uma vez que quanto mais fundo na pirâmide esta função se encontrar, maior a suscetibilidade para existirem conflitos de interesses e para retirar força ao CISO junto da administração. "Com este afastamento da segurança com os conselhos de administração a segurança perde força, perde independência e acaba por perder a essência do seu trabalho.", afirma E4. Apesar disto, E5 afirma que "em termos de serviços não financeiros, não há nenhum caso que eu conheça que o CISO reporte diretamente à administração.".

Quando abordado o tema do Cybersecurity Disclosure Act de 2017 e o seu objetivo de garantir que existam conhecimentos para os temas e riscos de segurança de informação nos conselhos de administração, no geral a opinião foi positiva (E1, E3, E4, E5 e E7), e foi considerado que deveria também ser aplicada uma medida semelhante em Portugal ou na Europa (E1, E3, E4 e E7). Apesar do impacto positivo que esta medida pode trazer, a preocupação que existe é que as organizações sigam esta medida apenas no ponto de vista de cumprimento (E5 e E7), "isto para mim é um não controlo ter uma pessoa lá que não saiba do que está a falar. O que pode acontecer é agarrarem num administrador e passar a ser também o CISO.", apresenta E5. E7 apresenta também o caso de uma organização "que nomeou um CISO que (…) de segurança percebe zero e ficou nomeado porque os outros (administradores) acharam que tinham que ter um CISO nomeado, porque faz parte das regras e o próprio regulador da área de atividade obriga a ter um CISO, e ficou aquele. Não pode ser assim.".

No entanto, foi possível verificar que já existe algum trabalho neste sentido em Portugal: E3 apresenta que "(…) existe uma entidade que regula o setor bancário e depois existe uma associação portuguesa de bancos (…) é um tema que já veio à baila e já se tem uma ideia de que forma isto poderá ser alavancado (…) vamos ter que propor um caminho de ação ao Banco de Portugal e mostramos a estratégia e mostramos o objetivo e o Banco de Portugal fica confortável o suficiente para depois transcrever para decreto (…)". Adicionalmente, E4 apresenta que "algumas das empresas supervisionadas por nós são obrigadas a comunicar-nos todos os incidentes que possam de alguma forma meter em causa a continuidade das operações das organizações. Nós quando fazemos estes trabalhos de supervisão, a nossa preocupação inicial é saber se o *board* tem conhecimentos e consciencialização para os riscos de cibersegurança e de segurança de informação. Não havendo conhecimento deixamos uma recomendação forte e dizemos que todas as *frameworks* e boas práticas apontam para isso, e no fim ainda dizemos que eles são responsáveis por qualquer risco. Isto não é apenas porque são boas práticas, a justificação é mesmo essa, é que ao final do dia aquilo pode pôr em risco a organização, toda a operacionalização da empresa e no limite esta poderá falir.".

5 – Discussão dos Resultados

De acordo com a análise realizada, foi possível verificar que, embora este paradigma se encontre agora em mudança, as organizações em Portugal ainda se encontram muito focadas numa vertente técnica e reativa da segurança, não existindo ainda uma forte ligação com o negócio, e não sendo vista como um tema estratégico. Tal como apresentado por Von Solms (2001), a segurança deve ser compreendida como uma disciplina multidimensional, e apesar de ter sido possível verificar organizações que começam a ter esta visão, ainda se verifica um nível de consciencialização muito reduzido para o tema.

Ao comparar estes resultados com a literatura, é possível verificar o atraso da maturidade da segurança em Portugal, uma vez que já em 2005 a ISO 27001 apontava para a necessidade de haver o compromisso por parte da gestão de topo no sistema de gestão da segurança de informação e, em 2007 Johnson & Goetz verificavam o aumento da consciencialização para os temas da segurança por parte das administrações (embora ainda muito reativa).

No entanto, apesar de ainda se verificarem vários casos em que a segurança de informação se encontra posicionada sob a alçada do TI, começa a existir algum alinhamento quanto a, tal como defendido por Sajko *et al* (2011), esta abordagem não ser suficiente para garantir uma influência global e adequada na organização. Nos casos em que foi possível verificar esta visão, são apresentadas as teorias de Calder & Watkins (2012) e Goodyear *et al* (2010), defendendo-se que esta necessidade deriva da informação e dos sistemas de informação serem cada vez mais elementos críticos e estratégicos para as organizações, sendo que os riscos a que estas estão expostas podem manifestar-se diretamente em riscos para as suas estratégias de inovação e crescimento.

Em 2007, Fitzgerald apresentava que, contrariamente a outros *C-levels*, a função do CISO ainda se encontrava em definição e evolução. Foi possível verificar ainda esta situação, que pode ser justificada pela falta de maturidade que existe para o tema em Portugal. Foi possível notar a visão que esta falta de compromisso é maioritariamente de responsabilidade cultural, derivada da realidade geográfica e geopolítica do país, o que contribui para a visão que os crimes de segurança de informação são um tema que não afeta nem tem grande impacto em Portugal.

Foi, no entanto, possível verificar que o ambiente de segurança nas organizações tem estado a mudar e a evoluir. Esta mudança tem advindo muito, de acordo com a expectativa de Brown (2017) e do já verificado em 2012 por Calder & Watkins, do impacto das recentes alterações legislativas e da mudança cultural que vieram trazer. Apesar de se verificar um baixo compromisso do Estado para as alterações regulamentares vindas da UE, verificou-se mesmo assim uma mudança cultural relativamente aos temas de segurança. É considerado que o que atualmente existe ainda não é suficiente, mas é um começo, esperando-se que diretivas como a SRI (que impactam diretamente no Estado) e alterações regulamentares internas possam contribuir para aprofundar a cultura e maturidade da segurança em Portugal.

Segundo Peltier (2013), as organizações de maiores dimensões deveriam considerar a necessidade de ter um CISO independente dos elementos organizacionais. Das entrevistas realizadas, verificaram-se apenas dois casos em que existia esta independência, embora num dos casos a independência tenha sido perdida (apesar de já existir o trabalho de voltar a regularizar a situação). Devido à imposição do RGPD que o DPO seja uma pessoa independente dentro da organização, e da possibilidade desta responsabilidade ser assumida por alguém de segurança, existia a expectativa de que este requisito viesse a trazer mais independência para a função da segurança nas organizações. No entanto, das entrevistas, verificou-se que o Regulamento não foi um grande contributo neste sentido, uma vez que o único caso em que foi alocada a responsabilidade a alguém de segurança, já existia um CISO independente.

Relativamente ao perfil e responsabilidades do CISO, verificou-se um alinhamento geral entre os entrevistados e a teoria de Cave (2017), Kark *et al* (2016), Peltier (2013), Fitzgerald (2007) e Ashenden & Sasse (2013), nomeadamente: (1) na necessidade do CISO ter experiência em cargos de gestão de risco e segurança, devendo também ter conhecimentos técnicos (Cave, 2017); (2) do CISO ter que ser um líder com visão estratégica (Kark *et al*, 2016; Peltier, 2013; Ashenden & Sasse, 2013); (3) na necessidade de estar focado na estratégia da organização (Kark *et al*, 2016); (4) relativamente à segurança não dever estar no fundo da hierarquia organizacional (Peltier, 2013); (5) do CISO dever ter uma próxima interação com os conselhos administrativos (Kark *et al*, 2016; Peltier, 2013); (6) do CISO dever ser independente (Peltier, 2013); e (7) de ter a

responsabilidade de estabelecer uma cultura de segurança na organização (Fitzgerald, 2007; Ashenden & Sasse, 2013).

Verificou-se igualmente um alinhamento com as 13 dimensões para a gestão da segurança de informação apresentadas por von Solms (2001), embora não tenha sido abordada a dimensão ética. Relativamente às responsabilidades do CISO apresentadas por SC Jobs (2017), não foi possível identificar organizações que tivessem o CISO incorporado nas equipas de gestão de topo, e nas organizações em que a segurança se encontra abaixo da alçada do TI a dimensão orçamental acaba por não estar à sua responsabilidade. Apenas os consultores especialistas partilharam a visão de que o CISO deveria ter uma posição nos conselhos de administração, não tendo sido possível verificar esta realidade em nenhuma das organizações dos entrevistados. Foi também possível fazer um levantamento dos principais desafios para o correto desempenho das suas funções em que, adicionalmente ao desafio de alinhar as pessoas com a segurança apresentado por Ashenden & Sasse (2013), verificaram-se adicionalmente outros desafios tais como na obtenção de financiamentos para investir em segurança, na comunicação eficaz à administração, no impacto direto que a segurança tem nas pessoas e nas operações de negócio, e em conseguir encaixar a segurança no contexto organizacional. No entanto, tal como apresentado por Ashenden & Sasse (2013), cabe ao CISO influenciar e melhorar a cultura organizacional de modo a suportar a segurança de informação.

No que toca à posição do CISO dentro da estrutura hierárquica da organização, verificaram-se vários casos em que a segurança se encontra sob a alçada da Direção de Sistemas de Informação (DSI), contrariamente ao defendido por Peltier (2013), Casaca & Florentino (2014) e por alguns dos entrevistados. Os entrevistados que se opõem à alocação da segurança abaixo do TI defendem que esta decisão compromete a independência da função da segurança, uma vez que as tecnologias de informação e a segurança têm interesses que podem ser conflituantes. Um dos entrevistados defende que consoante a dimensão da organização, a segurança pode ser colocada sobre a alçada da área de Risco, no entanto foi também apresentado por outro entrevistado que esta decisão pode também comprometer o correto desempenho das suas funções.

Não foi possível concluir relativamente à necessidade de o CISO pertencer aos conselhos de administração, conforme defendido por SC Jobs (2017), mas sim sobre a

necessidade de os temas de segurança chegarem sem filtros à gestão de topo e de existir uma grande proximidade entre o CISO e os conselhos de administração. O facto de não se conseguir tirar uma conclusão sólida sobre a necessidade de o responsável pela segurança da informação pertencer aos conselhos de administração poderá estar diretamente relacionado com a falta de maturidade e cultura para o tema em Portugal.

6 – Conclusões

Este estudo apresenta uma visão geral do estado atual da segurança de informação em Portugal, assim como do rumo que está a ser seguido. É possível concluir que a maturidade da segurança no país ainda é reduzida face ao expectável e desejado.

As recentes alterações regulamentares têm apresentado um impacto positivo na consciencialização para os temas da segurança nas organizações e no próprio país. O tema da privacidade imposto pelo RGPD está a causar uma mudança cultural para estes temas, e existe a esperança que a implementação da diretiva SRI possa reforçar a consciencialização para os temas da segurança, nomeadamente por parte do Estado português, que será fortemente afetado por esta diretiva.

Foi possível identificar uma relação entre a função do CISO nas organizações e a consciencialização que existe para o tema da segurança dentro das mesmas. Nas organizações em que se verificou uma menor maturidade para os temas da segurança, o responsável por esta área encontra-se tipicamente abaixo do TI e é responsável pela execução de funções técnicas, detetivas e reativas de segurança. Nas organizações em que os conselhos de administração estão mais consciencializados para os riscos da segurança de informação e do seu impacto nas operações de negócio, na estratégia organizacional e na sua reputação, o CISO tem uma maior proximidade e independência junto dos mesmos.

Nos Estados Unidos da América, o Cybersecurity Disclosure Act de 2017 vem exigir a necessidade de existir alguém com conhecimentos de segurança de informação nos conselhos de administração. Existe a visão que as recentes alterações regulamentares (RGPD e SRI) vêm aproximar a maturidade da Europa com a dos Estados Unidos. Apesar de existir a visão por parte dos consultores especialistas de que faz sentido continuar a existir esta aproximação e que deve ser imposta a necessidade de existir alguém com conhecimentos de segurança nas administrações das empresas, ainda não se verifica esta visão nas organizações em Portugal.

Conclui-se que a função do CISO nas organizações e a sua missão poderá estar diretamente relacionada com a sensibilidade que existe para o tema, verificando-se que a segurança não é apenas um tema organizacional, mas também social e cultural.

O presente trabalho apresenta-se como uma referência para a sociedade e organizações ao demonstrar as evoluções, dificuldades e tendências que têm sido verificadas para o tema da segurança, contribuindo para que a gestão consiga antecipar e adquirir uma melhor capacidade de resposta às mudanças que possam surgir no futuro.

6.1 – Limitações do estudo

A primeira limitação deste estudo é o facto de ser transversal e apenas recolher dados num único ponto do tempo, não permitindo perceber a evolução dos pontos em análise ao longo do tempo como um estudo longitudinal.

Por outro lado, o estudo realizado tem como base a realização de entrevistas, tendo sido realizada posteriormente uma análise qualitativa das mesmas. Assim sendo, está sujeito às limitações inerentes à própria técnica, tais como a falta de motivação para responder às questões ou a incompreensão das questões, fornecimento de respostas falsas de forma consciente ou inconsciente, inabilidade ou incapacidade de responder adequadamente, enviesamento por parte do entrevistador em relação ao entrevistado, e/ou condução das respostas por parte do entrevistador (Gil, 1999). Tendo em conta que a entrevista foi semi-estruturada, tendo sido realizadas questões de resposta aberta, em certos casos não foi possível obter respostas objetivas aos pontos desejados.

Adicionalmente, existem as questões relativas à possível falta de representatividade da amostra. Sendo esta pequena e heterogénea (nove entrevistas, de sete setores de atividade), os dados recolhidos e as conclusões retiradas poderão não ser generalizáveis à população, tanto nacional como internacional, visto que apenas foram entrevistados indivíduos pertencentes a empresas ou sucursais localizadas em Portugal.

Por fim, a impossibilidade de entrevistar um ou mais diretores executivos (CEO’s) privou este estudo de obter a visão da administração relativamente aos temas em análise.

6.2 – Oportunidades para pesquisa futura

Face à teoria analisada, à informação recolhida, às conclusões retiradas, e às limitações do estudo, foram identificadas diversas oportunidades para pesquisa futura, que permitirão ampliar a compreensão relativa aos temas estudados, fornecer novas visões, e eventualmente novos rumos no que diz respeito à segurança de informação a nível global.

Em primeiro lugar, a realização de um estudo semelhante com uma amostra significativamente maior e em mais setores de atividade permitiria retirar conclusões generalizáveis à maioria das organizações. Por outro lado, seria também importante avaliar a evolução e adaptação da visão e cultura de segurança às novas realidades, bem como do papel do CISO, ao longo do tempo, pelo que a realização de um estudo longitudinal, repetindo a análise em um ou mais pontos no tempo, poderia trazer um contributo valioso.

Uma vez que para a realização deste estudo foi obtida a visão de elementos das áreas de segurança e/ou tecnologias de informação, teria sido interessante obter de igual forma a opinião de administradores das empresas, de forma a obter uma visão mais alargada dos temas em análise. Assim, sugere-se que pesquisa futura tenha em consideração o contributo destes elementos dos conselhos de administração.

Adicionalmente, este estudo incluiu o tópico do impacto das alterações regulamentares, e seria importante realizar uma análise relativa ao impacto da SRI nas organizações e na sociedade após a sua implementação.

Por outro lado, tendo em conta que, como mencionado anteriormente, existe a ideia que Portugal não é um país grandemente afetado por riscos relativos à segurança de informação, sugere-se também a realização de um estudo idêntico em países com uma maior exposição a estes riscos. De igual forma, a maturidade no que diz respeito ao tema da segurança, bem como a função do CISO nas organizações poderiam também ser estudadas em países com uma maior cultura e sensibilidade para os temas de segurança, como por exemplo os Estados Unidos da América. Ainda no que diz respeito à função do CISO nas organizações, poderiam ser realizados *case studies* de empresas que o tenham colocado na equipa de gestão de topo.

Por fim, recomenda-se a realização de um estudo transversal sobre a forma como a cultura de segurança num país afeta a cultura das suas organizações e dos seus cidadãos.

Bibliografia

Allen & Overy (2017). *The EU General Data Protection Regulation*. Consultado em 18 março 2018. Disponível em http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Allianz (2016). *Allianz Risk Barometer - Top Business Risks 2016*. Consultado em 9 outubro 2017. Disponível em http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

Anisingaraju, S. (2013). What Does COBIT 5 Mean for Your Business?. *COBIT Focus, 4*.

Approach (2017). *Why do you need a CISO?*. Consultado em 18 março 2018. Disponível em https://www.approach.be/en/images/gdpr_-_why_you_need_a_ciso-short.pdf

Armstrong, C. J. (2009). An approach to visualising information security knowledge. In *IFIP World Conference on Information Security Education* (pp. 148-155). Springer, Berlin, Heidelberg.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, *39*, 396-405.

Ataya, G. (2017). *Can a CISO act as a DPO?*. Consultado em 18 março 2018. Disponível em https://www.linkedin.com/pulse/can-ciso-act-dpo-georges-ataya/

Augustinos, T. P., Bauer, L., Cappelletti, A., Chaudhery, J., Goddijn, I., Heslault, L., ... & Leverett, E. (2016). *Cyber Insurance: recent advances, good practices & challenges*.

Bardin, L. (2010). Análise de conteúdo.(1977). *Lisboa (Portugal): Edições*, *70*, 225.

Bird & Bird (2016). *NIS Directive: New Security and Reporting Requirements for Infrastructure Providers and certain Digital Businesses.* Consultado em 18 março 2018. Disponível em https://www.twobirds.com/en/news/articles/2016/global/new-security-and-reporting-requirements-for-infrastructure-providers-and-certain-digital-businesses

Boehmer, W. (2008). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. *Emerging Security Information, Systems and Technologies*. SECURWARE'08. Second International Conference on (pp. 224-231). IEEE.

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for managers. In *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*.

Bradbury, D. (2011). In plain view: open source intelligence. *Computer Fraud & Security, 2011(4),* 5-9.

Brotby, W. K. (2007). *Information security governance: Guidance for information security managers*. ISACA.

Brown, D. (2017). *Is New Regulation a Threat or an Opportunity for Security Strategy?*. Consultado em 18 março 2018. Disponível em https://www.fireeye.com/blog/executive-perspective/2017/05/new-regulation-security-strategy.html

Cadete, G. (2015). Using Enterprise Architecture for COBIT 5 Process Assessment and Process Improvement. *IST, Portugal*.

Calder, A., & Watkins, S. (2012). *IT Governance: an international guide to data security and ISO27001/ISO27002*. Kogan Page Publishers.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24-38.

Casaca, J. A., & Florentino, T. (2014). Information Security Research: Actual Trends and Directions. *Conference of Informatics and Management Sciences, 8,* 251-256.

Catarino, T. M., Vasconcelos, A., & da Silva, M. M. (2016). The Role of the Chief Information Security Officer. *IST, Portugal*.

Cave, K. (2017). *Does the CISO role need to be formalised?*. Consultado em 18 Março 2018. Disponível em https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=40736

Dunn Cavelty, M. (2013). A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers, 23*.

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *REGULATION (EU)*, 679.

Deloitte (2017). The New CISO: Leading the Strategic Security Organization. *The Wall Street Journal*.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4(02),* 92.

Doughty, K. (2003). Implementing enterprise security: a case study. *Computers & Security, 22(2),* 99-114.

Feldman, M. S., & March, J. G. (1981). Information in organizations as signal and symbol. *Administrative science quarterly, 26(2),* 171-186.

Ferreira, M. M., & Carmo, H. (1998). Metodologia da Investigação-Guia para Autoaprendizagem. *Lisboa: Universidade Aberta*.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security, 16*(5), 257-263.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social*. 6. ed. Editora Atlas SA.

Goodyear, M., Goerdel, H., Portillo, S., & Williams, L. (2010). Cybersecurity management in the states: The emerging role of chief information security officers. *Available at SSRN 2187412*.

Hathaway, M. (2013). *Best Practices in Computer Network Defense: Incident Detection and Response* (35). IOS Press.

Homeland Security Today (2017). *Oversight Transparency of Cyber Risks at Publicly Traded Companies Addressed in New Bill*. Consultado em 18 Março 2018. Disponível em https://www.hstoday.us/channels/global/oversight-transparency-of-cyber-risks-at-publicly-traded-companies-addressed-in-new-bill/

ICO (2017). *Guide to the General Data Protection Regulation*. Consultado em 18 Março 2018. Disponível em https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Identity Theft Resource Center (2016). *Data Breach Reports – 2016 End of Year Report.* Consultado em 9 outubro 2017. Disponível em https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

ISACA. (2016). *State of Cibersecurity Implications for 2016: An ISACA and RSA Conference Survey*. Consultado em 18 março 2018. Disponível em http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

ISACA. (2012). *COBIT 5 for Information Security*. Rolling Meadows: ISACA.

ISACA. (2012). *COBIT 5: Enabling processes*. Rolling Meadows: ISACA.

ISACA. (2012). *COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização*. Rolling Meadows: ISACA.

International Organization for Standardization. (2013). *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International Organization for Standardization.

International Organization for Standardization. (2014). *ISO/IEC 27001: 201*4: *Information security management systems - Overview and vocabulary*. International Organization for Standardization.

International Organization for Standardization. (2018). *ISO Survey of certifications to management system standards - Full results*. Consultado em 18 março 2018. Disponível em https://isotc.iso.org/livelink/livelink?func=ll&objAction=browse&objId=18808772&viewType=1

IT Governance Institute (2007). COBIT 4.1. *Rolling Meadows: ITGI*.

IT Governance Institute (2015). Cyber Security & ISO 27001: A short introduction. *Rolling Meadows: ITGI*.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy, 5(3)*.

Josi, M. (2016). *What does the new EU Network Information Security Directive imply?*. Consultado em 18 março 2018. Disponível em https://www.cyan.network/news/what-does-the-new-eu-information-security-directive-implies

Kark K., François M. & Aguas T. (2016). *The new CISO: Leading the strategic security organization*. Consultado em 9 outubro 2017. Disponível em https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

Kessinger K. (2010). *New Report Show Benefits of CISOs*. ISACA.

Klahr R. & Amili S. & Shah J. & Button M. & Wang V. (2016). *Cyber Security Breaches Survey 2016 – Main Report*. Consultado em 9 outubro 2017. Disponível em https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Legg, P., Moffat, N., Nurse, J. R., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks,Ubiquitous Computing,and Dependable Applications, 4*(4), 20-37.

Lepofsky, R. (2014). COBIT® 5 for Information Security. *The Manager's Guide to Web Application Security*. Apress, Berkeley, CA.

Médice, R. (2013). *O Papel do Security Officer (Agente de Segurança)*. Consultado em 18 março 2018. Disponível em https://www.profissionaisti.com.br/2013/07/o-papel-do-security-officer-agente-de-seguranca/

Morimoto, S. (2009). Application of COBIT to security management in information systems development. In *2009 Fourth International Conference on Frontier of Computer Science and Technology* (pp. 625-630). IEEE.

National Cyber Security Center (2017). *Networks and Information Systems (NIS) Directive: Security objectives and principles*. National Cyber Security Center

Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard business review*, *83*(10), 96.

Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics, 105(2)*, 883-904.

Parlamento Europeu e Conselho da União Europeia (2016). Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho. *Jornal Oficial da União Europeia*, *194*, 1-30.

Peltier, T. R. (2013). *Information security fundamentals*. CRC press.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, *23*(8), 638-646.

Qualified Audit Partners (n.d.). *Control Objectives for Information and related Technology (CobiT)*. Consultado em 18 março 2018. Disponível em http://www.qualified-audit-partners.be/index.php?cont=315&lgn=3

Roland, N. (2017). *Would my CISO be my DPO? Information Technology Privacy.* Consultado em 18 março 2018. Disponível em https://commyounity1.wordpress.com/2017/06/23/would-my-ciso-be-my-dpo/

Ross, A. (2017). *What is the Cybersecurity Disclosure Act of 2017?*. Consultado em 18 março 2018. Disponível em https://baydynamics.com/blog/video-cybersecurity-disclosure-act-2017/

Sajko, M., Hadjina, N., & Sedinić, I. (2011). Information security governance and how to accomplish it. *MIPRO, 2011 Proceedings of the 34th International Convention*. IEEE.

Saloojee, R., Groenewald, D., & Du Toit, A. S. A. (2007). Investigating the business value of information management. *SA Journal of Information Management, 9(1)*.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students 5th ed. *England: Pearson Education Limited*.

SC Jobs (2017). *Job Description: Chief information security officer*. Consultado em 18 março 2018. Disponível em https://www.scmagazineuk.com/job-description-chief-information-security-officer/article/629762/

Stroud, R.E. (2012). *Introduction to COBIT 5*. ISACA. Consultado em 18 março 2018. Disponível em https://www.isaca.org/Education/Upcoming-Events/Documents/Intro-COBIT5.pdf

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476-486.

Vanson, B. (2016). *EU General Data Protection Regulation (GDPR) Are you ready for it?*. CA Technologies.

Vala, J. (1986). A análise de conteúdo. *In A. S. Silva, & J. M. Pinto, Metodologia das Ciências Sociais* (pp. 101-128). Porto: Edições Afrontamento

Veltsos, C. (2017). *The Cybersecurity Disclosure Act of 2017 (S 536) - What's New?*, Consultado em 18 março 2018. Disponível em https://www.linkedin.com/pulse/cybersecurity-disclosure-act-2017-536-whats-new-christophe

Von Solms, B. (2001). Information security—a multidimensional discipline. *Computers & Security*, *20*(6), 504-508.

Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, *6*(5), 224-225.

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems, 48*(3), 15-19.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. *IFAC-PapersOnLine, 48*(3), 1846-1852.

Anexo I – Questões das entrevistas

Questões realizadas durante as entrevistas:

- Contexto geral do ambiente de segurança de informação na organização.
- Qual tem sido o direcionamento da Segurança de Informação na organização?
- Onde está o CISO hierarquicamente colocado na organização?
- A quem reporta? Quais os comités que está inserido?
- Quem é o responsável pela definição e aprovação do orçamento para segurança de informação?
- Quais deverão ser as principais competências e responsabilidades de um CISO?
- Quais considera serem os principais desafios do CISO?
- RGPD e NIS/SRI – Qual a estratégia de segurança de informação para responder a estas regulamentações?
- RGPD e NIS/SRI – Como se tem estado a organização a preparar?
- RGPD e NIS/SRI – Têm ou vão existir alterações estruturais na organização derivadas destes regulamentos?
- RGPD – Foi ser delegado um DPO? Qual o seu perfil/*background*?
- Qual o contributo do DPO para a segurança?
- Tem conhecimento do Cybersecurity Disclosure Act de 2017?
- Cybersecurity Disclosure Act - Qual a sua opinião sobre este regulamento?
- Considera que seria adequado uma medida semelhante em Portugal ou na Europa?

Anexo II – Resultados análise das entrevistas

Categoria	Subcategoria	Unidade de Registo	Unidades de Contexto	Freq.
Ambiente Geral de Segurança de Informação	Evolução do contexto de segurança nas organizações	A função da segurança de informação nas organizações era inicialmente técnica	E1 (comunicação pessoal) afirma que ainda em 2010 o ambiente de segurança da sua organização ainda era pouco maturo, sendo as coisas construídas ad-hoc e o foco era na monitorização de eventos e incidências, diagnostico e definição de políticas técnicas. "Comecei a trabalhar em segurança de informação em 2001. (…) Na altura as preocupações eram absolutamente técnicas (…)" (E3); "O nosso antigo responsável de segurança era técnico de sistemas de informação (...)" (E4) "Eu lembro-me que antigamente o objetivo da segurança era proteger o perímetro e não preocupar com o que se passa cá dentro (…) a partir do momento em que controlava o perímetro eu assegurava-me que estava seguro e a infraestrutura estava segura e nomeadamente os meus utilizadores e os meus dados estavam seguros." (E7)	4
		Ainda existem muitas organizações maioritariamente focadas nos temas técnicos de segurança	Na organização de E2 (comunicação pessoal), o investimento em segurança é recente, e ainda muito orientado a controlos técnicos " (...) temos uma pessoa, que vem da área de administração de sistemas, agora tem estado sempre dedicada aos temas de segurança. " (E6) "Isto ainda continua a existir (…) ainda tens muitas organizações focadas nos controlos técnicos e em implementar sistemas." (E7)	3
		As diferentes linhas de atividade da segurança devem estar integradas	"O mercado tenta sempre verticalizar as questões (...). Cá em Portugal ainda não se evoluiu muito para uma framework que existe no mercado há algum tempo que é a PAS 99 – Integrated Management System. Se temos temas que são comuns e transversais numa organização e em termos certificativos, em vez de fazemos controlo documental para responder a certa norma, devemos fazer o 'keep it simple' que é manter tudo integrado para ser mais eficaz." (E3)	1
		Cada vez mais existe consciência que proteger o perímetro de segurança não é suficiente	""Eu lembro-me que antigamente o objetivo da segurança era proteger o perímetro e não preocupar com o que se passa cá dentro (…). Cada vez mais o nível de exposição é diferente, cada vez mais a exposição não tem tanto a ver com a infraestrutura nem com o perímetro, porque deixou de haver noção de perímetros (…) as fronteiras esbateram-se completamente, tens metade da infraestrutura on-premises e metade da infraestrutura na cloud (…) portanto há todo o conjunto de movimentos que dissiparam completamente o que é a noção de perímetro e o que é a noção da segurança da infraestrutura. (…)Na banca, e em alguns outros setores, começa-se a perceber que a segurança é muito mais do que apenas proteger a infraestrutura e proteger sistemas e aplicações." (E7) "Acho que houve algo que mudou, em 2010 com o Stuxnet. O Stuxnet na minha opinião foi um marco, que foi um malware desenvolvido com um alvo muito específico (...) o Stuxnet mostrou que é possível entrar numa rede air gapped, por isso não se está simplesmente seguro porque se está isolado do mundo. Isso ajudou à mudança de mentalidade." (E8)	2
		Existem organizações que investiram em	E1 (comunicação pessoal) diz que foi feito um investimento num seguro de segurança "Agora também fizemos, com o incentivo da administração, um seguro para incidentes de ciber-segurança (…)" (E6)	2

		seguros contra incidentes de segurança		
		O CISO não é responsável pela definição de orçamentos	E1 e E2 (comunicação pessoal) apresentam que o orçamento para a segurança é feito com base no orçamento do IT “Anualmente tenho um orçamento para o IT (…) e aloco uma fatia à segurança.” (E6) “A parte da segurança não tem uma rubrica específica no nosso orçamento, está dentro do chapéu do IT” (E9)	4
		O CISO é responsável pela definição de orçamentos	“Tenho orçamento próprio que é aprovado pelo CEO” (E3) “A segurança de informação tem um orçamento próprio.” (E4)	2
		Existem poucos recursos de segurança em Portugal	"Nós temos um problema grave em Portugal de falta de recursos nesta área, e faria sentido que se partilhassem recursos e custos por todas estas entidades e daqui sai uma equipa que ajudaria a trabalhar com todas estas organizações, um bocado à semelhança de como está a funcionar o CERT-PT em termos da banca." (E7)	1
		As organizações em Portugal ainda têm uma maturidade de segurança muito reduzida e maioritariamente reativa	E2 (comunicação pessoal) apresenta que os atuais objetivos para a segurança é a defesa das ameaças externas e a implementação de procedimentos de monitorização e deteção de incidências “Em termos de segurança, empresas médias e pequenas em termos gerais não há nada. Existe um ou outro caso em que agem sempre como resposta a um incidente e fazem qualquer coisa. É reativo e não é suficiente. Não têm a noção do que é um CISO e do que é o governance nesse tema.” (E5) "Eu ainda vejo uma maturidade de segurança ainda muito baixa cá em Portugal."; "Se olharmos para os 5 maiores bancos portugueses (...) vemos que há uma grande diferença de investimento, uma grande diferença de conhecimentos (...). Isto demonstra, no meu entender, uma grande falha de maturidade mesmo nestas organizações. E além da falta de maturidade e uma grande falta de sensibilidade para os perigos e para os problemas de segurança." (E7) "O maior driver numa sociedade de advogados para a implementação de questões de segurança é o cliente, porque há clientes que nos obrigam."; "Nós tivemos um caso de uma advogada e suspeita-se que alguém acedeu à informação que ela tinha (…) por algumas notícias que circularam na imprensa. Isto criou aqui alguma tração e algum awareness em algumas pessoas que se preocupam com o tema." (E9)	4
		Existe um problema cultural no que toca à segurança de informação	"A falta de maturidade de segurança cá em Portugal, não é só em termos de investimento, não necessariamente em termos de contratação de pessoas, mas fundamentalmente da forma como as empresas encaram a segurança. A segurança continua a ser um centro de custo direto, e acaba por ser visto como um mal necessário nas organizações."; "O nosso país é muito assimétrico nestas coisas, e não era necessário. Mas isto tem a ver com a nossa cultura, porque nós achamos que o mal nunca nos acontece a nós. O mal vai acontecer aos outros e vai passar ao lado, porque somos muito pequenos ou porque ninguém nos conhece. É isto que se sente na grande maioria das organizações." (E7) "Nós precisamos de cultura de segurança de informação em toda a sociedade, não é só nas administrações (...) a verdade é que as pessoas no geral em Portugal não têm conhecimentos (...) nós temos que começar a incutir a cultura de segurança de informação na escola, da mesma maneira que nós incutimos a segurança rodoviária. Será um problema ao mesmo nível ou pior." (E8)	2
		Portugal tem uma baixa exposição	"Nós estamos extremamente pouco expostos e isto também é uma vantagem nossa, é uma vantagem geográfica, geopolítica e acaba por ser uma vantagem para a nossa segurança. As nossas organizações são pequenas, embora possam ser apetitosas, mas não são apetitosas o	1

		aos riscos de segurança comparativamente com outros países	suficiente para uma máfia de leste focar-se em fazer malware direcionado para nós." (E7)	
		As imposições regulamentares estão a alterar o contexto de segurança nas organizações	"(...) em termos de banca, eles estão a mudar um ligeiramente o paradigma de segurança, (...)eles estão a alinhar, ou seja, eles começam com uma framework de gestão de risco – que não vem do zero, foi imposto pelo Banco Central Europeu – e depararam-se com muitos riscos associados à segurança de informação, obviamente." (E5)	1
		A segurança deve ser uma preocupação estratégica	"A visão que as organizações têm perante este tema que não permite coloca-la ao nível de uma questão estratégica, que é onde ela deveria estar." (E7)	1
		Existem organizações que estão a adotar uma estratégia mais preventiva	E1 (comunicação pessoal) afirma que desde 2015 a sua organização está mais focada numa defesa mais profunda, em definir processos, formar pessoas e implementar framerworks. "(...) eles (banca) estão a mudar a abordagem perante a segurança no sentido em que, estão a trabalhar mais numa base de controlos preventivos de segurança, muito associado claramente ao tema de dados, passando muito mais para uma ótica preventiva do que da ótica detetiva e reativa." (E5)	2
		Ainda há pouco trabalho de security intelligence e intelligence gathering	E1 (comunicação pessoal) planeia a curto prazo investir em security intelligence na sua organização. "No entanto o que é que ainda não se vê, ainda não fazem muito intelligence gathering (recolha de indícios, ataques que possam surgir, etc) (…)" (E5)	2
		Está a haver um trabalho de alterar o modelo de governo da segurança de informação	"(…) (as entidades bancárias) estão agora muito a trabalhar na ótica da framework de cibersegurança e na função de cibersegurança. Há vários nomes para isto, mas na prática estão a definir uma componente de governance de segurança" (E5)	1
		O CISO muitas vezes não está totalmente focado nos temas de segurança	"Tipicamente este elemento (o CISO) faz outras tarefas, muitas vezes não está dedicado totalmente ao tema de segurança." (E5)	1
		O CISO deve trabalhar com uma equipa	"O CISO não pode ser só uma pessoa, tem que ser uma equipa. É mais um custo, é verdade, mas este custo acrescenta valor e acrescenta alguma vantagem competitiva em relação às concorrentes ou pelo menos em relação aos perigos que existem, é isto que temos que avaliar." (E7) "Depois isto pode ser, dependendo da dimensão da organização, isto pode estar tudo numa pessoa, pode estar em equipas." (E8)	2

		Os crimes de segurança de informação estão cada vez mais organizados e tem que haver a mesma organização do lado da defesa	“Para quem estiver totalmente dedicado a ganhar dinheiro a fazer o mal e executando este tipo de ações (cibercrime), não é com os investimentos que se fazem em firewalls no nosso país que vão proteger." (E7) "(…) as ameaças hoje em dia são o crime organizado, extremamente organizado, e que faz disto negócio. E há números que indicam que o valor movimentado no cibercrime é comparável com o valor movimentado no tráfico de estupefacientes. O que faz com que tenha que existir o mesmo nível de organização do lado de cá. Nós não podemos levar o tema da segurança de forma acessória." (E8)	2
		Há organizações que estão a contratar serviços de deteção e monitorização de modo a estarem mais focadas na estratégia de segurança	"(...) o que estamos a olhar é investir em SOC, trabalhar com uma empresa externa que nos faça mais toda esta parte operacional e que tire esta carga da pessoa que temos cá dentro para que esta se foque em tudo o que é temas de visão, de estratégia e de tecnologia."(E6)	1
	Estrutura hierárquica e linhas de reporte	A segurança não deve estar no fundo da cadeia hierárquica da organização	“Quando a segurança está muito no fundo da pirâmide ou quando está muito dependente de uma certa área, há sempre conflitos de interesses, que podem ser desde financeiros como de estratégia” (E3) "Quanto mais próximo o CISO está do conselho de administração mais facilmente consegue passar a mensagem e ganhar empowerment, uma vez que acaba por ganhar exposição para transmitir os riscos de uma qualquer alteração do contexto de sistemas de informação e qual o impacto que tem para a organização." (E4)	2
		O CISO deve ser independente	“Nós não somos um departamento, não somos uma direção, somos alguém que reporta ao CEO de forma completamente independente (...). No passado cá, o antigo CISO reportava inicialmente à direção de Risco e Controlo e depois por decisão do CEO foi desagregada para ser mais independente.” (E3) “Entre 2014 e 2017 (...) existia independência total. (…) Com este afastamento da segurança com os conselhos de administração a segurança, a segurança perde força, perde independência e acaba por perder a essência do seu trabalho.”; “A IOSCO tem uma boa framework onde o artigo 2.3.4 menciona sobre a independência do responsável pela segurança (Guia de resiliência de cibersegurança no setor financeiro)” (E4)	3
		Em organizações não financeiras o CISO não reporta diretamente à administração	"Em termos de serviços não financeiros, não há nenhum caso que eu conheça que o CISO reporte diretamente à administração." (E5)	1

		O responsável pela segurança não deve reportar diretamente ao IT	"Um CISO tipicamente pendura-se no IT ou em Risco/Auditoria. Nem sempre garantimos a isenção para não haver conflito de interesses. Estando do lado do IT, se houver uma medida que do lado de segurança eu identifique que vai onerar o budget do IT e se o IT tiver um budget reduzido, (...) é fácil perceber para onde isto vai tender. No ponto de vista do Risco/Auditoria, às vezes cai muito na tentação de produzir KPI's em excesso, podendo-se perder tão ou mais tempo a mostrar aquilo que fazemos, que em fazer." (E3) "(…) houve uma necessidade identificada por parte de uma auditoria interna, que levou a que a segurança fosse separada do IT (...) o primeiro passo do trabalho do CISO é sempre uma análise de risco (...). 80 ou 90% dos riscos são de Sistemas de Informação, e se ele estiver debaixo de uma área de Sistemas de Informação, o colaborador não vai dizer mal do diretor." (E4) "Fora dos serviços financeiros, nas grandes organizações que conheço que têm um CISO, a maioria reporta, na minha opinião, erradamente ao IT manager. Na minha opinião, e em alguns casos na opinião dos próprios. (…) quando eles querem reportar uma certa situação que pode ser uma vulnerabilidade de segurança, mas vai contra os princípios de quem está a fazer a gestão do IT, vai haver ali uma colisão. "; "Quando há uma reunião com o conselho de administração em que ele (o CISO) esteja lá, e esteja abaixo do IT manager, ele não consegue reportar algo que vá contra aquilo que o IT manager diz porque é o chefe dele, no limite até pode ser despedido." (E5) "Eu vejo que a segurança continua muito focada e enquadrada dentro das áreas de IT, e cada vez mais deve começar a ter também uma separação (...)"; "O CISO não é um CSO (Chief Security Officer), esse sim deve estar debaixo do IT ou deve estar enquadrado no IT, deve ter responsabilidades operacionais e o CISO deve ter responsabilidades estratégicas." (E7) "Eu genericamente tendo a dizer que o CISO nunca deve reportar ao CIO porque as funções são de certa maneira ortogonais, ou seja, os objetivos do CIO são garantir que os sistemas de informação se adequam aos objetivos da organização, que nem sempre é compatível com os requisitos de segurança, e o mindset necessário é um bocado diferente. Em muitas organizações ainda vemos o CISO debaixo do CIO."; "Depende muito das organizações, mas a mudança que andamos a ver nos últimos anos é o sair debaixo da informática, ser uma função separada e paralela da informática, até para que os dois possam falar de igual para igual." (E8)	5
		O CISO deve fazer parte dos conselhos de administração	"O CISO tem um lugar no conselho de administração, e isto está correto." (E5) "O CISO é cada vez mais uma pessoa que deve estar num conselho de administração, é um C-level." (E7)	2
		O CISO deve reportar diretamente aos conselhos de administração	E1 (contacto pessoal) apresenta que tem reuniões 3 vezes ao ano com os conselhos de administração, e que são liderados por ele (CISO). Defende que o objetivo destas reuniões é "casar" a segurança com a estratégia da sua organização. "A segurança tem que ser crítica e pragmática. Obviamente eu tenho que fazer muito reporting, mas, felizmente (...) temos esta independência. No limite eu estou a discutir com o meu CEO questões que de outra forma não chegavam aos ouvidos dele." (E3) " Entre 2014 e 2017 havia reporte direto do CISO ao conselho de administração e existia independência total. De 2017 para a frente, trabalhamos mais em alinhamento com Sistemas de Informação e menos com o conselho de administração (…) Com este afastamento da segurança com os conselhos de administração a segurança, a segurança perde força, perde independência e acaba por perder a essência do seu trabalho."; "O board tem que ouvir os riscos, os riscos não podem vir filtrados para o board. As áreas de atuação do CISO acabam por advir daí" (E4) "Em termos de banca, do que conheço, não vi nenhum caso em que o CISO faça report direto à administração. Embora vejo no geral que os CISO's têm a opinião que faria mais sentido esta relação e é uma razão de queixa. Devia haver nem que seja uma meeting de segurança periódica ou sempre que necessário, e deve ser ele (o CISO) a liderar essa reunião com a comissão executiva." (E5)	5

			"Eu penso que o CISO deve reportar a alguém que faça parte da administração, do board, em organizações que têm uma área de risco, provavelmente ao Chief Risk Officer, é uma posição que me parece fazer mais sentido, porque a função do CISO é muito mais lidar com o risco que com os sistemas de informação. " (E8)	
Função do CISO	Perfil do CISO	Deve ter um background técnico, mas não puramente técnico. Deve ter também uma visão de gestão e governo	E1 (contacto pessoal) defende que é aconselhável que o CISO tenha alguns conhecimentos técnicos para conseguir ter uma visão crítica sobre os temas de segurança, mas no entanto existem outras competências que são tão ou mais importantes. "No geral, as pessoas que trabalham em segurança de informação, nasceram no mundo tecnológico (...) e depois começaram a assumir a responsabilidade pela área. Não é uma má visão, mas no meu ponto de vista peca numa questão: quando estou a falar com o meu board tenho que falar em alto nível, em negócio, não posso estar a falar em tecnologia." (E3) "O CISO não tem que ser um hacker. Nem todos os polícias para aprender a ser polícias tiveram que ser ladrões. Tem que ter conhecimento das técnicas, tem que ter conhecimento do que quer proteger, tem que ter muitas competências de controlos de segurança a implementar nos sistemas de informação (lógica e física) (...) O conhecimento técnico é bom para avaliar o contexto, só. (...) A questão de ter um background totalmente técnico é sempre complicado para depois passar a mensagem certa para cima. " (E4) “O perfil ideal para o CISO, não tem que ser uma pessoa demasiado técnica, mas tem que ter algum background técnico. Tem que ter 2 backgrounds distintos, que são muito importantes e equiparados. Um deles é o técnico (...) tem que o que se está a falar para falar a linguagem conjuntamente com os técnicos. Mas depois tem a 2ª que é toda a componente de governance, tem que ser uma pessoa muito equilibrada nessa componente (...). Estas duas estão equiparadas, (...) sendo que será muito pior, na minha opinião, se for uma pessoa puramente teórica e não tiver nenhum conhecimento prático. Uma pessoa prática consegue ganhar essa sensibilidade, mas muito dificilmente vejo um teórico a ligar-se à componente técnica.” (E5) "Tem que ter um background técnico, não pode ser puramente teórico, (...) na minha forma de pensar um CISO tem que vir do mundo técnico e tem que perceber como as coisas funcionam, porque o CISO é quem vai conseguir fazer a tradução dos problemas para as outras pessoas que não entendem a linguagem técnica e querem ver aquilo ligado a números, investimento e retornos."; "Beneficiamos muito se o CISO vier do mundo técnico e se tiver alguém dentro da equipa dele pessoas que saibam fazer essas análises mais financeiras e que saibam colocar isto mais de um ponto de vista de negócio"; "(...) no entanto não deve ser um técnico puto, deve estar focado em definir modelos de governo, em participar (mesmo que não faça parte dos conselhos de administração) nas reuniões de administrações, deve entender o negócio, deve ser uma pessoa que perceba onde é que a segurança se enquadra no negócio." (E7) “Eu vejo que na perspetiva de segurança têm que haver 2 perfis de utilizadores (...) tem que haver um perfil preocupado com as questões de awareness e de processos, e tem que haver um perfil técnico de uma perspetiva de auditoria regular, montar um SIEM, olhar para logs, etc...” (E9)	6
		Deve ter um background de auditoria	"No entanto não há nada melhor que questionar as equipas operacionais, por isso é que é bom um bom background de auditoria de sistemas de informação, porque sabe fazer as perguntas certas, às pessoas certas, no tempo certo" (E4)	1

		Deve ter visão estratégica	E1 (comunicação pessoal) afirma que as funções e responsabilidades de um CISO não diferem das funções de um qualquer outro diretor: definir uma estratégia (neste caso de segurança) e desenhar um roadmap para atingir estes objetivos "Tem que ser alguém que perceba do tema (segurança) e que leve o tema de uma forma totalmente estratégica." (E7) "(...) mudança do papel do CISO, porque começa-se a perceber que a segurança não pode ser algo desgarrado do negócio, não é uma função de suporte às tecnologias de informação, não é uma questão meramente tecnológica e é preciso trabalhar no ponto de vista estratégico e a longo prazo. Para isto é preciso alguém que perceba o estado atual, as tendências e olhar para a segurança como ela irá evoluir e como a organização deve evoluir."" (E8)	2
		Deve ter espírito crítico	"O CISO tem que demonstrar espírito crítico e independência de modo a ter uma visão global e detalhada sobre os reports e KPI's que lhe são disponibilizados por terceiros" (E3)	1
		Deve ser um líder	E1 (comunicação pessoal) defende que a competência relacional de um CISO é óbvia, sendo que é muito importante para a execução da sua missão que tenha boas capacidades de liderança e para gerir recursos humanos	1
		Deve ter uma boa capacidade de comunicação (para cima e para baixo)	E1 (comunicação pessoal) defende que para existir uma ligação e compromisso com a administração é crucial comunicar de forma que os temas de segurança sejam compreendidos e que tenham impacto nos boards "Quando estou a falar com o meu board tenho que falar em alto nível, em negócio, não posso estar a falar em tecnologia." (E3) "O mais importante num CISO até diria que é a comunicação e a passagem da mensagem (…)" (E4) "Como é lógico, uma apresentação que eu faça à administração sobre os temas de segurança, não é a mesma que eu faço à minha equipa ou a outro tipo de fórum. Desde que a mensagem vá bem formatada e que não entre em detalhes demasiado técnicos que eles não compreendem e que seja algo mais simples, acho que não há qualquer obstáculo e até vejo interesse por parte deles." (E6)	4
		Deve saber lidar com o stress e pressão / Deve ser comedido e assumir riscos calculados / Não deve ser impetuoso	"Atualmente tens uma frente de ataque tão grande que acabas por ser desafiado pelas pessoas que te estão a atacar. (…) Há cerca de 1 ano houve um ataque, o WannaCry (...) e há coisas muito simples que poderiam ter sido feitas, como analisar o que estava a correr na máquina (...) e identificar um padrão ou uma possível assinatura e colocar numa IPS e validar se resulta e se consegue impedir a propagação. Não é como muitas entidades fizeram que foi, identificarem que estavam a ser atacadas, entrar em pânico e desligar as máquinas, causando uma negação de serviço a si próprias." (E3)	1
	Competências e responsabilidades	Capacidade de reporting	E1 (comunicação pessoal) afirma que um dos fatores críticos para a capacidade de comunicar ao seu board é ao apresentar ratings e avaliações de segurança realizados na sua organização, de modo a consciencializar sobre o ambiente de segurança na sua organização. "O reporting que eu faço ao CEO é bastante assertivo, somos bastante objetivos naquilo que reportamos. O board gosta desta vertente mais challenged que temos cá dentro (...). Nem sempre é pacifico, mas sentimo-nos bem em fazer isto, uma vez que o nosso objetivo é que a organização progrida como um todo." (E3) "(o CISO) tem que ter capacidade para (…) fazer o report à administração e todos os seus outros reports periódicos" (E5)	3

		Além dos riscos financeiros, compreender os riscos sociais e ambientais da atividade da sua organização	E1 (comunicação pessoal) considera que o principal fator de sucesso na sua relação com os conselhos de administração é a capacidade de traduzir os temas de segurança em temas de risco para o negócio e, face ao setor da sua organização, em risco social e ambiental "(...) O COSO atualmente encontra-se na versão de 2018 em que o grande fulcro são riscos ambientais e riscos sociais. Tipicamente a nossa banca está muito focada no COSO 2013 que são riscos financeiros, não temos grande capacidade de evolução rápida nesse sentido. E muitas das vezes é preciso fazer notar a um board e a um top management que se calhar nem tudo o que fazemos é absolutamente correto e tentar fazer algumas mudanças, porque a mudança será por aí." (E3)	2
		Ter uma relação próxima do negócio e não ter uma visão de segurança puramente focada no IT	"Nós quando viemos para cá e começámos a fazer testes (de continuidade de negócio), nós decidimos não só fazer testes de IT. (...) Começámos a envolver e falar com as áreas e perceber efetivamente no negócio como eles trabalham diariamente, que ferramentas utilizam, de que forma registam o que fazem, quais os "helpers" ou a que recorrem para tarem a fazer o seu trabalho normalmente e fazer o mapeamento com o ponto de vista tecnológico, mas não só (que é um erro crasso que aí também se vê em continuidade de negócio)." (E3) "Às vezes também é preciso aproximar mais o CISO das áreas (da organização), explicar o que está a fazer, o que vai acontecer e quais as implicações de não fazer. " (E5)	2
		Acompanhar os projetos de sistemas de informação de raiz	"Trabalhamos mais em alinhamento com Sistemas de Informação, tudo o que seja security by design (…)" (E4) "A questão é, fazer a proteção de um ativo, não é só fazer a proteção uma vez a proteção. Durante todo o ciclo de vida deste equipamento eles têm que estar precavidos que ele realmente vai correr. Isto tem que ser corrigido na génese. Quando um software entre para produtivo, um software não pode entrar em produção sem ter as devidas validações, seja análise de código fonte, seja análise o próprio teste de introdução, se em desenvolvimento estiver ok, depois vai a produção. Eu não conheço nenhuma empresa neste momento que faça isto nestes moldes. (E5) " (…) nos projetos que envolvem Sistemas de Informação, para conseguir gerir e identificar os requisitos de segurança e possuir uma arquitetura de segurança para a organização na qual consegue enquadrar não só os sistemas que existem, mas também os novos que vão existir. A segurança tem que começar logo no início do projeto, hoje em dia usa-se muito o chavão de "security by design", mas é mesmo uma necessidade porque é muito mais barato mexer num projeto numa fase de requisitos que numa fase de testes" (E8)	2
		Focar-se na melhoria continua das suas atividades	"O business continuity que tínhamos era muitas vezes visto como, e isto é outra coisa que é típico nas organizações, que é (…) fazer um conjunto de documentos que digam de A a Z como é que nós vamos fazer isto, fazemos um teste anual feito sempre da mesma forma e do mesmo formato e da mesma maneira, ficou tudo verde e está fechado. Muitas vezes temos que fazer o challenge (...) se mantemos as pessoas na zona de conforto, não evoluímos. Pegando no ITIL, estamos a falar na melhoria continua que não é preciso ser muito disruptiva, às vezes basta mudar uma peça." (E3) "(...) associado a isto tudo, temos a monitorização e melhoria continua dos nossos processos." (E4) "A paisagem à nossa volta vai mudar e está a mudar, a função do CISO é estar atento e adaptar-se." (E8)	3
	Áreas de intervenção	Gestão de risco	E1 (comunicação pessoal) defende que o CISO deve ser capaz de gerir e comunicar os riscos de segurança, assim como desenvolver capacidades para mitigar estes riscos "O primeiro passo do trabalho do CISO é sempre uma análise de risco (…) ter esta competência e visão de risco e controlo. Diria que isto é fundamental na posição." (E4)	5

			"(…) se o CISO tiver dois fogos, ele nem sabe qual vai tratar primeiro se não souber o que tem mais impacto por não estar linkado com o risco associado." (E5) "Quem trata da área da segurança de informação muitas vezes também está envolvida nas equipas (...) operacionais de risco e da gestão desse próprio risco (...)" (E7) "O CISO tem que ser responsável pela gestão dos riscos de informação da organização (...)" (E8)	
		Gestão de continuidade de negócio	E1 (comunicação pessoal) apresenta a continuidade de serviço (negócio) como uma das áreas à sua responsabilidade "Temos cá implementado um business continuity, pelo qual eu sou responsável (...)" (E3) "O meu trabalho é focado (...) na parte de continuidade de negócio."(E4) "Quem trata da área da segurança de informação muitas vezes também está envolvida nas equipas de continuidade de negócio (...)" (E7) " (…) faz parte das responsabilidades de um CISO a definição de PCN's, planos de gestão de incidentes, preparar e testar cenários de emergências. Ele tem que ter uma visão da organização suficientemente precisa para perceber como aquela organização pode funcionar numa situação de emergência" (E8)	5
		Definição de um modelo de governança	E1 (comunicação pessoal) defende que uma das responsabilidades do CISO é a definição de um modelo de governo da segurança "(o CISO) tem que ter capacidade para definir políticas e saber fazer cumprir as políticas (…)" (E5) "(o CISO) deve estar focado em criar Diretivas e em determinar processos (...)" (E7) " (...) tem que ser responsável pela gestão de todo o programa de segurança, desde a definição de políticas, processos, responsabilidades e alocação de recursos." (E8)	4
		Gestão de incidências	"O meu trabalho é focado (...) na gestão de incidentes (...)"(E4) "(o CISO) tem que ter capacidade para (…) tratar do processo de incident management(…)" (E5) "Uma grande componente para a qual o CISO deve olhar é a gestão dia-a-dia da função de segurança, dos incidentes, do SOC a uma equipa de resposta a incidentes (CSIRT), isto implica que o CISO tenha visão sobre essa equipa e que acompanhe a análise da threat landscape, e da monitorização da segurança, de incidentes e de como estes estão a ser geridos" (E8) "Eu vejo que na perspetiva de segurança (...) tem que haver um perfil técnico de uma perspetiva de (...) montar um SIEM, olhar para logs (...)" (E9)	4
		Compliance	"O meu trabalho é focado (...) nas boas práticas no mercado (…) boas práticas e regulação, porque nós também somos obrigados obviamente a cumprir com algumas Diretivas" (E4) "(...) tem que perceber que tipo de certificações e que tipo de compliance é que são precisos para aquela área de negócio" (E8)	2

		Formação e consciencialização	E1 (comunicação pessoal) defende que onde a segurança se diferencia das restantes áreas é na necessidade de espalhar uma cultura de segurança pela organização "(…) esta aproximação (com as pessoas) é importante para depois conseguir coloca-los aqui neste barco para ver se eles aceitavam de uma forma mais simples e mais expedita essas alterações que vão surgindo. " (E5) "Nós uma coisa que fazemos é, todos os colaboradores que entram na nossa organização, na 1ª semana de entrada há uma série de formações que são dadas, e anteriormente não existia nenhuma componente de segurança, e agora já existe (…) esta mudança de cultura ajuda que as pessoas tenham mais sensibilidade perante estes temas."; "Hoje em dia a segurança técnica já não é suficiente, porque 80% ou mais dos ataques informáticos não são através da tecnologia, são através das pessoas. As pessoas são o elo mais fraco, posso ter 50 mil firewalls e antivírus instalados, mas se tenho uma pessoa que não tenha os cuidados básicos, não há firewall que resista a isto." (E6) "Tem que ser garantido que haver dentro das organizações que o grosso ou a grande maioria das pessoas têm conhecimentos básicos de segurança." (E7) "Há vários números, dependendo das fontes que queremos utilizar, mas de 70 a 80% dos incidentes de segurança há o elemento humano envolvido (...) a função de segurança de informação não pode ser responsabilidade de uns poucos, precisa de ser de todos os colaboradores." (E8) "Como eu costumo dizer, segurança é 100% formar pessoas."; "Faço uma iniciativa de consciencialização sempre quando entram novos estagiários" (E9)	6
		Auditoria	E1 (comunicação pessoal) defende que uma das áreas de intervenção do CISO é na auditoria periódica aos processos, riscos e controlos que se encontram sob a sua responsabilidade "Um CISO tem que ter (...) uma visão de auditoria, onde o CISO tem que demonstrar espírito crítico e independência de modo a ter uma visão global e detalhada sobre os reports e KPI's que lhe são disponibilizados por terceiros, sendo por vezes necessário que vá ele próprio validar que a informação que lhe está a ser disponibilizada, está de facto correta." (E3) "Tamos a trabalhar no sentido de fazemos auditorias regulares de segurança. Fizemos duas auditorias na perspetiva dos processos e aos sistemas." (E9)	3
		Gestão de utilizadores e acessos	E1 (comunicação pessoal) apresenta que a gestão de utilizadores e acessos é uma das suas responsabilidades como CISO E2 (comunicação pessoal) afirma que com as implicações do RGPD, uma das primeiras áreas de intervenção da equipa de segurança foi na análise e gestão de acessos	2

	Desafios	Impacto da segurança nas pessoas	E1 (contacto pessoal) defende que um dos desafios do CISO é a capacidade de tornar a segurança mais inteligente e menos intrusiva, mantendo a sua missão com menor impacto nas pessoas e na operação do negócio “Nós tínhamos esta questão do data loss (...) que tinha um down size muito grande para os utilizadores. Como nós não temos uma política de classificação de informação e não tínhamos a visão clara no passado do que era importante e do que realmente era confidencial na nossa casa e não poderia sair de forma alguma, fomos para o default: encripta-se tudo e não se permite nada. E daqui fazemos a ponte outra vez do que é prático para o utilizador e do que não é prático. Isto tem impacto para o utilizador que podia ser muito bem resolvido se tivermos uma visão critica do que fazemos cá dentro e de quais são os nossos processos, não nos limitando a ficar pela rama.” (E3) "O CISO que tem que tentar fazer uma aproximação do negócio, senão não consegue ir avante. Pode conseguir por imposição algumas coisas, as restantes não consegue. E é sempre importante levar as coisas a bem, porque mesmo com todos os controlos que existem, as pessoas continuam a ser a maior falha nos temas de segurança." (E5) "(...) eu nunca tive problemas em implementar coisas que não tivessem impacto nas pessoas (...)" (E9)	4
		Alinhar as pessoas com a estratégia de segurança	E1 (comunicação pessoal) refere que um dos grandes desafios da segurança é fazer com que esta seja vista de forma holística na organização “Quando o CISO quer tornar algo mais seguro, o primeiro obstáculo são as pessoas. Estas pessoas começam com a administração que são resistentes à segurança e a querer furar os controlos." (E5) "Gasta-se muito pouco em awareness interno, as pessoas têm muito pouca noção do que é a segurança e de quais os perigos que têm. Conhecem os básicos porque se falou muito, as questões do spam, do phishing, e mesmo assim continuamos a ter campanhas de phishing com grandes taxas de sucesso (para o volume que é expectável)." (E7) "É muito mais importante na minha perspetiva consciencializar os colaboradores, garantir que os colaboradores percebem o impacto das suas ações e o que está em jogo do que adicionar controlos aos colaboradores. Não quer dizer que não se faça, mas este mix tem que ter sempre presente a componente humana e a componente de awareness e training. É a partir da formação e do awareness que conseguimos que as pessoas tomem um comportamento diferente e suspeitem de alguma coisa que não suspeitariam antes, e que resistam a algumas pressões, inclusive pressões sociais."; "(...) o maior desafio que nós temos é a consciencialização e a passagem de conhecimentos de segurança, porque os sistemas de IT são diferentes dos restantes artefactos que as pessoas estão habituadas a usar.”" (E8) "Eu acho que os meus sistemas são relativamente seguros (…) mas os meus utilizadores é que não. Tenho utilizadores que são capazes de tudo."; "(...) o nosso problema não é orçamental, é cultural"; "Quando entram os estagiários eles já estão mais atentos a este tema, as dificuldades que eu tenho são com as pessoas que estão há mais tempo na organização" (E9)	5
		Resistência à mudança	"(…) As mudanças que a segurança pode trazer nem sempre são fáceis, uma vez que nas organizações existe sempre muita ‘luta de cadeiras’.” (E3) "Aqui as grandes dificuldades em termos de segurança é a resistência das pessoas, a resistência de terem que fazer o mesmo, de maneira diferente ou mais trabalhosa" (E9)	2

		Alinhar a segurança com o contexto organizacional	"Um CISO (…) tem que ter a visão mais lata, de como tudo se vai encaixar e que a segurança não é um objetivo a todo o custo – temos que equacionar os prós e os contras e o que realmente é importante e que não vai impedir o negócio" (E3) "(…) o que se vê em muitas empresas, é a implementação de dezenas de políticas que não têm aderência nenhuma à realidade." (E5) "Um dos desafios do CISO é perceber muito bem o negócio, perceber muito bem o panorama de ameaças, perceber o risco a que a organização está exposta e conseguir, em conjunto com a administração, entender qual é o sweet spot. Ou seja, quanto é que deve gastar em segurança (gastar, não é só investimento), que impacto a segurança deve ter no negócio, quer seja através de gastos diretos ou indiretos, para atingir aquele sweet spot que se considera que é o risco aceitável para fazer aquele negócio." (E8) "Na nossa organização não há uma liderança vincada, e isto cria muitas dificuldades quando queremos impor algumas regras." (E9)	4
		Impacto da segurança nas operações do negócio	E1 (contacto pessoal) defende que um dos desafios do CISO é a capacidade de tornar a segurança mais inteligente e menos intrusiva, mantendo a sua missão com menor impacto nas pessoas e na operação do negócio "A segurança normalmente tem (...) que a segurança e a agilidade normalmente não andam de mãos dadas. Quando se investe em segurança perde-se um bocado em flexibilidade e em rapidez, o que se tenta fazer é minimizar esse impacto e tentar explicar às pessoas que em termos de segurança esta resistência traz outros benefícios." (E6) "A segurança não é algo absoluto, é um compromisso face a um panorama de ameaças, à nossa perceção de risco, ao nosso apetite para o risco e às limitações que estamos dispostos a assumir no ponto de vista do nosso negócio, da nossa operação para ter um determinado nível de segurança. A segurança não é barata, e não é no sentido de comprar o IDS ou a firewall, não é pagar à pessoa que trata de segurança, é nós termos de fazer algumas coisas de forma diferente que vão ter impacto no negócio" (E8)	3
		Comunicar eficazmente à administração	E1 (comunicação pessoal) defende que um dos desafios do CISO é a capacidade de comunicar eficazmente os temas de segurança à gestão de topo "Maior parte das vezes tem-se um CISO porque fica bem no organigrama, os boards alocam mas não compreendem porque maior parte destes perfis vêm do IT e acabam por ter dificuldades de passar a mensagem para cima. " (E4) "O problema dos perfis técnicos é que identifica um problema, mas não sabe comunicar o porquê, quais as implicações, qual o custo associado, o que é preciso para resolver…" (E5) "Passar a mensagem à administração é complicado (…)" (E9)	4

		Conseguir investimentos numa área que não dá retornos financeiros diretos	"É muito difícil de vender segurança, porque tamos sempre a trabalhar sobre a previsão. Estar a meter o dinheiro num saco onde não se vê qualquer tipo de retorno é muito difícil. A mensagem que tem que ser passada é que o não investimento poderá ter um custo muito maior." (E4) "(...) depois temos a resistência da área produtiva, que diz que a segurança não é o que vende e não é o que dá dinheiro à empresa. Têm muito esta ideia, mas se o serviço for abaixo, não se vende nada." (E5) "É difícil fazer ver que o investimento em segurança é importante porque no fundo não estamos a criar nada, estamos a tentar evitar que haja alguma coisa." (E6) "(...) este custo acrescenta valor e acrescenta alguma vantagem competitiva em relação às concorrentes ou pelo menos em relação aos perigos que existem, é isto que temos que avaliar." (E7) "Em 2008 quando eu quis por todas as passwords a mudar regularmente e a terem requisitos de complexidade, foi logo recusado"; "A parte da segurança não tem uma rubrica específica no nosso orçamento, está dentro do chapéu do IT, ainda não há uma área específica. A parte mais difícil que eu tive em termos de aprovação foi a contratação de um recurso específico de segurança"; "Já tentei por a política de bloquear as portas USB de todos os devices, ou seja, só pens ou discos externos autorizados é que poderiam ser ligados naquelas portas USB, mas nunca consegui que essa questão fosse aprovada."; "Fizemos 2 auditorias na perspetiva dos processos e aos sistemas, nunca foi aprovado fazer um teste de intrusão"; "Uma das questões que tentei e nunca consegui, foi implementar uma certificação 27001" (E9)	5
		Investir em pessoas	"Os desafios é justificar recursos e a associação de recursos à área. Se investir em equipamentos é difícil, investir em recursos ainda mais." (E4) "A banca já começa a ter uma visão mais clara para os perigos de segurança, percebem os danos reputacionais, falta às vezes alguma sensibilidade para o investimento, nomeadamente em capital humano."; "Para mim o maior problema neste momento é que em termos de investimento e de compra de soluções há algum foco, mas há muito pouco foco no conhecimento e nas pessoas. " (E7)	2
Impacto regulamentar	Regulamento Geral de Proteção de Dados	Procura aproximar a maturidade da Europa com a dos EUA	"Se há uma coisa que o nosso RGPD nos traz é nos aproximar dos standards e do nível de maturidade que os EUA acrescentam. Existem regras e leis de privacidade nos EUA há mais de 10 anos ao nível de dados e dados pessoais." (E7)	1

		Elevou a awareness de segurança	E1 (comunicação pessoal) afirma que o Regulamento trouxe mais visibilidade à segurança na organização ao abordar temas que inicialmente nem eram considerados relevantes. E2 (comunicação pessoal) sente que passou a existir uma maior sensibilização para temas os temas de segurança, tanto por parte da administração como transversalmente por toda a organização, tendo esta consciencialização sido conseguida pela necessidade de alterar processos e procedimentos em várias direções da organização (principalmente a DRH) de modo a garantir conformidade com o Regulamento. "O RGPD ajudou muito ao nível de awareness e ao próprio nível de modelos de governo das organizações que estão neste momento a ser adaptados"; "O RGPD veio abrir a consciência a muitas organizações. Muitas delas mal aconselhadas, muito delas com erros de interpretação, mas pelo menos foi suficientemente concreto para alertar para várias questões"; "Para quem trabalha em segurança como eu o RGPD é algo libertador porque de facto vem abrir as mentes das pessoas e as pessoas percebem que isto não é apenas uma questão de se acontece ou não acontece, é mais uma questão cultural, é mais uma questão das próprias organizações entenderem." (E7) "O regulamento tem uma contribuição interessante, que é a contribuição de levar à administração o problema, porque de repente eles são criminalmente responsáveis e a organização é responsável e poderá ter coimas avultadas. O que coloca o tema nos conselhos de administração, e esta foi uma boa contribuição do regulamento." (E8)	4
		Em termos de segurança é um ponto de partida, mas não responde a todas as necessidades	"Eu costumo dizer isto sempre 'não olhem para isto apenas para os dados pessoais, a partir do momento em que eu estou preocupado em criar condições para proteger os dados pessoais, porque não também os dados de negócio? Aliás faz todo o sentido, se calhar para vocês uma multa de 20 milhões, que é a multa máxima que podem ter por causa de perda de dados pessoais, é muito má porque se calhar nunca pensaram quanto pode custar perderem o negócio todo'." (E7) " Através da privacidade chegámos ao tema da segurança, mas a segurança não chega só para a privacidade, e os conselhos de administração precisam de perceber isso." (E8)	2
		Potenciou a segurança nas organizações	E1 (comunicação pessoal) defende que o regulamento potenciou a exposição da segurança perante as administrações, nomeadamente dando mais força devido ao seu cariz obrigatório E2 (comunicação pessoal) sente a consciencialização ganha para os temas de segurança derivados do regulamento aumentaram a sua força na sua organização, levando a que fosse feito um investimento em constituir uma equipa de segurança e em começar a planear investimentos em segurança no orçamento anual da DSI. "O RGPD foi bom para potenciar o que é a segurança, eu costumo dizer aqui, inclusivamente ao meu conselho de administração que existe segurança sem privacidade, mas não existe privacidade sem segurança." (E4) "Com o RGPD houve uma melhoria grande em termos de empowerment de segurança (...)" (E5)	4
		As organizações têm estado a delegar DPO's com *background* em direito	Na organização de E1 (comunicação pessoal) a função de DPO é executada por um gabinete de advogados. "Na minha opinião, ao inicio o DPO devia ser alguém de direito, e quando a coisa está a funcionar trabalhar em conjunto com a segurança e como equipa." (E4) "Eu sou apologista que um DPO não deve ser um advogado, mas é o que eu tenho estado a ver mais." (E8) "Temos um DPO, um jurista (…)" (E9)	4

		Foi delegado um DPO com *background* em segurança	"O nosso DPO veio da minha área, era CISO noutra organização." (E3)	1
		O RGPD não teve impacto na segurança da organização	"Nós temos uma dificuldade quanto ao RGPD. Os advogados têm um estatuto na ordem de advogados que têm um artigo que diz que há sigilo profissional por parte do advogado, que tem que ser respeitado. (…) E a visão é que o sigilo profissional se sobrepõe ao RGPD." (E9)	1
		O DPO não trabalha em conjunto com a segurança	"Temos um DPO (…) que não trabalha connosco." (E9)	1
		Independentemente do seu perfil, o DPO deve trabalhar em conjunto com a segurança	Na organização de E1 (comunicação pessoal) a função de DPO é executada por um gabinete de advogados, que, no entanto, trabalha em conjunto com o CISO "O nosso DPO veio da minha área, era CISO noutra organização. Tivemos que trabalhar com advogados para trabalhar a parte de direito (...) Estamos confortáveis com a maneira que estamos a fazer as coisas" (E3) "Na minha opinião, ao inicio o DPO devia ser alguém de direito, e quando a coisa está a funcionar trabalhar em conjunto com a segurança e como equipa." (E4) "Um DPO até pode ser um advogado, mas não pode ser só um officer, tem que ser um office, tem que ter pessoas dentro do gabinete dele com estes conhecimentos e que sejam isentas, e o CISO acaba muito também por ser isto" (E7)	4
	Network and Information Security (NIS)	Impacto pouco abrangente face às necessidades do país	"O NIS é para prestadores de serviços essenciais, o que causa que tenha um impacto muito menos generalizado na sociedade." (E8)	1
		Atualmente ainda tem pouca visibilidade	"O RGPD abafou o tema do NIS (…) " (E5)	1
		Em termos de segurança é mais importante/urgente que o RGPD	"Em termos de segurança e em termos das grandes organizações no nosso país, eu acho que o NIS vai ser muito mais importante do que o RGPD neste sentido, em termos de segurança específico." (E7) "Eu acho que o NIS era mais urgente que o regulamento, ou que esta versão do regulamento (…) A NIS era urgentíssima, principalmente porque a maior parte dos fornecedores de serviços essenciais são estatais ou com algum controlo do estado." (E8)	2
		Poderá ajudar a aumentar a cultura de segurança em Portugal	"Por isso eu acho que a Diretiva NIS foi muito importante para obrigar o estado enquanto operadora de serviços essenciais a tomar algum tipo de cuidados que não iria tomar porque não tem recursos e porque não estava na prioridade, e agora terá que ser uma prioridade." (E8)	1

		É desejado que seja um complemento ao RGPD	"A minha expectativa perante o NIS é que complemente o RGPD, porque tem uma vertente ligeira de direito e muito forte de segurança." (E5)	1
	Cybersecurity Disclosure Act de 2017	É uma iniciativa positiva e que deveria ser seguida em Portugal e pela Europa	E1 (comunicação pessoal) acha que a imposição de algo semelhante na europa teria um impacto bastante útil e positivo “Faz sentido, mas lá está, em Portugal avança-se pouco (…)” (E3) “Acho que na Europa ainda temos uma maturidade muito pequena relativamente a esse tema, apenas temos guias. Mas acho que deve ser este o caminho.” (E4) “Eu diria que sim, faz sentido (…) é sem dúvida fundamental, mas não serve ter lá uma pessoa que não sabe o que está lá a fazer.” (E5) "Neste tipo de coisas os EUA costumam estar muito à frente de nós e acho que algo assim (imposição de conhecimentos de segurança de informação nos boards) deve ser fundamental." (E7)	5
		Haver alguém com conhecimentos de segurança nos conselhos de administração é uma necessidade, mas esta alocação tem que ser sustentada	"Sem dúvida que o CISO tem que existir, tem que ser a pessoa certa e tem que ter um report na administração. Mas isto para mim é um não controlo ter uma pessoa lá que não saiba do que está a falar. O que pode acontecer é agarrarem num administrador e passar a ser também o CISO." (E5) "Não é como por exemplo numa empresa (...) que nomeou um CISO quando uma das pessoas do conselho de administração saiu para ir fumar e ficou aquele. De segurança percebe zero e ficou nomeado porque os outros acharam que tinham que ter um CISO nomeado, porque faz parte das regras e o próprio regulador da área de atividade obriga a ter um CISO e ficou aquele. Não pode ser assim." (E7)	2
		Já existem entidades reguladoras que recomendam a consciencialização dos riscos de segurança por parte dos conselhos de administração	"Algumas das empresas supervisionadas por nós são obrigadas a comunicar-nos todos os incidentes que possam de alguma forma meter em causa a continuidade das operações das organizações. Nós quando fazemos estes trabalhos de supervisão, a nossa preocupação inicial é saber se o board tem conhecimentos e consciencialização para os riscos de cibersegurança e de segurança de informação. Não havendo conhecimento deixamos uma recomendação forte e dizemos que todas as frameworks e boas práticas apontam para isso. E no fim ainda dizemos que eles são responsáveis por qualquer risco, isto não é apenas porque são boas práticas, a justificação é mesmo essa, é que ao final do dia aquilo pode por em risco a organização, toda a operacionalização da empresa e no limite esta poderá falir.” (E4)	1
		Existe o trabalho de criar esta visão na Banca	“(…) de que forma é que isto está a ser endereçado atualmente, existe uma entidade que regula o setor bancário e depois existe uma associação portuguesa de bancos (…) é um tema que já veio à baila e já se tem uma ideia de que forma isto poderá ser alavancado (…) vamos ter que propor um caminho de ação ao Banco de Portugal e mostramos a estratégia e mostramos o objetivo e o Banco de Portugal fica confortável o suficiente para depois transcrever para decreto (…)” (E3)	1

		Tem que haver conhecimento e sensibilidade para os temas de segurança por parte da administração, mas ao nível adequado	“Tem que haver sem dúvida uma sensibilidade por parte dos conselhos de administração para o tema da segurança, aqui na nossa organização felizmente existe, mas lá está, tem que ser um conhecimento. Acho que não têm que ter conhecimento técnico nem de alto nem de baixo nível, agora sim, tem que haver uma consciencialização que o tema da cibersegurança é um tema importante, tem que haver, e no nosso caso existe, um mapeamento dos riscos da empresa, e o risco da cibersegurança está sempre lá em cima. Portanto, acho que sim, acho que tem que haver sem dúvida uma sensibilização por parte da administração para os temas da cibersegurança, mas ao nível adequado.” (E6)	1
	Desafios da regulamentação	Fiscalização e auditoria	"(...) o meu receio é que como isto não está linkado com nenhum processo, testou-se uma vez e ficou resolvido.” (E5) "Podíamos estar a pensar no que podemos fazer, mas a questão é que nós sabemos o que podemos fazer e temos uma estratégia de onde queremos chegar todos, mas não temos forma de garantir que alguém vai ser o sponsor disto. Podes ter um RGPD, podes ter um NIS, mas se ninguém fiscaliza e se ninguém faz o trabalho de garantir que está tudo a ser bem feito, vai ter que ser o cidadão, mas o cidadão se o cidadão se queixa e depois não existe consequências, o cidadão vai acabar por desistir." (E7) "Não podíamos continuar no estado em que estávamos com a anterior Diretiva (de proteção de dados), em que as comissões nacionais de proteção de dados ou equivalentes não tinham capacidade nenhuma para intervir (...) por isso na realidade a fiscalização era insuficiente. Eu espero que o regulamento ajude." (E8)	3
		Falta de compromisso do estado	“(...) nós tivemos foi um problema muito grave em termos de RGPD no nosso país que foi, infelizmente, o péssimo trabalho que o governo fez sobre o tema do RGPD, nomeadamente na administração pública, que veio inquinar o processo, veio mais uma vez criar mais uma assimetria de o que são as exigências de uns e das exigências de outros, portanto, o estado português fez um péssimo trabalho ao país todo em relação a estes temas. Criou-se mais um conjunto de pedras numa engrenagem que estava a começar a funcionar, muito com base no medo, é verdade, mas às vezes as grandes transformações e as grandes mudanças culturais acontecem com base no medo. E isto vem atrasar um bocado estes processos e nós sentimos isso, nós temos sentido que há organizações que afrouxaram o esforço que andaram a fazer.” (E7) “(...) cerca 60% dos dados pessoais, do manuseamento e tratamento dos dados pessoais na vida das pessoas passa pela administração pública, que está excluída do processo.” (E9)	2