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

Isadora Rodrigues Costa Lima

A Segurança da Informação no Contexto das Sociedades de Revisores Oficiais de Contas Portuguesas

Coimbra, outubro de 2019.

A Segurança da Informação no Contexto das Sociedade de Revisores Oficiais de Contas Portuguesas
Isadora Rodrigues Costa Lima
ISCAC | 2019

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

Isadora Rodrigues Costa Lima

A Segurança da Informação no Contexto das Sociedades de Revisores Oficiais de Contas Portuguesas

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Auditoria Empresarial e Pública**, realizada sob a orientação da Doutora Isabel Maria Mendes Pedrosa, Professora Adjunta.

Coimbra, outubro de 2019

TERMO DE RESPONSABILIDADE

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

"Once you get the data and you've got the technology, boy, you are in a powerful place!"

Graeme Yorston – Former CEO of Principality Building Society

Aos meus pais.

Sem o vosso apoio eu nem teria começado esta jornada.

AGRADECIMENTOS

No decorrer deste percurso, tive o gosto de conhecer e de estar com pessoas que impactaram positivamente a minha vida e ajudaram a amenizar as dores de estar longe de casa. Tive o apoio de muitos, e deixo aqui a minha gratidão a todos:

Agradeço em primeiro lugar aos meus pais e avós, por estarem sempre presentes (mesmo que pelo WhatsApp ou FaceTime) e me apoiarem em cada decisão que tomei nesta vida, sem vossa compreensão e apoio eu nem teria começado. Ao Gustavo, pela paciência e compreensão, por todas as boleias às sextas às 23h e aos sábados às 8h30 da manhã. À Margarida, pela hospedagem. À avó Lena, pelos almoços e pelas conversas. Ao "tio" Paulito pela boa companhia e pelos passeios. À minha família do Porto: Isabella e João, por toda a dedicação em ajudar-me quando preciso; Marco e Génesis (tens sempre um lugar sob o nosso teto) por terem sempre uma palavra amiga e serem sempre boas companhias.

Agradeço também à minha querida e "super-orientadora" Professora Isabel Pedrosa pelo acompanhamento incrível, pelas críticas, sugestões, pela paciência e principalmente por todas as horas dedicadas ajudar-me com este estudo. Agradeço ao Professor Raul Laureano pela abertura e disponibilidade para colaborar com este trabalho.

Ainda, não posso esquecer-me de todos os meus colegas do MAEP, em especial, às amigas que fiz e que quero levar para a vida: Joana Andrino (minha fiel companheira em todos os trabalhos, do início ao fim), Filipa Aguiar, Joana Amorim e Margarida Costa. Com vocês os trimestres pareceram ser bem mais fáceis e passaram rápido demais. Já tenho saudades da vossa companhia em sala de aula.

Por último, agradeço a todos que dedicaram tempo em participar do inquérito aplicado, representando e garantindo resultados a este trabalho.

RESUMO

Existem, na literatura portuguesa e internacional, estudos que abordam a temática do uso da Tecnologia da Informação (TI) no contexto da realização de trabalhos de auditores financeiros. Muitos procuraram melhorar a forma como estes profissionais utilizam as TI de forma a facilitar e gerar maior eficiência no trabalho realizado, bem como perceber as suas motivações para o uso da tecnologia com base na recomendação de organismos e entidades reguladoras. No entanto, nenhum estudo ainda havia sido realizado no sentido de aprofundar o conhecimento das atuais Políticas de Segurança da Informação (PSIs) adotadas pelas SROCs, no contexto da realização do trabalho destes profissionais, nem sobre aspetos relacionados com cibersegurança.

Sendo a informação gerada pelos clientes das SROCs um dos principais objetos de trabalho do auditor financeiro, é importante que existam PSIs eficientes, dada a confidencialidade e sigilo necessário no seu tratamento. A troca de informação através da Internet é, também, um aspeto relevante nesta temática. A literatura sobre o assunto apresenta os principais aspetos das PSIs que auxiliam na gestão das organizações. Estão também disponíveis relatórios sobre o atual estado da cibersegurança, bem como as principais ameaças para os próximos anos e como combatê-las.

O presente estudo, portanto, aborda esta importante questão através da aplicação de um inquérito, através de questionário online, a profissionais que atuam com auditoria financeira em Portugal, de modo a colmatar esta lacuna temática que, com base em dados obtidos, buscou cumprir objetivos definidos através da avaliação do atual cenário das SROCs no âmbito das PSIs aplicadas, independente da dimensão das organizações.

Esta dissertação apresenta contribuições significativas com impactos para obtenção de dados importantes acerca do atual contexto da Segurança da Informação no âmbito dos profissionais que atuam diretamente com auditoria financeira em Portugal: principais políticas adotadas relacionadas com o uso de tecnologia, perspetivas para atualização e melhoria nas políticas de segurança, relação entre dimensão da SROC e suas PSIs.

Palavras-chave: Auditoria, Segurança da Informação, Cibersegurança, Políticas da Segurança da Informação; Auditoria Financeira; Revisores Oficiais de Contas, Sociedades de Revisores Oficiais de Contas, SROCs.

ABSTRACT

There are, in Portuguese and international literature, studies on the research topic of the use of Information Technology (IT) in the context of financial auditors. Many have sought to improve the way these professionals use IT to facilitate, generate greater work efficiency and motivations for technology use based on the recommendation of regulatory bodies and entities. However, no study has yet been conducted to deepen the knowledge of the Information Security Policies (PSIs) adopted by the auditors' firms in Portugal, known as "SROCs", without the context of professional work and quality assurance.

Since clients' information used by SROCs is one of the main work objects for the auditors, it is important to have efficient information security policies, given the confidentiality required in information treatment. The exchange and sharing of information through the Internet are also part of this theme. The literature on this subject presents the main aspects of PSIs that help in the management of organizations. Reports are also available on the current state of cybersecurity, as well as the main threats for the coming years and how to combat them.

The present study, therefore, addresses this important question by using the application of an online questionnaire, aimed at financial audit professionals in Portugal, to fill this thematic gap. Based on the collected data, it will be possible to assess the current scenario of the SROCs within the scope of the applied PSIs regardless of the size of the organizations.

This dissertation presents contributions applied with the impact to important data about the current context of Information Security in the scope of professionals who work directly with financial audits in Portugal: main policies adopted related to the use of technology, perspectives for updates and improvement in information security policies, and the relation between dimension of the SROCs and its PSIs.

Keywords: Audit, Information Security, Cybersecurity, Information Security Policies, Financial Audit, Statutory Auditors, Statutory Auditors' Firms.

ÍNDICE GERAL

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

AICPA – *American Institute of CPAs*

ACL – *Audit Command Language*

CAATT – *Computer-assisted Audit Tools and Techniques*

CAQ – *Center Audit Quality*

CEAOB – *Comittee of European Auditing Oversight Bodies*

CISA – *Certified Information Systems Auditor*

CLC – Certificação Legal das Contas

CMVM – Comissão do Mercado de Valores Mobiliários

COBIT – *Control Objectives for Information and Related Technology*

COSO – *Committee of Sponsoring Organisations*

CPA – *Certified Public Accountants*

CSC – Código das Sociedades Comerciais

DDoS – *Distribute Denial of Service*

DoS – *Denial of Service*

DS – *Deliver and Support*

DSS – *Deliver, Service, Support*

EFRAG – *European financial Reporting Advisory Group*

IAASB – *International Auditing and Assurance Standards Boards*

IDEA – *Interactive Data Extraction and Analysis*

IoT – *Internet of Things*

ISA – *International Standards on auditing*ISACA - *Information Systems Audit and Control Association*

ISO – *International Organization for Standarization*

ITGC – *Information Tecnology General Controls*

OROC – Ordem dos Revisores Oficiais de Contas

PCAOB – *Public Company Accounting Oversight Board*

PSI – Política de Segurança da Informação

ROC – Revisor Oficial de Contas

SGSI – Sistema de Gestão de Segurança da Informação

SI – Segurança da Informação

SOX – Lei Sarbanes Oxley / SOA – *Sarbanes Oxley Act*

SPSS – *Statistical Package for the Social Sciences*

SROC – Sociedade de Revisores Oficiais de Contas

TI – Tecnologia da Informação

VPN – *Virtual Private Network*

INTRODUÇÃO

No âmbito do processo de globalização, que tomou força no século XX e foi responsável pela necessidade de harmonização de conceitos, princípios e práticas contabilísticas, o desenvolvimento de um bom sistema de gestão de informação bem como adoção de políticas de segurança de informação revelam-se de extrema importância para o bom funcionamento das organizações, independente do setor em que operam, devido ao aumento do fluxo informacional consequente desta globalização. Dessa maneira, é preocupação comum de todas empresas a segurança da informação gerada, por ser a base de qualquer tipo de negócio. De acordo com Luz (2010) a qualidade das informações e amplitude de conhecimentos pessoais e organizacionais são decisivos no futuro dos negócios das organizações.

No que diz respeito às Sociedades de Revisores Oficiais de Contas (SROC), o assunto não é diferente e acaba por se tornar ainda mais delicado visto que os profissionais desta área trabalham, muitas vezes, com informação confidencial e sigilosa de seus clientes, uma vez que entram em causa reputação das organizações bem como consequências através de multas e sansões de órgãos reguladores. Para garantir que todo o conteúdo informacional gerado e adquirido dentro das organizações se encontra protegido de diversos tipos de ataques e que seus sistemas de informação estão em conformidade com as normas existentes, os Revisores Oficiais de Contas (ROCs) investem numa série de procedimentos que vão desde tecnologias de informação e mecanismos de segurança até formação específica na área da segurança da informação. Os Revisores levam em consideração inovações tecnológicas nas organizações para adaptarem os seus controlos e metodologias de trabalho à necessidade de proteger todo fluxo e conteúdo informacional.

Em Portugal ainda nenhum estudo havia sido realizado no âmbito de conhecer as atuais Políticas de Segurança da Informação adotadas pelas SROCs no contexto da realização de trabalho destes profissionais.

1.1 Objetivos da Pesquisa

Este trabalho tem como objetivos gerais:

- Avaliar o atual cenário das SROCs no que diz respeito às políticas e ferramentas de segurança aplicadas, independentemente de suas dimensões (*big four* ou não),

que estão vinculados ao processamento eletrónico da informação dos seus clientes (e até mesmo das próprias organizações), de maneira a garantir a segurança necessária e a mínima exposição ao risco;

- Verificar e relacionar as atuais preocupações e perspetivas futuras para atualização das mesmas bem como implementação de novas Políticas de Segurança da Informação (PSIs), conforme a necessidade da organização, em um curto prazo;

De maneira a complementar o estudo, como objetivos específicos, pretende-se:

- Identificar as práticas utilizadas no atual contexto de segurança da informação, ou seja, na operação dos sistemas de informação das organizações, além de evidenciar os aspetos positivos consequentes da implementação da gestão de segurança da informação dentro das organizações;
- Relacionar as práticas e políticas de segurança adotadas nas SROCs com suas dimensões;
- Averiguar tipos de tecnologias utilizadas pelas organizações no que diz respeito às Políticas de Segurança da Informação (PSIs).

Esta dissertação deverá permitir, como resultado, uma reflexão sobre a atual prática e situação da Segurança da Informação dentro das organizações do tipo SROCs em Portugal, inclusive no que diz respeito a cibersegurança, bem como implementação de novas práticas de acordo com a realidade das organizações.

O presente estudo, portanto, aborda esta importante questão através da aplicação de um inquérito através de questionário *online* de modo a colmatar esta lacuna temática através de uma pesquisa descritiva e a cumprir os principais objetivos definidos no próximo subcapítulo. O inquérito foi aplicado a profissionais que atuam diretamente com auditoria financeira (ROCs ou não) de maneira a obter maiores informações acerca das políticas de segurança da informação no contexto das organizações onde desempenham suas atividades.

1.2 Justificação do estudo e principais resultados esperados

No contexto atual e informacional quantidade de dados gerados pelas organizações dentro e fora de Portugal, onde o conceito de Segurança da Informação (e Regulamento Geral de Proteção de Dados, RGPD) estão em voga, existem imensas reflexões a serem feitas

sobre a atual situação das PSIs dentro dessas organizações. Desta forma, este estudo é justificado pelos seus principais objetivos diante da importância deste assunto.

Sendo a abordagem principal deste estudo um tema de extrema importância para o cotidiano de Sociedades de Revisores Oficiais de Conta em Portugal, no sentido de discutir as principais Políticas de Segurança da Informação adotadas por estes tipos de organizações e o entendimento que seus colaboradores possuem sobre as mesmas, o resultado deste estudo por si só acaba por se tornar um grande contributo para o tema em Portugal.

1.3 Estrutura do trabalho

Este estudo está estruturado de maneira a introduzir o tema através de cinco capítulos:

- Este primeiro capítulo corresponde à introdução ao tema e contextualização dos restantes capítulos;

- No segundo capítulo será feita uma abrangente revisão de literatura de maneira a contextualizar aspetos da origem da contabilidade, evoluindo para a profissão de auditor financeiro e atual realidade da Segurança da Informação, bem como expor conceitos a partir de definições e perspetivas de investigações realizadas nesta área.

- O terceiro capítulo trata sobre a metodologia de trabalho e elaboração do inquérito aplicado e a pesquisa propriamente dita.

- No quarto capítulo serão discutidos analisados os resultados obtidos através da aplicação do inquérito elaborado, bem como apresentado um quadro com sugestões de PSIs para SROCs.

- Por fim, no capítulo quinto, será apresentada a conclusão com discussão sobre implicações, dificuldades do estudo e oportunidades para pesquisas futuras.

2 Revisão da Literatura

Este capítulo é composto pelos principais assuntos vinculados ao trabalho efetuado, de maneira a compor bases literárias que proporcionem possibilidades de análises e reflexões diante das informações coletadas e abordadas.

De início comenta-se sobre a origem da contabilidade como é conhecida atualmente, o surgimento da auditoria financeira e a atual profissão de Revisor Oficial de Contas, dando destaque às informações por ele utilizadas e principais características de seu trabalho. De seguida procura-se apresentar definições sobre a segurança da informação e conceitos acerca do processamento de informações, políticas de segurança da informação e tecnologia de sistemas de informação. Por último será abordado o tema da Segurança da Informação no âmbito das SROCs.

2.1 A contabilidade

2.1.1 A Origem da Contabilidade

O método das partidas dobradas começou a surgir gradativamente nos séculos XIII e XIV em diversos centros de comércio ao norte de Itália, época da Renascença, tendo sofrido várias alterações efetuadas por diversos povos no decorrer dos anos, entre eles, os árabes (Hendriksen & Van Breda, 1999). A medida que o comércio mundial se expandia, fazia cada vez mais sentido manter a documentação sobre o que era negociado: o que eram posses de negociantes (ativos e capital), responsabilidades (passivos) e as noções de contabilidade como é conhecido hoje, se formava.

Já com influência da Revolução Industrial começaram a surgir os primeiros profissionais (ou especialistas, por assim dizer) em contabilidade no Reino Unido e Estados Unidos. Por volta de finais do ano 1890 surgiram organizações que certificavam profissionais da contabilidade pública (*Certified Public Accountants* – CPA).

De acordo com Iudícibus (1995) a contabilidade pode ser definida como um sistema de informação e avaliação que se destina a prover seus utilizadores (*stakeholders*) com demonstrações e análises de natureza económica, financeira, com relação à organização objeto de contabilização. Atualmente, o objetivo da contabilidade permanece inalterado já que fornece informações diferentes para cada usuário de acordo com suas necessidades.

As mudanças, no entanto, verificaram-se nos tipos de utilizadores e formas de divulgação de informação que têm sido demandadas (Iudícibus, 1995).

De maneira geral, a função da contabilidade é produzir informações relevantes e fidedignas que sejam importantes a órgãos de gestão, executivos, utilizadores diversos e organizações que sirvam de base para que possam influenciar tomadas de decisões em relação ao negócio em questão de maneira a alcançar objetivos planeados para a gestão de uma organização.

Com objetivo de garantir maior segurança no âmbito da divulgação de informações pela contabilidade, é preciso que os profissionais sigam Princípios Contabilísticos determinados pela Estrutura Conceptual.

2.1.2 A contabilidade no atual contexto profissional

Diante do atual crescente fluxo de informação que gira em torno da contabilidade, é evidente a influência tecnológica no contexto do profissional da contabilidade. O manual de escrituração contabilística foi substituído de papéis para formato eletrónico, a contabilização dentro das organizações passou a ser realizada através de sistemas eletrónicos graças ás Tecnologias da Informação, mesmo sem que a essência de débitos e créditos seja alterada. É possível perceber, portanto, que a dependência das organizações e de seus profissionais quanto à tecnologia é cada vez maior.

De acordo Luz (2010) as mudanças que ocorreram devido a adoção da tecnologia na profissão da contabilidade permitiram uma reformulação do papel de contabilista de maneira a resgatar seu valor intelectual no que diz respeito a privilegiar outras áreas de atuação profissional tais como *controller*, gestor e auditor financeiro (ou revisor), todas elas de enorme importância no âmbito da divulgação de informações e que envolvem o ambiente organizacional.

2.2 A auditoria Financeira

A auditoria surge como uma atividade de controlo económico-financeiro ao mesmo tempo em que a propriedade dos recursos financeiros deixou de estar sob cuidado de um só conjunto de pessoas (Almeida, 2004), já sendo utilizada por civilizações antigas como forma de controlo dos oficiais aos quais eram confiados os dinheiros públicos. Existem, atualmente diversos tipos de auditorias, sendo exemplos: auditoria interna, forense, operacional, de gestão, prospetiva e estratégica, qualidade, sistemas, entre outras. Para o

contexto da pesquisa, será tratado apenas o conceito da auditoria financeira propriamente dita.

Até o ano de 1884, segundo Almeida (2014), a deteção de fraude era aceite como o principal objetivo da realização de auditoria e, durante este período, era requerido aos auditores que conduzissem trabalhos de auditoria com razoável destreza e cuidado de maneira a procurar a existência de fraudes. Posteriormente, normas de auditoria passaram a dar suporte aos profissionais de maneira a garantir que o seu trabalho fosse assegurar e garantir (*assurance)* a credibilidade dos relatórios emitidos pela gestão de uma organização. Por outro lado, a responsabilidade de prevenção e deteção de fraude seriam dos órgãos de gestão, através da implementação do controlo interno. De acordo com Luz (2010), a Revolução Industrial também foi ponto relevante no processo evolutivo da auditoria, de maneira a proporcionar surgimento de organizações de maior porte e com estruturas complexas que requeriam procedimentos de controlo mais rigorosos com objetivo principal de proteger seus ativos e confiabilidade de informação.

Assim, Almeida (2014) define auditoria financeira como:

"*Um processo* ***objetivo e sistemático****, efetuado por um* ***terceiro independente, de obtenção e avaliação de prova*** *em relação às* ***asserções*** *sobre ações e eventos económicos, para verificar o grau de correspondência entre essas asserções e os* ***critérios estabelecidos, comunicando os resultados*** *aos utilizadores da informação financeira*". (Almeida 2014, p. 3)

2.2.1 O atual contexto da auditoria financeira

Já no início do século XXI mais mudanças ocorreram no contexto da auditoria. Devido a uma série de acontecimentos que acabaram por quebrar a confiança do Mercado de Capitais: com a falência de inúmeras e gigantes organizações, entre elas Enron e WorldCom (ambas no início dos anos 2000), o Governo Norte-americano implementou a Lei Sarbanes Oxley Act ou simplesmente "SOX" ou "SOA" e um organismo de supervisão com responsabilidade de criação de normas de auditoria, o PCAOB (*Public Company Accounting Oversight Board).*

Acreditava-se que a Enron, líder em distribuição de energia, era uma das empresas mais sólidas financeiramente dos EUA. A gestão da organização cometeu fraude: manipulava seus balanços e escondia dívidas por anos, inflacionando artificialmente seus lucros com ajuda de subsidiárias, bancos e até mesmo de seus auditores financeiros (na época, a

Arthur Andersen, que colapsou em seguida). Já a WorldCom era responsável pela distribuição de serviços de telefonia e internet, efetuava interpretações incorretas sobre as normas contabilísticas de maneira que pudesse maximizar seus ganhos financeiros (Brickey 2003, Bonotto 2010).

A SOA, portanto, reforça necessidade de independência e discernimento crítico entre os profissionais de auditoria e as organizações para que prestam serviços, de maneira a tornar ilegal um leque de diversos serviços "extra auditoria" que antes eram prestados de maneira deliberada. Apesar da SOA apenas ser aplicada às empresas públicas, o impacto que teve na profissão de auditor financeiro foi importante: a profissão de ROC passou de uma fase de autorregulação para regulamentação e supervisão exercidas por organismos quasi-governamentais (Almeida 2014, p. 3). Surgiram posteriormente outros órgãos como IAASB (*International Auditing and Assurance Standards Boards),* CEAOB (*Comittee of European Auditing Oversight Bodies)* e EFRAG *European financial Reporting Advisory Group)* também com impacto na profissão de auditoria. A independência, para a profissão de ROC é uma das características mais importantes, sendo citadas tanto no Código de Ética da Ordem dos Revisores Oficiais de Contas, OROC (no Capítulo 4 – Independência) como no Código das Sociedades Comerciais (CSC), no que diz respeito à profissão em Portugal. Já a nível Europeu, a Diretiva 2014/56/EU e Regulamento (UE) n. °537/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos requisitos específicos para a revisão legal de contas das entidades de interesse público impõe a obrigatoriedade de "rotação" de empresas de auditoria dentro das organizações (de caráter público) no sentido de gerar maior independência entre os profissionais. A fiscalização do cumprimento da Diretiva cabe à Comissão do Mercado de Valores Mobiliários (CMVM).

O quadro abaixo indica a existência de dois tipos de independência relacionadas a profissão de ROC.

Tabela 1: Independência na profissão de ROC

	Independência de Facto	**Independência Aparente**
Característica	Independência como se conhece de facto. Inexistência de conflitos de interesses: não depender de qualquer forma ("*state of mind")*	Independência para terceiros. Maneira de se evitar situações onde se possam gerar dúvidas aparentes. Exemplo: familiares a trabalhar em altos cargos nas organizações onde o ROC está a atuar

Fonte: Elaboração Própria

Estes dois tipos de independência estão diretamente relacionados com a profissão de ROC. Atualmente, caso sejam identificados motivos para os quais a independência de um profissional esteja comprometida, muito possivelmente poderá ocorrer existência de conflito de interesses. Deste modo, tendo em vista a cumprir as normas internacionais para realização de trabalhos de auditoria, os profissionais devem declarar-se independentes das organizações para as quais irão prestar serviços.

2.2.2 Objetivos da Auditoria financeira

A principal finalidade de uma auditoria financeira é certificar que uma organização está a divulgar informações reais nas suas demonstrações financeiras, bem como que está a cumprir regras do Código das Sociedades Comerciais, CSC, e a aplicar corretamente as Normas Contabilísticas de acordo com a base de apresentação de suas contas. Os ROCs verificam, também, se estão a divulgar informações fidedignas que sejam relevantes aos seus utilizadores. Para tal cumprem uma série de procedimentos que vão desde a avaliação dos controlos internos e riscos de uma organização, aos testes de detalhes que consistem na observação, coleta de provas de auditoria, confirmações e entrevistas com colaboradores da organização a ser auditada de maneira a validar todas as asserções definidas previamente. Ao concluir o trabalho, o ROC deve ser capaz de emitir uma opinião acerca das contas de seu cliente através da Certificação Legal das Contas, CLC, e Relatório de Auditoria.

2.2.3 Auditoria no atual contexto da Tecnologia da Informação

O atual cenário económico sofreu transformações provocadas pela imensa variedade de inovações tecnológicas disponibilizadas num curto espaço de tempo. O mercado da auditoria financeira tornou-se mais competitivo em todo o mundo e, devido a importância da segurança da informação, o que proporcionou novos desafios para os ROC. De acordo com Padoveze (2002,) as novas tecnologias como utilização de ficheiros em Excel e processamento distribuído em sistemas não afetam o objetivo das auditorias propriamente ditas, contudo, influenciam em grande parte do processo do tratamento e utilização da informação. Ainda, é possível dizer que a troca e criação de informação através da Internet também tem parte nisso. Resumidamente, o fluxo de informação – principal ferramenta de trabalho de um auditor – é mais intenso e rápido hoje em dia.

Atualmente os auditores utilizam tecnologias da informação de modo a realizar tarefas que facilitam o trabalho que realizam o qual, anteriormente, iria requerer trabalho manual

(Dias, 2000) e, dessa maneira, a utilização de instrumentos informatizados torna-se essencial para o processo de auditoria, chegando a ser indispensável para o desempenho da profissão de auditor financeiro. Um exemplo da utilização da tecnologia da informação na auditoria é o cálculo do tamanho de uma seleção por amostragem através de uma dada população, materialidade e outras características definidas previamente, no momento da aplicação de uma abordagem substantiva em análises através de testes de detalhe (Guy, Carmichael e Whitttington, 2001) (Blanch, 2000). Segundo Almeida (2013), em uma abordagem substantiva, os auditores devem definir os objetivos da auditoria, as distorções (ou erros) considerados toleráveis, a população de onde será extraída a amostra e, posteriormente, a técnica de amostragem mais apropriada bem como a dimensão da amostra. Plataformas como o SIPTA (Sistema Informático de Papéis de Trabalho de Auditoria) permite realizar a gestão da informação no decorrer dos trabalhos de auditoria e auxiliar com melhores abordagens no momento da definição de testes, seleção de amostra de acordo com as características dos dados (Baptista, 2017).

Não obstante da utilização da tecnologia de informação para realização de tarefas automatizadas, o uso das mesmas vai mais além: segundo Gusmão (2017), os sistemas de informação estão relacionados aos processos de gestão e estratégico das organizações e muitas vezes produz informações vitais para as organizações.

O estudo de Pedrosa (2015) possui grande relevância no sentido em que foi capaz de identificar as principais ferramentas de TI utilizadas pelos auditores financeiros, bem como identificar os principais fatores que fazem com que os profissionais utilizem CAATTs (*Computer-assisted Audit Tools and Techniques*) na resolução de seus trabalhos.

As CAATTs são ferramentas que auxiliam o trabalho de auditoria, como o próprio nome em inglês, em tradução livre: "técnicas de auditoria auxiliadas por computadores"; segundo o ISACA, a associação internacional que suporta e patrocina o desenvolvimento de metodologias no âmbito das atividades de auditoria e controlo e em sistemas da informação, são:

"Any automated audit technique, such as Generalized Audit Software (GAS), test data generators, computerized audit programs and specialized audit utilities" (CISA Review Manual 2013, 2012, pp . 389)

O termo "*Generalized Audit Software*" é utilizado em Lovata (1990) e refere-se a

"*todas as ferramentas que podem ser usadas para executar todos os testes possíveis numa (ou mais) áreas funcionais*".

(Lovata, 1990, pp . 60)

Assim, desde que utilizadas de maneira correta, as CAATTs podem melhorar a eficiência, eficácia, produtividade, trabalho colaborativo e segurança e diminuir o tempo gasto e a ocorrência de erros em cada auditoria. (Pedrosa, 2015). A autora ainda apresentou em seu estudo as principais ferramentas utilizadas efetivamente pelos auditores financeiros, entre elas, é possível destacar: folhas de cálculo ou planilhas eletrónicas, CAATTs personalizados pelas organizações onde atuam, DRAI (Dossier de revisão/auditoria informatizado), IDEA (Interactive Data *Extraction and Analysis*), ACD Auditor e ACL (*Audit Command Langague*).

Para cada tipo de organização e auditoria são definidos critérios para que possam ser utilizadas as CAATTs, de acordo com normas internacionais, metodologia definida e os riscos suportados (ou aceites) para determinados tipos de trabalho em cada uma das fases da auditoria: planeamento, execução do trabalho de auditoria, documentação e reporte ISACA (2008). Em relação à utilização das CAATTs, Pedrosa (2015) investiga o que é recomendado pelas ISA (*International Standards for auditing,* em tradução livre, as normas internacionais para auditoria) no quanto ao uso de ferramentas de suporte à auditoria

No entanto a tecnologia de informação está também relacionada a novos riscos no âmbito do armazenamento de informação confidencial que acrescentam novas variáveis referentes ao planeamento e execução de um trabalho de auditoria: os riscos associados à produção de informação em computadores, segundo Padoveze (2002), criam necessidade dos revisores pesquisarem como identificar os riscos nos ambientes organizacionais de maneira a conseguirem mitigá-los e comunicá-los a sua própria gestão.

Neste sentido também surge a importância dos testes aos ITGCs (*Information Tecnology General Controls*) das organizações, ou seja, as práticas de controlo interno associadas a tecnologia da informação, dentro das organizações em que os auditores estão a realizar trabalho. Os ITGCs são, por norma, testados por profissionais com grande conhecimento no funcionamento e parametrizações de sistemas da informação, com formação em TI. Estas práticas podem influenciar diretamente os trabalhos de auditoria no âmbito de obtenção de quantidade evidência de trabalho que deem conforto sobre determinadas asserções a nível das demonstrações financeiras (Pirta & Strazdina, 2012).

2.2.4 Profissão de auditoria em Portugal

Dos primitivos sistemas jurídicos da monarquia portuguesa até os dias atuais, Almeida (2014) mostra que a profissão de auditor financeiro ou revisor de contas esteve sempre presente tendo denominações diversas como:

- **Ouvidor**: cuja função era ouvir as partes, apurar provas e levar casos à decisão do senhor (ou órgão superior);

- **Vedor**: função parecida a de ouvidor, mas que também inclui julgamento de questões surgidas na coroa;

- **Conselhos fiscais**: já com surgimento do Código Comercial, em 1888, tinham funções principais de examinar escrituração de sociedades, fiscalizar administração da mesma, cumprimento de estatutos das sociedades, dar parecer sobre balanços, inventário e relatório apresentados pela administração.

No entanto, foi apenas em 1911 que surge o conceito de Revisão Legal das Contas e posteriormente, apenas na década de 60 é que o assunto sobre a independência do auditor passa a objeto de discussão na realidade portuguesa, aumentando e aperfeiçoando a fiscalização das sociedades anónimas devido a importância dos interesses e volume de negócios gerados através das mesmas.

Atualmente, um Revisor Oficial de Contas (ROC) é um profissional que atua como auditor financeiro externo com a responsabilidade e competência legal para e certificar contas a qualquer tipo de entidade e organização através da emissão de uma CLC. Cabe a este profissional verificar se as informações a serem divulgadas pelas organizações auditadas estão em conformidade com o que é estipulado pelas normas técnicas - nacionais ou internacionais - ou reconhecidas pela Ordem dos Revisores de Contas (OROC).

Para atuar profissionalmente como um ROC em Portugal, é necessário cumprir uma série de critérios e condições específicas impostas pela OROC, para além da realização de exames de alto nível divididos em 4 grupos que acontecem no espaço de um ano.

No entanto, não são apenas os ROCs que podem trabalhar com auditoria financeira em Portugal. Na maioria das vezes, as SROCs estão organizadas da seguinte forma:

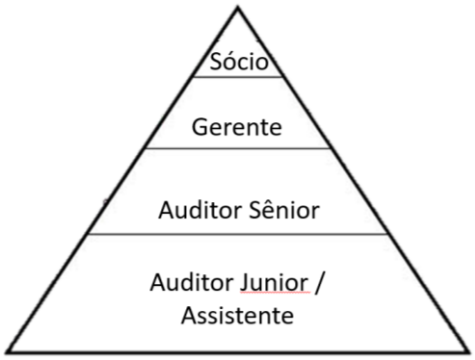


Figura 1: Estrutura de uma SROC

Fonte: Adaptado de Almeida (2014)

2.2.5 Tipos de informação no dia a dia de um ROC

Como em todas as organizações, a informação é considerada um ativo importante para as SROCs. No entanto, estes tipos de organizações não lidam apenas com as informações geradas internamente já que o principal objeto de trabalho de um ROC é a informação gerada pelas organizações para as quais está a realizar seu trabalho, sendo estas, muitas vezes, extremamente confidenciais.

Dessa maneira, é comum encontrar no Código de Conduta das SROCs tópicos muito importantes sobre a confidencialidade e ceticismo profissional no ambiente de trabalho dos profissionais bem como relações de independência e boas práticas para utilização das informações de seus clientes.

Entre os principais documentos associados ao processo da realização da auditoria , principalmente no que diz respeito aos testes substantivos aplicados, encontram se memorandos de reuniões, atas (Assembleia Geral e Conselho de Administração), faturas, extratos contabilísticos e bancários, balancetes, estimativas de folhas de pagamentos, especializações, reconhecimento de subsídios, Relatórios e Contas, Demonstrações Financeiras e outros mais (dependendo da realidade da empresa e do tipo de serviço que está a ser feito). Como estas informações muitas vezes são consultadas em caráter original, diretamente pelos auditores, é de extrema importância que a equipa tenha recebido informação acerca das políticas de segurança da informação de seus clientes.

2.3 A Segurança da Informação

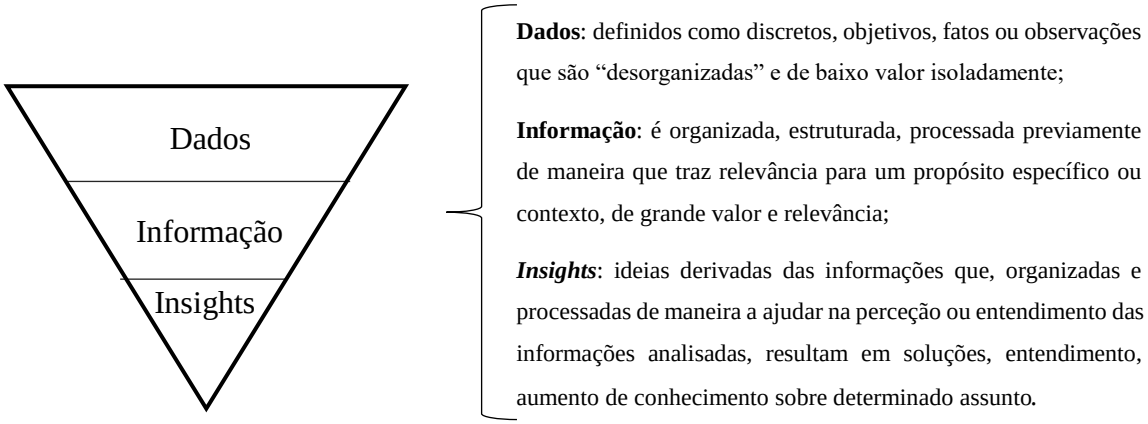
Nesta seção será feita uma breve contextualização acerca da Segurança da Informação bem como políticas de segurança até principais ameaças e preocupações. Posteriormente

será feita uma breve descrição no que diz respeito a 'segurança lógica' e 'segurança física' da informação.

2.3.1 Contextualização

Desde o surgimento das primeiras organizações até dias atuais, a informação em si possui papel essencial na sociedade e, com o passar do tempo, este recurso/ativo passa a ter cada vez mais valor para as entidades, já que pode ser materializado em muitos formatos distintos (Gouveia, 2016). Piattini (2000) descreve a sociedade atual como a "sociedade da informação". Abaixo é possível verificar o fluxo informacional a partir da composição do que se entende por informação:

Figura 2: Fluxo de conhecimento (*insights*)



Fonte: Adaptado de Tipologia de Davenport (1998).

Desta maneira, é preciso garantir a segurança deste ativo, uma vez que este é a base da continuidade de uma organização. Para tal, as organizações passaram a aplicar tipos de controlos cada vez mais sofisticados de maneira a atingir seus objetivos no que diz respeito a segurança da informação: proteger contra situações adversas, quer as mesmas aconteçam intencionalmente ou não. Segundo Santos (2014), o foco desta proteção encontra-se na informação e em seus elementos críticos bem como *hardware* e sistemas que processam e armazenam as informações das organizações.

O ISACA faz a seguinte definição sobre segurança da informação, sendo que esta seria algo que "*assegura, dentro da organização, que a informação é protegida da divulgação a utilizadores não autorizados (confidencialidade), das modificações inapropriadas (integridade) e da ausência de acesso quando requerido (disponibilidade)*" (ISACA 2012). Ainda, Wallace, Lin, & Cefaratti (2011) acreditam que o termo "Segurança da

Informação" refere-se às medidas adotadas de maneira a proteger não só a informação das organizações, bem como os sistemas de informação de acessos não autorizados, divulgação, interrupção, modificação, etc.

Assim, os principais pontos (ou elementos) básicos a serem garantidos através da Segurança da Informação são, segundo Gouveia (2016), três aspetos críticos da informação, que são: a confidencialidade, a integridade e a disponibilidade

- Confidencialidade: apenas quem possui devida autorização pode ter acesso à informação. Para protegê-la haverá de se existir sistemas de informação adequados que garantam sua segurança e confidencialidade;

- Integridade: A informação deve ser acedida e recuperada em sua forma original. Deve-se garantir que não hajam modificações intencionais ou acidentais que não sejam autorizadas;

- Disponibilidade: a qualquer momento, deve estar disponível quando houver necessidade de utilização da mesma.

Ainda, Dias (2000) acredita que para que a informação possa ser considerada segura, um sistema de informação deve respeitar outros critérios, havendo destaque para os seguintes:

- Autenticidade: deve-se garantir que a informação ou o usuário da mesma sejam autênticos;

- Não repúdio: deve-se garantir a impossibilidade de negação da existência de um serviço ou operação que possam ter criado (ou alterado) uma informação. Ainda, não é possível negar que sejam enviadas ou recebidas informações ou dados;

- Auditoria: deve ser possível efetuar o rastreamento de cada um dos passos do processo de geração de informação de maneira a identificar os participantes, locais, horários de cada etapa de geração da mesma. A auditoria aumenta a credibilidade de uma organização.

Segundo o ISACA (2010), um dos mais importantes fatores na proteção da informação e seus elementos básicos está na determinação de boas bases de uma gestão eficaz da segurança da informação. De acordo com Luz (2010) a variável tecnológica é uma entre as diversas ameaças no âmbito da segurança da informação que mais se destaca visto que a mesma é vulnerável a ações de agentes internos e externos.

Desta maneira, segundo Gouveia (2016, p. 15), "*a segurança da informação é a proteção de informação, dos sistemas e dos dispositivos (hardware) que usa, armazena e transmite informação. O objetivo da segurança da informação é o de proteger de forma adequada os ativos de informação de modo a assegurar a continuidade de negócio (ou de operação, se for preferido o uso de um termo menos associado à vida empresarial), minimizando potenciais perdas que possam ocorrer (da perda ou destruição de valor desses ativos) e maximizando o retorno de investimento (uma vez que os esforços associados com a proteção de informação tem de ser cobertos pelo seu valor ou pelo valor que deles se possa extrair)".*

Ainda, a correta apresentação e aplicação de controlos para a segurança da informação garante a credibilidade das mesmas e das organizações que as detém sendo, na atualidade, um requisito praticamente obrigatório para tal.

2.3.2 Políticas de Segurança

Gouveia (2016, p. 15) define a política de segurança como *"uma declaração de alto nível de propósito e intenção de uma organização em relação a segurança de informação*". Esta deve ser apoiada em recursos tecnológicos (*hardware* e *software*) em complemento de conscientização e formação de colaboradores no âmbito do uso eficiente e responsável das componentes da informação (Luz, 2010).

No âmbito das organizações atuais, a segurança da informação é um desafio, pelo que é muito comum o uso de correio eletrónico, redes sociais, usos de dispositivos como *Flash USB* que permitem partilha rápida e "despreocupada" de informação sensível e relevante para as organizações (Gouveia, 2016). Estudos recentes realizados pelo ISACA (2013) apontam que 6 em cada 10 indivíduos (entre 18 e 35 anos) utilizam seus próprios dispositivos nas organizações onde trabalham. Esta tendência denominada de "*Bring your own device"* ou apenas "BYOD" implica na necessidade de definição de políticas de segurança que lidem com estes desafios. Desta maneira, ao mesmo tempo que as organizações aumentam seu fluxo de informação, devem também aumentar seus investimentos políticas de segurança das informações de maneira a reduzir as ameaças a estes ativos.

Sendo os sistemas de informação ferramentas de grande importância para as organizações, para que os mesmos sejam utilizados da melhor maneira possível, e para que dados e informação inseridos estejam protegidos, é necessário haver controlos que

devem existir desde a fase de sua parametrização: Segundo Gouveia e Ranito (2007) é preciso que sejam definidas prioridades de tratamento de informação e estabelecer canais necessários para o efeito, mesmo para que procedimentos automáticos, sem intervenção humana.

De maneira a determinar quais são as Políticas de Segurança mais adequadas para cada tipo de negócio, as organizações devem entender sob quais vulnerabilidades é que estão expostas. Segundo Gouveia (2016) estas podem ser determinadas através de uma análise de risco, investigações cuidadosas em seus sistemas, ambientes e tudo o que poderá correr mal em um fluxo informacional. Uma vez que as políticas de segurança estão estabelecidas em uma organização, é necessário definir como cumpri-las através de um guia ou manual corporativo ISACA (2014).

É também necessário analisar os riscos e ameaças relacionadas ao negócio da organização. Martins & Santos (2005) Esclarece que o diagnóstico dos riscos deve ser definido junto à alta gestão da empresa: quais são os riscos que a organização está disposta a aceitar e quais não são aceitáveis, escolhendo uma das opções: reduzir nível de risco, aceitá-lo ou transferi-lo.

Ferramentas como COBIT 5 e COSO são de grande utilidade para definição das políticas de segurança de uma organização, de acordo com sua dimensão, modelo de negócios, cultura e processos.

2.3.2.1 COSO, COBIT e ISOs 17799, 27001 e 27002

De maneira a definir suas políticas e processos relacionados à segurança da informação, algumas organizações usam *frameworks* como estruturas que auxiliam na execução de tarefas necessárias e de melhoria na segurança das mesmas. Estes *frameworks* são uma série de processos definidos e os mais comuns são o COSO, COBIT e ISO 17799.

Servindo como base para estruturação do controlo interno de empresas (COSO, 2017) o COSO (*Committee of Sponsoring Organizations),* organização norte-americana com a iniciativa de estudar aspetos que podem levar a emissão de relatórios fraudulentos dentro das entidades. Possui um modelo de governança que, segundo Harris (2006), o COSO auxilia na definição de seus principais riscos ao nível de negócio, estabelece um quadro geral de maneira a auxiliar organizações a ter controlo e fazer a gestão dos mesmos, ainda que não forneça metodologias de gestão de risco por si só. O COSO surgiu espelhado no crescimento e aumento da complexidade das organizações).

Figura 3: COSO 2017

Fonte: COSO (2017)

O COBIT (*Control Objectives for Information and related Technology*), por outro lado, é uma estrutura desenvolvida pelo ISACA que define metas para os controlos adotados pelas organizações para realizar a gestão das políticas de Segurança da Informação de acordo com as necessidades operacionais das organizações (Harris, 2006).

Um dos principais objetivos do COBIT é gerar valor para as organizações e para seus processos. As diversas práticas adotadas nas diversas categorias auxiliam as entidades de desde o planeamento até monitorização dos resultados com a gestão da Segurança da Informação através de processos de Tecnologia da Informação. Para que sejam cumpridos os objetivos, o COBIT possui 5 princípios: a) Identificação das principais necessidades da organização; b) implementação de soluções completas; c) aplicação de *frameworks* simples e integrados; d) permitir abordagem holística; e) separação de governança e gestão.

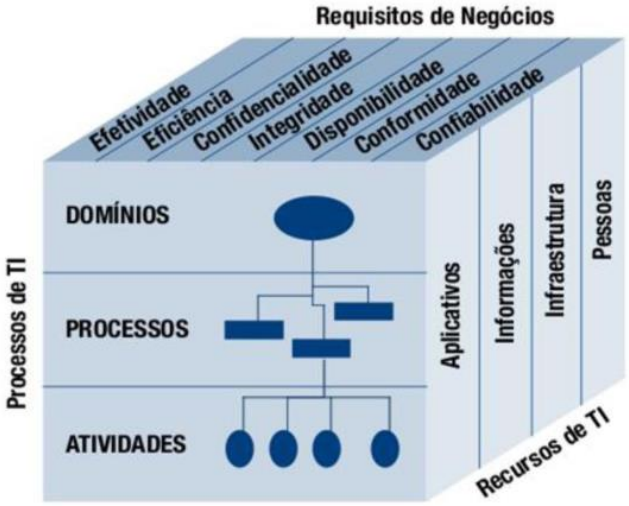


Figura 4: Cubo do COBIT

Fonte: Adaptado de ISACA-ITGI 2007 p. 25

A ISO 17799:2005, norma internacional de origem britânica de 1987, lista de maneira detalhada uma série de controlos que podem ser usados por organizações de maneira a se implementar as políticas de segurança de informação (Wallace et al., 2011) Esta norma tem sido adotada por diversas entidades de forma a criar estrutura para suas políticas de segurança. As principais abordagens da norma são: 1) entendimento dos requisitos da segurança de informação de uma organização e necessidade de estabelecer políticas e objetivos para tal; 2) implementação e operação de controlos de gestão de riscos dentro de uma organização; 3) monitorização e análise do desempenho dos controlos implementados; e 4) melhoria contínua de processos da gestão da segurança (ISO 17799). Em 2005 a ISO foi atualizada e foi usada como base para emissão das seguintes normas: ISO 27001 e 27002. A primeira delas, segundo Wallace et al. (2011), possui uma relação de controlos de gestão que organizações devem seguir de maneira a garantir e certificar os Sistemas de Gestão da Segurança da Informação (SGSI). Já a segunda manteve como principal objetivo e conteúdo uma abordagem semelhante a ISO 17799.

O foco principal das políticas de segurança é permitir a criação de uma estrutura que seja aplicável às principais necessidades e objetivos das organizações, tanto em níveis operacionais como em níveis de negócio. Assim, as organizações possuem ferramentas disponíveis que podem ser usadas como base na definição de seus principais objetivos e, posteriormente, nas suas políticas de Segurança da Informação através do controlo interno.

2.3.3 Ameaças, vulnerabilidades e preocupações

À medida que a informação se torna ativo essencial para funcionamento das organizações (ISSO 17799:2005, 2005) e, no caso das SROCs, o principal objeto de trabalho, passam também a se tornar vulneráveis, uma vez que a maioria dos sistemas de informação onde são armazenadas e processadas estão conectados em redes externas.

No que diz respeito aos sistemas de informação, as principais vulnerabilidades e ameaças estão relacionadas aos acessos a recursos e dados de maneira a implicar erros, perda de informação ou recursos, roubo de equipamentos ou perda ou modificação de informações, bem como envolvimento de terceiros não relacionados ao negócio (Pinheiro 2007).

Dias (2000) classificou em categorias as ameaças que afetam os recursos das organizações como um todo, tal como se encontra descrito na tabela 2, onde são tipificadas como: 1) ameaças associadas a erros humanos; 2) associadas à identificação e autenticação; 3) associadas à disponibilidade; 4) associadas à integridade; 5) associadas ao controlo de acesso; e 6) ameaças legais.

Tabela 2: Ameaças à informação

Tipo de Ameaças	Exemplos
Ameaças associadas a erros humanos	- Destruição ou modificação acidental de informações
	- Fornecimento acidental de informações confidenciais
	- Configuração incorreta do sistema operacional
	- Instalação de *hardware* e *software* não autorizado
	- Ameaças programadas (vírus, por exemplo)
Ameaças associadas à identificação e à autenticação	- Ameaça programada que mascara a sua própria identificação
	- Invasores que se fazem passar por utilizadores autorizados;
Ameaças associadas à disponibilidade	-Desastre natural (incêndio, terremoto);
	- Desastres causados por pessoas (guerras, bombas);
	- Falha em equipamento ou sabotagem;
Ameaças associadas à integridade	- Modificação deliberada de informações;
	- Dano Deliberado ao conteúdo de arquivos ou sistemas confidenciais;
Ameaças associadas ao controlo de acesso	- Acesso a arquivos de palavras passe;
	- Acesso não autorizado aos sistemas;
Ameaças legais	- Usuários internos que pratiquem atos ilegais;
	- Não cumprimentos de normas legais.

Fonte: Adaptado de Dias (2000, p. 71)

Quando uma ameaça se torna ataque, ou seja, quando ela se concretiza, passam a ser classificadas como ataques ativos ou passivos (Piattini, 2000): ataques passivos são caracterizados pela observação com objetivo de adquirir informações e são, consequentemente, mais difíceis de serem identificados; e ativos aqueles onde é verificado ato malicioso com intenção de interferir em sistemas ou informações de uma organização e são mais fáceis de serem detetados mas mais difíceis de se prevenir.

É possível verificar, na Tabela 3, exemplos de ataques ativos e passivos no contexto das organizações em dias atuais, onde se destacam: nos passivos o *sniffing* e o *eavesdropping* e, nos ativos: *pishing*, *spamming*, DoS e DDoS.

Um estudo da Kaspersky Lab realizado em maio de 2019 aponta que Portugal ocupa o segundo lugar no ranking mundial no que diz respeito ao número de utilizadores atacados por *spam* e *phishing*, com 23% dos ataques registados por utilizadores. Segundo o estudo, o *e-mail* institucional é o primeiro acesso para dados relacionados com as organizações sendo as multinacionais estabelecidas em Portugal as maiores vítimas dos ataques cibernéticos em território nacional. Em dados gerais, no ano de 2018 as organizações portuguesas sofreram cerca de 120 milhões de ataques através de e-mails maliciosos. À frente de Portugal está o Brasil, onde se concentram quase 28% dos ataques registados na pesquisa. De acordo com a Kaspersky Lab, o aumento no número de ataques de *phishing* decorre do aumento da eficiência nos métodos de engenharia social utilizados para atrair utilizadores a visitarem páginas fraudulentas, tendo o ano de 2018 ficado marcado pela exploração ativa de novas maneiras de aplicar este tipo de "golpe".

Tabela 3: Ataques Passivos e Ataques Ativos

Tipo de ataque	Descrição
Ataques passivos	- observação e análise de uma rede com objetivo de conhecer a infraestrutura de maneira completa;
	- *eavesdropping:* espionagem com intenção de se obter informações;
Ataques ativos:	- *phishing:* copia de *websites* de organizações de maneira a enganar utilizadores;
	- *spamming:* associada ao envio de mensagem a grande número de utilizadores, muitas vezes com vírus
	- DoS (*Denial of Service):* possui objetivo de sobrecarregar o sistema, remotamente, de maneira a conseguir que o utilizador não consiga processar nada no computador;
	- DDoS (*Distribute Denial Of Service);* onde se é possível utilizar computador da organização tendo como objetivo lançamento de ataques a outros computadores da mesma organização.

Fonte: Elaboração própria

Segundo Santos (2014), o fator imprevisibilidade acaba por se tornar mais valia para quem elabora os ataques visto que nunca se sabe quais são as principais razões e motivos para praticar estes atos, podendo ir essas motivações de simples divertimento (o ataque serve apenas para comprovar que se conseguiu) a questões políticas e económicas. Ainda assim, ataques acabam sempre por interferir e causar danos às entidades.

O ISACA (2019) em seu relatório sobre o Estado da Cibersegurança aplicou um inquérito a organizações membros da associação em diversos países e de diversos setores – sendo que 28% são da área da consultoria e 20% serviços financeiros e banca – de maneira a verificar quais eram consideradas as principais ameaças à segurança da informação dentro destas organizações: 44% dos participantes classificaram *phishing* como principal ameaça, a ocorrer com maior frequência; seguidos por (31%) *malware* e (27%) *social engineering*. Como forma de combaterem os ciberataques, organizações investem em: programas de formação (77%); *e-learnings online* (64%); comunicação de riscos através de *newsletter* (63%); e simulação de *phishing* (57%).

De maneira geral, 2018 foi um ano de estabilização, reflexão e tomada de ações contra ameaças, mas, ainda assim, espera-se que a frequência de ciberataques continuem a aumentar, mesmo que possuam relativamente as mesmas características (ISACA, 2019).

2.3.3.1 Impactos do RGPD

A partir do dia 25-05-2018, com a entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) na Europa "Regulamento da União Europeia 2016/679", de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, uma entidade ou indivíduo que sofra ataques a qualquer tipo de informação ou dados possui o dever de comunicação de violações de dados às autoridades competentes, até 72 horas após o incidente. Ainda, entre outras implicações do RGPD estão:

- Realização de reforços no que diz respeito às obrigações das entidades no âmbito da privacidade;

- Se aplicável, a nomeação de um Responsável pela Proteção de Dados (aplica-se de acordo com a necessidade de se manter um responsável com vista a apoiar a entidade na adoção de medidas que assegurem o cumprimento das obrigações impostas pelo Regulamento);

- Possibilidade de aplicação de sanções por incumprimento, que podem atingir os 20 milhões de Euros ou 4% do volume anual de negócios das entidades;

- Avaliações de impacto sobre a privacidade obrigatórias em casos determinados;

- Definição de requisitos mais exigentes aplicáveis à informação a prestar ao titular dos dados.

Com a entrada em aplicação direta da RGPD em Portugal, a OROC emitiu a circular nº 47/18, de 30 de abril de maneira a esclarecer o enquadramento no âmbito do regulamento nos serviços prestados pelos ROCs. Tais serviços compreendem consulta e verificação de conjuntos de informações julgadas necessárias para a realização de suas funções de interesse público e que o auditor conservará como prova de auditoria. O cumprimento dos deveres do Estatuto da OROC, no que diz respeito ao sigilo profissional, está de acordo com os deveres do RGPD. Segundo site da BDO Portugal:

"O tratamento da informação recolhida pelo ROC não configura tratamento de dados pessoais efetuados por conta dos Clientes uma vez que o ROC não é subcontratante do Cliente na aceção do artigo 28.º do RGPD. Assim, para os Serviços do ROC prevalecem os acordos escritos firmados com os Clientes, mediante contrato de prestação de serviços e/ou de carta de compromisso, em conformidade com a lei, com as normas internacionais de auditoria e cumprindo as orientações da OROC aplicáveis." (BDO Portugal, 2018).

No sentido de cumprir com os pontos estabelecidos pelo RGPD, é necessário compreender o que se entende por "dados pessoais", tal como se refere na Tabela 4, nomeadamente, o que permite identificar uma pessoa diretamente e os que, embora isolados não permitam a identificação da pessoa, combinados permitem a identificação.

Tabela 4: O que são dados pessoais?

Definição	São informações que permitem identificar uma pessoa direta ou indiretamente como, por exemplo:	Existem ainda dados que, isoladamente, não permitem identificar uma pessoa singular, mas que quando combinados com outros permitem identificá-las:
Exemplos	- Números de identificação	- Cargo (por exemplo: diretor)
	- Registos de Automóveis	- Género (por exemplo: masculino)
	- Morada	- Entidade empregadora
	- Endereços de IP	Estes dados, quando unidos, podem permitir identificar um indivíduo.
	- Endereços (pessoais) de e-mail	

Fonte: Elaboração Própria

Para além do tipo de informação exemplificada acima, existem ainda dados considerados especiais. São informações que, devido a sua natureza, podem colocar em risco os direitos e liberdades fundamentais da pessoa singular exposta. É por esse motivo que é preciso ter cuidado ao tratá-los ou utilizá-los. São exemplos de dados especiais: dados biométricos, origem étnica ou racial, dados genéticos, opinião política, orientação sexual e convicções religiosas (RGPD, 2019).

2.3.4 Segurança da Informação e Cibersegurança

Em muitos aspetos, as diferenças entre segurança da informação e cibersegurança são insignificantes no que diz respeito às responsabilidades dos auditores, uma vez que este último conceito apenas se tornou parte das preocupações no âmbito da governança corporativa recentemente (Lanz, 2014). Gyun No e Vasarhelyi (2017) definem a Cibersegurança como um conceito abrangente que engloba a segurança da informação e a garantia da informação. No entanto, o ISACA (2016, p. 9) define a cibersegurança como "*Proteção dos ativos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas de informação interligados*" e, assim, é possível concluir que tem como foco a informação digital dentro e fora das organizações. O IIA (*Institute of Internal Auditors*) (2016, p.5) garante a importância da cibersegurança no âmbito dos "*sistemas que suportam os objetivos de uma organização relacionados a eficácia e eficiência das operações, fiabilidade de relatórios internos e externos, bem como a conformidade com normas e regulamentos aplicáveis*". A principal diferença entre os dois conceitos, portanto, é que a definição de Segurança da Informação possui um alcance mais amplo que a cibersegurança, sendo esta última um conjunto de tecnologias, processos e práticas que salvaguardam a proteção dos ativos de uma organização (informações e sistemas). No âmbito desta revisão de literatura, será considerado o facto de que a cibersegurança está englobada no conceito de segurança da informação, pelo que serão tratados os termos como "um só", como apenas Segurança da Informação.

2.4 A segurança da informação nas SROCs

Sendo a informação gerada pelos clientes das SROCs um dos principais objetos de trabalho, é de grande importância a existência de políticas de segurança de informação eficientes visto que, muitas vezes, os dados e informação são confidenciais, requerem sigilo uma vez que podem, inclusive, interferir no mercado económico e financeiro

(Teixeira, 2017). A autora ainda se refere a importância nas relações baseadas na confiança entre os ROCs e seus clientes da qual resulta o estrito cumprimento dos deveres de confidencialidade e privacidade. Deste modo é natural que qualquer impacto relacionado com a segurança da informação acrescente desafios para o dia a dia destes profissionais.

2.4.1 Contextualização

Em Portugal, ataques com intenção de se obter vantagens económicas estão no topo: segundo Teixeira (2017) verificou-se aumento exponencial dos casos noticiados em Portugal relativamente a extorsão cibernética (*ransomware*), que tomam poder de bases de dados e/ou de informação confidencial dos ROCs e realizam pedidos de resgate ou outras exigências de pagamento para a sua recuperação.

Segundo a Grant Thornton, quinta maior empresa de auditoria financeira, consultoria e *outsourcing* a nível mundial, fez um levantamento, em 2017, onde apontou que os prejuízos consequentes de ataques cibernéticos giraram em torno de US$280 mil milhões naquele ano. O estudo foi realizado com base em respostas de 2500 líderes de organizações ao redor do mundo, em 36 diferentes setores. Em cerca de 30% dos casos, os ciberataques resultaram em perda de reputação das organizações e 52% das entidades, apesar de terem noção da existência do risco de ataques deste género, não fazem investimentos de maneira a mitigá-los.

As consequências no caso de uma informação confidencial tornar-se pública, ou no caso da utilização da mesma por terceiros não autorizados, estão, não apenas ao nível das relações com clientes, mas também podem causar danos irreparáveis na reputação das SROCs ou de qualquer outro tipo de entidade. Segundo o *Recorded Future* (2016) ciber criminosos do tipo *hacktivists* (Hackers Ativistas, em tradução livre) geralmente não são motivados pelo dinheiro que ganham a sequestrar informações de organizações, mas sim quando causam perdas de conteúdos críticos capazes de causar danos irreversíveis na reputação da organização em causa. Além de prejuízos e processos judiciais, a perda, acesso indevido ou utilização inadequada de uma informação no contexto de uma SROC é provável que possam gerar impactos na economia, principalmente no âmbito das entidades cotadas em bolsa se, por exemplo, a mesmas respeitarem a situação económico-financeira do cliente.

De acordo com o BI *Intelligence* é expectável que as organizações invistam cerca de 600 bilhões de euros em iniciativas que envolvam cibersegurança entre 2015 e 2020 em todo o mundo (*Business Insider*, 2016). Tais investimentos seriam em segurança em computadores nas empresas (cerca de 300 bilhões), segurança em *IoT (Internet of Things) devices* (cerca de 200 bilhões) e segurança em dispositivos moveis (100 bilhões). Na tabela 5 é possível verificar exemplos de ataques à informação e defesas que podem ser implementadas como maneira de mitigar tais ataques.

Segundo a PwC (através do relatório "*Global State of Information Security Survey*", 2018), os incidentes atribuídos a *hackers*, concorrentes e indivíduos externos às organizações diminuíram. No entanto, aqueles incidentes atribuídos a pessoas de dentro da organização, como terceiros - incluindo fornecedores, consultores e contratados - e funcionários, permaneceram praticamente iguais ou aumentaram tanto por erro como intencionais. Duncan & Whittington (2014) afirmaram a existência de ameaças internas dentro de organizações:

"There is also the internal threat to consider. Disaffected employees, laziness, sloppy installation of systems, simple naivety or perhaps lack of training in the importance of security" (Duncan & Whittington, 2014 p. 5)

Tabela 5: Tipos de Ataques e Tipos de Defesas

5 tipos de ataques	5 tipos de defesa
Zero-Day Attacks: têm como alvo vulnerabilidades em *software* que ainda serão descobertas	*Network Defenses*: Impede que os *hackers* tenham acesso às informações sensíveis e críticas nos sistemas das organizações.
Cloud-Data Leakage: Acontece quando colaboradores fazem *upload* de informações das organizações em serviços de *cloud* tipo *Dropbox*	*Endpoint and Mobile Device Protection*: impedem que *hackers* comprometam dispositivos móveis.
Mobile Malware: Especificamente desenhado para fazer como alvo os sistemas operacionais de dispositivos móveis de maneira a roubar as informações lá inseridas pelos usuários	*Data in Motion Defenses*: Incluem proteção de dados enquanto está a ser enviada de um dispositivo a outro.
Targeted Attacks: Usam uma variedade de métodos de *hackeio* com organizações ou usuários definidos préviamente como alvo	*Data At Rest Defenses*: Inclui proteção de dados quando estão a ser armazenadas em bases de dados corporativas
SQL Injection: permite que os *hackers* executem códigos maliciosos em um servidor de maneira que os permita roubar, modificar ou apagar dados no mesmo.	*Analysis & Correlation Tools*: Ajuda a monitor o fluxo de data pela rede corporativa e bases de dados para encontrar atividades suspeitas.

Fonte: Adaptado de Business Insider (2016)

2.4.2 Políticas de Segurança da informação para as SROCs

O processo de definição das Políticas de Segurança da informação no âmbito das SROCs não se diferencia em relação ao das demais entidades: é necessário realizar um levantamento de questões relacionadas às principais vulnerabilidades do da organização e de seu ambiente para obter, através de respostas objetivas, práticas que, ao aplicadas, se tornarão parte de suas Políticas de Segurança. No entanto, ao contrário de outras organizações, as SROCs não só devem se preocupar em possuir e estabelecer PSIs para proteger a sua própria informação, mas também a dos seus clientes e, neste sentido, as Políticas devem estar sempre atualizadas e aplicáveis a qualquer tipo de cenário que possa surgir.

Segundo Lanz (2014, p. 6) em um passado não tão distante, era comum organizações deixarem de lado questões sobre segurança informacional (principalmente relacionadas a cibersegurança) e atribuírem essas responsabilidades apenas aos departamentos de Tecnologia da Informação (TI). Com o passar do tempo, ao perceberem que praticamente todos os processos das organizações estavam relacionados com tecnologia, passaram a notar a necessidade de passar a responsabilidade também aos responsáveis diretos pelo negócio. Nesta ótica, a quarta parte do inquérito aplicado possui afirmações em escala Likert que têm por objetivo obter maior entendimento sobre a perceção sobre a sensibilização feita dentro das organizações (SROCs) no âmbito das PSIs aplicadas e postas em práticas.

É de se destacar que as Políticas de Segurança adotadas pelas entidades não significam a eliminação total de riscos, mas sim a mitigação dos mesmos.

Ainda, sendo o trabalho desenvolvido pelas SROCs potencialmente relacionado com tipos de serviço com sanções e valores monetários altos no caso de perda de informação por ciberataques ou má utilização de informação e tratamento de dados por terceiros, existe atualmente a possibilidade de transferência do risco para obter salvaguarda que permita financeiramente e forneça apoio necessário em caso de incidentes. Teixeira (2017) menciona a existência de diferentes tipos de apólices de seguro especialmente desenhadas para responder aos desafios do dia a dia das SROCs com coberturas que visam indemnizar terceiros lesados (clientes, colaboradores ou fornecedores, arcam com custos de defesa em ações judiciais e procedimentos administrativos), coberturas para "danos próprios", na medida que satisfaz o ressarcimento do próprio ROC; e cobertura para "despesas com serviços" de maneira a arcar com a despesa com peritos em informática

forense, advocacia, consultoria de imagem e comunicação como apoio na resolução do sinistro.

2.4.3 As responsabilidades dos ROCs e impacto em seu trabalho

Estudos prévios demonstram que incidentes que afetam a segurança da informação de uma companhia, principalmente relacionados a cibersegurança, podem afetar negativamente organizações (Campbell, Gordon, Loeb, & Zhou, 2003) (Gatzlaff & McCullough, 2010) (Yayla & Hu, 2011) (Gordon, Loeb, & Zhou, 2011) (Hinz, Nofer, Schiereck, & Trillig, 2015).

O Centro de Qualidade em Auditoria (*The Center for Audit Quality* - CAQ, 2014) emitiu, em 2014, um alerta de maneira a resumir as responsabilidades dos revisores oficiais de contas em relações sobre questões de cibersegurança. O documento sugere, por exemplo, que os auditores sejam responsáveis por avaliar a contas da empresa para perdas relacionadas à cibersegurança, por avaliar o impacto nas demonstrações e divulgações financeiras da organização e por examinar os controlos da mesma relacionados ao registo e divulgação tempestivos das informações necessárias.

De acordo com o *Recorded Future* (2016) existem 4 tipos de "cibercriminosos" que ameaçam a segurança da informação de modo que causam impactos negativos de diversas formas às organizações. A tabela 6, de elaboração própria adaptada para interpretação do estudo mencionado, relaciona os 4 tipos de cibercriminosos e possíveis impactos negativos sobre as SROCs. De um lado, o *Modus Operandi* dos 4 tipos de criminosos apontados pelo estudo e, do outro os possíveis e principais impactos sobre uma entidade do tipo SROC.

Tabela 6: 4 tipos de cibercriminosos e consequências para as SROCs

Tipo de Ameaça	***Modus Operandi***	**Impacto em SROC**
Organizações de cibercrime organizado	Grupos muito bem equipados com ferramentas e *know how* suficiente para encontrar qualquer tipo de informação dentro da rede. Possuem interesse por dinheiro, podem atuar "por conta própria " ou "para terceiros" de maneira a extorquir o dono da informação por dinheiro ou vender a mesma na *dark web*. Geralmente atuam com envio de *phishing* contendo *malwares.*	Devido ao grande fluxo informacional no decorrer dos trabalhos, há risco de sequestro de informações devido ao mau uso de ferramentas de segurança, gerando prejuízo ao cliente e prejudicando a reputação da SROC

Tipo de Ameaça	***Modus Operandi***	**Impacto em SROC**
Hackactivists	Muito equipados, realizam ataques por DDoS. Atuam de maneira a atacar websites de maneira que serviços e acesso às informações fiquem "fora do ar".	Se um cliente sofre estes tipos de ataque, os trabalhos de auditoria são indiretamente prejudicados, devido ao aumento dos riscos. Já se o ataque é diretamente na SROC, a reputação da mesma é prejudicada devido a baixa segurança que aparenta ter sobre seus próprios dados
State-Sponsored (Ciber Espiões)	Não atuam com interesse direto em obtenção de lucro imediato. Buscam acesso silencioso às informações mais sensíveis de uma organização, muitas vezes de países terceiros (indústria de tecnologia, indústria farmacêutica e financeira são principais alvos). Possuem interesses políticos, governamentais.	Se um cliente sofre estes tipos de ataque, os trabalhos de auditoria são indiretamente prejudicados, devido ao aumento dos riscos. Já se o ataque é diretamente na SROC, a reputação da mesma é prejudicada devido a baixa segurança que aparenta ter sobre seus próprios dados
A ameaça Interna	Muitas vezes, um colaborador em sua melhor intenção pode deixar "perder" algum conteúdo sigiloso dentro de uma companhia. Não é esse o caso deste tipo de ameaça, visto que não "deixam vazar", mas sim “apropriação intencional” de dados ou informação da SROC onde o colaborador atuava.	Em organizações do tipo SROC a rotatividade de colaboradores é relativamente alta, devido as grandes quantidades de horas trabalhadas em determinadas épocas do ano. Deste modo, o risco de que colaboradores que estejam insatisfeitos com as organizações realizem esquemas para prejudicar as mesmas.

Fonte: Adaptado de *Recorded Future* (2016)

comprovado que os *fees* podem aumentar se os incidentes tiverem impacto diretamente no risco de existência da organização. Os valores dos serviços cobrados sofrem impacto devido aos incidentes visto que os mesmos podem estar associados ao Risco de Distorção Material: a ocorrência de um incidente relacionado com cibersgurança pode aumentar o risco de negócio do cliente e este é um dos fatores que influenciam na tomada de decisão dos revisores no que diz respeito a aceitar ou não um cliente (Li, No, & Boritz , 2016).

Um estudo realizado pela Deloitte Portugal (2013) que diz respeito a Segurança Digital e Privacidade no Setor Bancário indica que as organizações haviam começado a apresentar crescente preocupação com a temática da segurança devido a exigência de seus clientes e evolução de requisitos de órgãos reguladores. Estes dois pontos são importantes, pois se tratam de aspetos comuns que os dois segmentos de negócio (SROCs e bancas) têm em comum. Nesta ótica, a terceira parte do grupo de questões elaboradas no inquérito aplicado no presente trabalho foi inspirada no estudo realizado pela organização. Através destas questões o que se pretende é verificar as principais preocupações da organização

onde o participante trabalha no âmbito da segurança da informação bem como o atual contexto das mesmas e tipos de tecnologia associada a segurança de dados.

Segundo o Relatório do Cenário de Ameaças à Segurança da Informação emitido pelo ENISA (*European Union Agency for Network and Information Security)*, organismo da União Europeia que tem por objetivo garantir alto nível de segurança em redes de informação na Europa:

"*os smartphones serão os dispositivos mais comuns para acesso à Internet"* (ENISA, 2010 p.33)

Neste momento, e 9 anos após a emissão do relatório referido é possível comprovar que o estudo esteve correto na estimativa definida. Segundo a CNBC (2019), um estudo realizado pela WARC (*World Advertising Research Center*) indica que, até 2025, mais de 70% do acesso à Internet será realizado através de *smartphones*.

Segundo o ENISA (2010, p. 33), os riscos dos *smartphones* são: a. Perda de dados; b. Desativação inadequada; c. Disponibilização não intencional de dados; d. *Phishing;* e. *Spyware;* f. *Network spoofing attacks*; g. *Surveillance.*

A organização ainda classifica ameaças como *phishing* e *spyware* como principais tendências nas ocorrências relacionadas a cibersegurança (ENISA, 2016)

No Relatório de Ameaças à Segurança da Informação correspondente ao ano de 2018 a ENISA (2019) listou ações de mitigação associadas às principais ameaças com destaque para:

- Uso de encriptação em todo o armazenamento e fluxo de informação que se encontram fora do perímetro de segurança (dispositivos móveis, serviços na nuvem);

- Imposição de limite de acesso a áreas com informação ou equipamentos sensíveis;

- Implementação de política de segurança física bem documentada e integrada com dispositivos móveis;

- Elaboração de guias de utilizadores ou "boas práticas";

- Elaborar e estabelecer procedimentos que garantam proteção física: dano, perda, roubo;

- Contratação de seguros, de forma a transferir riscos associados às ameaças

É neste sentido que, tanto a terceira e, principalmente, a quarta parte das questões/afirmações elaboradas para o inquérito estão relacionadas com a política de

segurança da informação associada a dispositivos móveis dentro das organizações. As afirmações da quarta parte, onde se utiliza escala Likert, foram elaboradas com intuito de obter a perceção da sensibilização dos colaboradores em relação às políticas de segurança da informação das SROCs onde trabalham.

3 Metodologia de Trabalho

3.1 Abordagem e desenvolvimento da pesquisa

Neste capítulo serão apresentados os procedimentos metodológicos adotados de maneira a fazerem-se cumprir os objetivos deste estudo já definidos previamente através de análises qualitativas e pesquisa descritiva, sendo estes: analisar a prática das políticas de segurança aplicadas em SROCs, de maneira a garantir a segurança necessária e mínima exposição ao risco; e identificar as tecnologias utilizadas pelas organizações bem como as fragilidades no contexto da segurança de informação das organizações.

Collis e Hussey (2005) consideram como pesquisas descritivas aquelas que são usadas com objetivos de obter características de determinados problemas. Desta maneira o estudo foi organizado da seguinte forma: inicialmente foi realizada uma revisão bibliográfica sobre os temas: contabilidade & auditoria financeira, segurança da informação & cibersegurança, políticas de segurança e estrutura das SROCs em Portugal. Os conteúdos disponíveis auxiliaram na perceção e contextualização do tema principal do estudo "a segurança da informação nas SROCs" apesar de não haver literatura dedicada totalmente ao estudo sobre Segurança da Informação em organizações deste tipo em Portugal

3.2 Definição do instrumento de recolha de dados e amostra

Atendendo a que não existem estudos prévios que abordem a segurança da informação nas SROCs em Portugal, a metodologia de investigação definida para o estudo foi aplicação de inquérito através de questionário aos profissionais que trabalham em SROCs, sejam eles ROCs ou não, de maneira a obter dados sobre as políticas de Segurança da Informação adotadas dentro do atual contexto das organizações. O inquérito foi considerado como a melhor forma de obtenção de respostas dos participantes em alternativa a entrevistas, uma vez que os participantes no estudo se encontram dispersos e, em determinadas épocas do ano, possuem elevada carga de trabalho.

3.2.1 Definição do questionário

Com base no conhecimento adquirido através da revisão bibliográfica deste estudo, e documentado no capitulo anterior, o questionário foi elaborado com um total de 14 questões destinadas a profissionais que atuem na área de revisão legal de contas, ou seja, trabalhem em SROCs. A versão final do mesmo foi obtida após a validação de

especialistas em auditoria que puderam verificar se as questões estavam adequadas ao contexto da pesquisa. Um pré-teste *online* foi realizado com alunos do Mestrado em Auditoria que se encontravam em Estágio ou a desenvolver trabalho em SROCS. No pré-teste foram obtidas 13 respostas e sugestões quanto à forma como diversas questões deveriam ser melhoradas.

O questionário final possui a seguinte estrutura de perguntas: A primeira parte, voltada para obtenção de informação de carácter profissional dos respondentes, foi elaborada com base no estudo de Pedrosa (2015) de maneira a possibilitar a comparabilidade das informações obtidas após aplicação do inquérito; a segunda parte está associada com informações relacionadas aspetos dimensionais e área de atuação da organização onde o respondente trabalha; a terceira parte, com afirmações mais específicas acerca das políticas, ferramentas de segurança da informação adotadas pela organização bem como preocupações e perspetivas futuras para as PSIs implementadas, foi elaborada com questões adaptadas do estudo feito pela Deloitte (2013) em Portugal, no que diz respeito a Segurança Digital e Privacidade no setor bancário e, deste modo, se torna possível verificar se este setor vai o de encontro da realidade das SROCs no que diz respeito a este assunto; a quarta e última parte contém afirmações em escala Likert de maneira concluir sobre o entendimento do colaborador no que diz respeito à sensibilização efetuada pelas SROCs onde trabalham em relação às políticas de segurança adotadas nas organizações onde trabalham. Esta última parte foi elaborada conforme entendimento das principais políticas de segurança, no contexto de atividade profissional exercida em uma SROC de grande porte em Portugal. O questionário completo encontra-se no Apêndice 5 deste trabalho. Entende-se que as respostas deverão permitir inferir o grau de utilidade da informação conforme a opinião de profissionais que atuam na área da auditoria em Portugal no que diz respeito à Segurança da Informação dentro das SROCs.

A escala Likert permite medir a atitude e opinião de indivíduos e proporciona uma gama de respostas a questões ou declarações definidas pelo pesquisador Jamieson (2004). Como a pesquisa enquadra-se como descritiva e qualitativa, a pontuação das respostas das afirmações apenas apresenta o quão são relevantes ou quão são, na opinião dos respondentes, postas em prática as políticas de segurança mencionadas. É relativamente impossível, visando fiabilidade e verificabilidade das informações, a transformação da análise das informações obtidas em variáveis quantitativas (Fávero et al., 2009)

Pretende-se que os dados coletados reflitam a opinião da amostra de profissionais que trabalham com auditoria em Portugal. 5

Após elaboração das questões, as mesmas foram introduzidas na plataforma Lime Survey através do acesso restrito para alunos do Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra. Foi criada uma base de dados de endereços de email para permitir enviar, de forma personalizada, o questionário, garantindo, assim, que se poderia acompanhar as respostas iniciadas e controlar as insistências de resposta efetuadas. Posteriormente, foi enviada mensagem com o questionário aos endereços eletrónicos dos participantes. A opção por esta plataforma foi definida devido a permissão para criação de identificadores específicos que se associa a cada participante (*Tokens)* de maneira a garantir que cada resposta era associada a um único utilizador.

3.2.2 Envio e aplicação do inquérito

Numa primeira fase foram introduzidos os e-mails e nomes dos ROCs registados na OROC, pelo que desta maneira foi possível elaborar mensagens personalizadas de apresentação, convites e lembretes para participação do inquérito a todos os contactos bem como associação de *tokens* aos participantes (Apêndices 3 e 4). Posteriormente foram enviadas mensagens a SROCs a solicitar a participação de colaboradores que trabalham com auditoria financeira, mas que não são ROCs a entidades registadas no *website* da OROC. O inquérito ficou disponível a partir do dia 11 de julho de 2019, até o dia 13 de setembro de 2019, data da última resposta registada.

3.2.3 Participantes

Não é objetivo de trabalho obter informações apenas de profissionais registados na OROC, mas sim incluir todos os colaboradores que trabalhem com auditoria dentro das SROCs, sejam eles assistentes ou sócios das organizações.

Sendo assim, como anteriormente descrito, foram coletados, através do site da OROC, os contactos eletrónicos dos ROCs registados na Ordem: um total de 1470 endereços de correio eletrónico profissionais ativos em Portugal.

Posteriormente, foram obtidos os contactos eletrónicos de SROCs em Portugal, sejam elas de grande ou pequeno porte de forma a possibilitar o envio do questionário a

colaboradores que executassem atividades profissionais relacionadas a auditoria, num total de 204 SROCs registadas em Portugal.

Através da plataforma Lime Su

rvey foram enviadas mensagens aos 147 endereços eletrónicos acima mencionados. No entanto, foi registado na plataforma que 11 indivíduos optaram por não responder ao inquérito. Outros 6 indivíduos responderam a mensagem a informar que não exercem atividade como ROC e, sendo assim, não iriam responder o inquérito.

3.2.4 Técnicas de Análise e Representatividade da Amostra

Foi efetuada uma avaliação da fiabilidade das variáveis do estudo, estendida na dimensão de consistência interna, através da análise dos itens, na qual foram ponderadas as correlações por intermédio do Alfa de Cronbach (Cronbach, 1951), uma das medidas de consistência interna mais utilizadas, definida como o quadrado da correlação entre as pontuações da variável latente e o fator subjacente que a variável se propõe medir. Foi utilizado como suporte estatístico o *software* SPSS como recurso informático necessário ao desenvolvimento da análise de dados.

Aceita-se como limite inferior de adequada consistência interna o valor de 0,70 (Nunnally & Bernstein, 1994; Robinson et al. 1991). As variáveis que tiveram correlações ponderadas dizem respeito às perguntas P11.2, P11.3 e P11.4, uma vez que pelo tipo detalhe da análise efetuada no capítulo 4.4 fez sentido efetuar-se a ponderação.

4 Apresentação e Discussão dos Resultados

Este capítulo tem como objetivo, em primeiro lugar, evidenciar os resultados obtidos através da aplicação do inquérito, relativamente à caracterização dos respondentes e das organizações onde trabalham. Posteriormente, serão apresentadas as técnicas de análise das variáveis e resultados obtidos, seguido pelo entendimento relativamente às políticas da Segurança da Informação dentro das SROCs.

4.1 Caracterização dos respondentes

O questionário foi aplicado a profissionais que atuam diretamente em auditoria financeira, em SROCs de Portugal, sendo os profissionais ROCs ou não. Os ROCs foram contactados através do e-mail disponibilizado pela Ordem no portal eletrónico, num total de 1470 endereços eletrónicos ativos. Destes, 11 profissionais optaram por clicar na opção de não participar da pesquisa (*opt out*, opção disponível para o efeito no Lime Survey). 6 profissionais responderam a mensagem de convite com a informação de que não exerciam atividades em SROCs ou de ROC, portanto não iriam responder o inquérito. Além disso, das 204 SROCs registadas, foi possível obter 138 endereços de e-mail, efetivando o número de convites enviados diretamente as SROCs, inteirando o total de convites através do correio eletrónico. Desta maneira, a população total do estudo foi de 1591 endereços eletrónicos, foram obtidos 175 registos de respostas foram considerados válidos para a análise, representando uma proporção de 11%. Abaixo é possível verificar as características gerais dos participantes.

A maioria dos respondentes é do género masculino (58%) e tem menos de 50 anos (80%). A média de idades dos respondentes é de 41 anos, sendo que o respondente mais velho possui 76 anos de idade e o mais novo 23 anos de idade. Cerca de 65% dos trabalhadores trabalham com auditoria financeira há, pelo menos, 5 anos, sendo a média de anos com experiência nesta área de aproximadamente 15 anos. 61% dos respondentes são Revisores Oficiais de Contas (ROCs). Abaixo é possível fazer uma comparação entre o estudo feito por Pedrosa (2015). É importante referir que o estudo de Pedrosa (2015) envolveu apenas ROCs em atividade e daí que nos possamos aperceber de algumas diferenças, nomeadamente relativamente à idade do inquirido mais novo (23 neste estudo e 31 no anterior) bem como no estudo presente a existência de um maior conjunto de inquiridos com menos de 50 anos. Por norma, o acesso à profissão de ROC estabelece a necessidade

realização de exames, estágio, entre outros procedimentos, sendo que o acesso é mais tardo quando comparado com o exercício da função de auditor financeiro não sendo ROC.

Tabela 7: Comparação entre informações gerais obtidas através dos estudos

Género dos Respondentes	**Neste estudo (%)**	**Pedrosa (2015) (%)**
Masculino	58%	71.3%
Feminino	39%	28.7%
Optaram por não se identificar	3%	0%
Idade dos Respondentes	**Neste Estudo**	**Pedrosa (2015)**
Mais velho	76 anos	78 anos
Mais novo	23 anos	31 anos
Com menos de 50 anos	80%	67%
Idade média	41 anos	47 anos
Em relação a profissão de Auditor Financeiro	**Neste Estudo**	**Pedrosa (2015)**
Média de anos trabalhados como Auditor Financeiro	14,8 anos	16,7 anos
Profissionais registados na OROC (ROC)	61%	100%

Como já mencionado na seção de contextualização da profissão de auditoria em Portugal, as Sociedades de Revisores Oficiais de Contas (SROCs) possuem estruturas organizacionais e posições hierárquicas que podem variar, mas que são muito semelhantes entre si. Deste modo, no que diz respeito ao nível hierárquico que cumprem dentro das empresas, a maioria dos respondentes são sócios das organizações (36%) e, logo em seguida, os seniores (16%) e auditores juniores (14%), como é possível identificar na Tabela 8, abaixo. Nesta questão, foram registadas 174 respostas.

Tabela 8: Nível hierárquico dos respondentes dentro das organizações

Nível Hierárquico dentro da SROC	**Indivíduos**	**%**
Sócio	64	37%
Auditor sénior ou equivalente	27	16%
Auditor júnior ou equivalente	24	14%
Assistente (estagiário) ou equivalente	20	11%
Gerente (supervisor) ou equivalente	20	11%
Diretor ou equivalente	19	11%
Total	174	

4.2 Características das organizações

As três questões relacionadas com as organizações onde os participantes trabalham tiveram como objetivo indicar apenas o segmento de negócio para os quais exerciam prestação de serviços (ou seja, a quais setores os seus principais clientes pertenciam) e dimensões da organização através da questão sobre número de colaboradores e atividades no exterior. Não foram colocadas questões relacionadas com aspetos económicos (resultados e rácios) em relação as organizações. Também não foram feitas distinções entre as *big four* e outras SROCs, mas, através das duas questões, é possível verificar a dimensão das organizações no que diz respeito à presença das organizações noutros países para além de Portugal.

Para esta segunda parte do inquérito, foi possível selecionar várias opções dentro das afirmações, uma vez que as SROCs podem atuar em vários segmentos. Assim, apenas 32% dos participantes informaram que as suas organizações atuavam no segmento de serviços financeiros (bancas ou seguradoras, por exemplo), 73% dos participantes indicaram que suas organizações estavam no setor da indústria de produção (químicos, papel e celulose, tecnologia, agricultura) e 69% dos participantes indicaram que suas organizações atuam no segmento de outros serviços (como, por exemplo, energia, turismo e entretenimento). 13% dos respondentes indicaram ainda que as suas organizações atuam em outros segmentos, tais como administração pública e construção civil. Juntos, representam 42% do total.

A Tabela 9 abaixo indica a proporção do número de colaboradores que as organizações possuem, bem como se as organizações estão presentes noutros países, para além de Portugal. Noventa e quatro indivíduos (53%) responderam que as organizações onde trabalham estão presentes em outros países e 71 (41%) colaboradores assinalaram “não” para esta opção. 4% dos participantes optaram por não responder a esta questão.

Cerca de 32% dos respondentes trabalham em organizações de pequena dimensão, que possuem entre 1 a 10 colaboradores, e 33% dos participantes indicam que trabalham em organizações de maior dimensão, tendo alguns referido a existência de mais de 1000 colaboradores em seu quadro, através da seleção da opção “1000+ colaboradores”.

Percebe-se, desta forma, que os participantes se encontram distribuídos em organizações com diferentes realidades, o que garante a este estudo “a oportunidade” de conhecer o contexto das PSIs em organizações com dimensões muito distintas umas das outras. Deste

modo, será possível relacionar a dimensão das organizações com o nível de políticas e práticas de segurança implementadas.

Tabela 9: Dimensão das organizações inquiridas

Quantos colaboradores (aproximadamente) a organização onde realiza suas atividades profissionais possui?	**Indivíduos**	**%**
1 - 10 colaboradores	56	32%
11 - 50 colaboradores	28	16%
51 - 100 colaboradores	6	3%
101 - 500 colaboradores	12	7%
501 - 1000 colaboradores	5	3%
1000+ colaboradores	58	33%
N/D	10	6%
Total	175	100%
A organização onde realiza atividades profissionais está presente em outros países, para além de Portugal?		
Sim	94	53%
Não	71	41%
N/D	10	6%
Total	175	100%

4.3 As Políticas de Segurança da Informação nas SROCs

Como mencionado na seção 3.2, a terceira e quarta parte do questionário estão relacionadas com as políticas de segurança adotadas pelas organizações onde os participantes do questionário exercem atividade profissional.

Através da Tabela 10, elaborada partindo da última questão da quarta parte do inquérito, é possível perceber que 130 indivíduos indicaram ter conhecimento sobre as políticas de segurança da informação nas organizações onde trabalham, apenas 7 não indicaram não ter conhecimento e 38 optaram por não responder a esta pergunta.

Desta maneira, considera-se que grande parte dos colaboradores, independente da dimensão da organização onde trabalham, tem conhecimento sobre o atual contexto das Políticas de Segurança da Informação que estão a ser aplicadas.

Tabela 10: Conhecimento sobre as políticas de SI dentro das organizações

P14 - "De maneira geral, acredito ter conhecimento sobre as políticas de segurança da informação que são aplicadas na organização onde trabalho"		
Resposta	**Observações**	**%**
Sim	130	74%
Não	7	4%
N/D	38	22%
Total	175	100%

Na Tabela 11 é possível perceber as principais características dos colaboradores que não possuem conhecimento sobre as políticas de segurança da informação de suas organizações.

Tabela 11: Principais características dos que não conhecem as políticas de SI

Atual Posição Hierárquica	**Nº Observações**
Auditor Sénior ou Equivalente	2
Diretor ou equivalente	2
Auditor Júnior ou equivalente	2
Assistente (estagiário) ou equivalente	1
TOTAL	**7**
É membro da OROC	
Sim	3
Não	4
TOTAL	**7**
Dimensão da organização onde trabalham	
1-10 colaboradores	3
1000+ colaboradores	3
11 - 50 colaboradores	1
TOTAL	**7**
Média de anos de trabalho com auditoria financeira	**12**

4.4 Perceção dos colaboradores em relação às PSIs

Esta parte do inquérito contém afirmações mais específicas acerca das políticas de segurança da informação adotadas pela organização onde os participantes trabalham. Foi elaborada partindo de questões do estudo realizado pela Deloitte (2013) em Portugal, no que diz respeito a Segurança Digital e Privacidade no setor bancário e que foram adaptadas à realidade das SROC. Enquanto o estudo da Deloitte (2013) apresentou as afirmações em escala Likert, já o presente trabalho adaptou para questões de escolha

múltipla, onde o participante poderia escolher mais de uma opção, uma vez que era intenção apenas obter respostas positivas ("sim") ou negativas ("não") em relação às questões propostas.

A primeira afirmação (P9) da terceira parte do inquérito diz respeito ao entendimento do participante em relação às preocupações das organizações em aspetos como os que seguem abaixo:

P9 – "Fazem parte das principais preocupações da organização onde trabalha, aspetos como:"

P9.1 Perda de dados relacionada com perda ou roubos de dispositivos;

P9.2 Software malicioso em dispositivos;

P9.3 Inconsistência nas soluções para proteção de dados em diferentes plataformas móveis;

P9.4 Ausência de soluções para proteção ou perda de dados através de dispositivos móveis;

P9.5 Ausência de segregação entre informações corporativas e utilizadores;

P9.6 Não possuem qualquer tipo de preocupação em relação as fragilidades em dispositivos móveis;

P9.7 Não conheço as políticas da minha empresa quanto a este tema;

P9.8 Outros

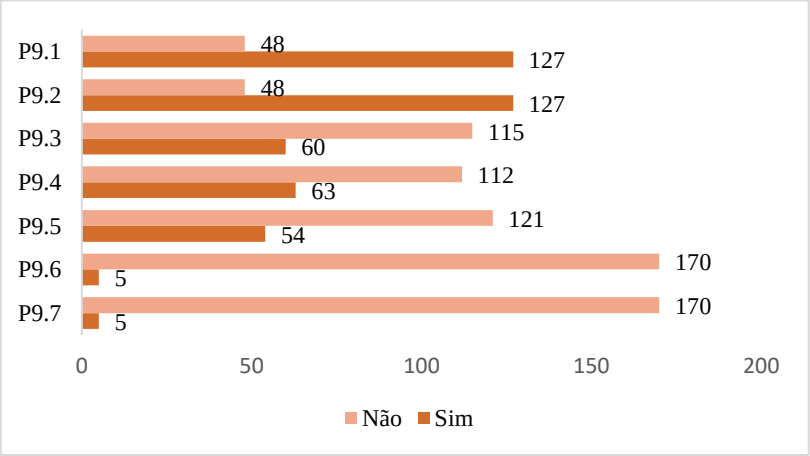


Figura 5: Principais preocupações das organizações

É possível encontrar semelhança na seleção das observações P9.1 e P9.2 entre o estudo realizado pela Deloitte (2013) e o presente estudo: cerca de 75% dos participantes do

estudo da organização indicaram fazer parte da preocupação das organizações bancárias fatores como perda de dados relacionada a perda ou roubo de dispositivos bem como *software* Malicioso, 72% dos participantes, com 127 seleções nestas duas observações.

Foi registada apenas uma observação na alternativa opção "Outros" com a indicação de que a organização tem como preocupação a "*fragilidade na proteção da transmissão eletrónica de dados e informação*".

A segunda afirmação (P10) da terceira parte diz respeito ao entendimento do participante em relação às principais políticas e ferramentas de segurança implementadas que estejam relacionadas com os dispositivos utilizados no âmbito da realização do trabalho de auditoria.

P10 - "A SROC onde trabalha possui políticas de segurança e ferramentas implementadas relacionadas a:"

P10.1 Telemóveis disponibilizados aos colaboradores;

P10.2 *Tablets* disponibilizados aos colaboradores;

P10.3 Computadores disponibilizados aos colaboradores;

P10.4 Uso pessoal de redes sociais (como, por exemplo, Instagram, Facebook ou Twitter)

P10.5 Uso profissional de plataformas de partilha de informações e sincronização (como, por exemplo, Google Drive ou Dropbox);

P10.6 Uso profissional de ferramentas tipo *Software as a Service* - SaaS (como, por exemplo, G-Suite ou Microsoft Office 365);

P10.7 Não conheço as políticas da minha empresa quanto a este tema;

P10.8 Outros

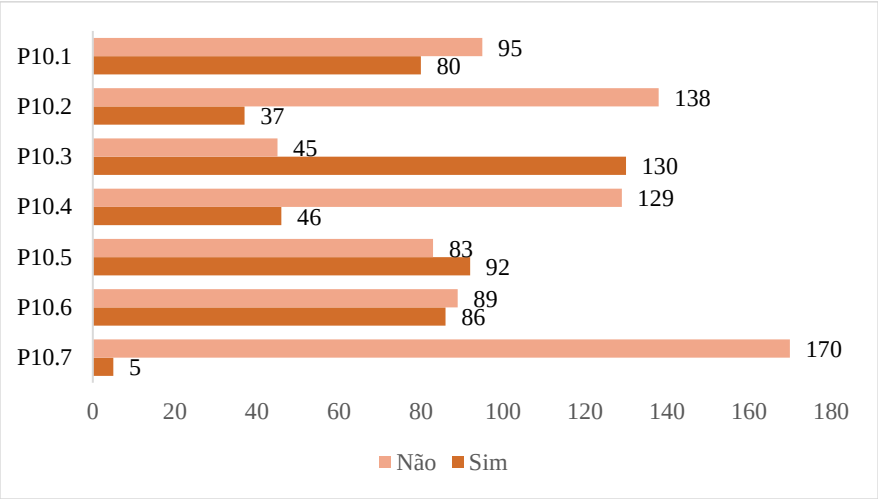


Figura 6: Principais políticas de Segurança da Informação

Nesta questão houve observações na opção "Outros", os indivíduos indicaram que as SROCs onde trabalham possuem políticas relacionadas a: *"backup de informação"*, *"armazenamento de informações em locais diferentes do escritório"* e *"criptografia de dados"*.

No entanto, de acordo com o entendimento de maioria dos participantes, as SROCs onde trabalham não possuíam PSIs relacionadas a dispositivos móveis (telemóveis ou *tablets*), em relação aos SaaS utilizados e também em relação ao uso de redes sociais, tendo, porém, quanto aos computadores disponibilizados aos colaboradores.

De forma a obter maior entendimento sobre as dimensões das organizações que responderam de determinada forma às opções desta questão, a Tabela 12 foi elaborada com destaque para as principais dimensões representadas nas respostas dos participantes: 1 a 10 colaboradores (56) e 1000+ colaboradores (58). Optou-se por apresentar os dados das restantes, entre 11 a 1000 colaboradores, (61) de maneira unificada.

Assim, conforme apresentado na Tabela 12, é possível perceber que grande parte dos participantes que desempenham suas atividades profissionais em organizações de dimensões maiores (1000+ colaboradores) têm conhecimento de que as entidades possuem PSIs relacionadas aos dispositivos móveis e SaaS utilizados, mas apenas 38% indicaram as alternativas que dizem respeito a PSIs em *tablets* e relacionadas com o uso de Redes Sociais.

A principal alternativa selecionada pelos colaboradores de organizações com menor dimensão (1 a 10 colaboradores) está relacionada às PSIs aplicadas aos "computadores disponibilizados pelas organizações". Esta também foi a principal alternativa assinalada

quando analisadas as respostas dos participantes que desempenham atividades nas organizações restantes. De notar que a % apresentada na tabela 12 se refere ao número total de respondentes em cada grupo: 1 a 10 colaboradores com 56 participantes, 1000+ colaboradores com 58 e Restantes com 61 respondentes. O número de respostas total é superior ao número de respondentes atendendo a que, cada participante, poderia assinalar várias possibilidades.

Tabela 12: Existência de PSIs em relação a dimensão das organizações

	Dimensão das organizações					
Pergunta	1 a 10 Colaboradores	%	1000+ Colaboradores	%	Restantes	%
P10.1	15	27%	47	81%	18	30%
P10.2	8	14%	22	38%	7	11%
P10.3	44	79%	49	84%	37	61%
P10.4	8	14%	22	38%	16	26%
P10.5	24	43%	40	69%	28	46%
P10.6	24	43%	36	62%	26	43%
P10.7	3	5%	0	0%	2	3%

A terceira afirmação (P11) da terceira parte diz respeito ao entendimento do participante em relação aos tipos de tecnologia associados às questões de segurança em dispositivos móveis.

P11 - "Que tipos de tecnologias estão presentes em questões de segurança de dados em dispositivos móveis (telemóveis, por exemplo):"

P11.1. Adotam bases de políticas de segurança de dispositivos, como palavras passe, bloqueio remoto e limpeza remota;

P11.2. Adotam sistemas de gestão de segurança (como *MobileIron* ou *AirWatch*) para garantir a proteção dos dados nos dispositivos;

P11.3 Infraestrutura de área de trabalho virtual para acesso do utilizador a dados corporativos em smartphones e tablets;

P11.4 Aplicações do tipo *Sandbox* para separar, nos dispositivos, informação corporativa da informação pessoal;

P11.5 Não adotam qualquer tipo de política para proteção de dados em dispositivos móveis;

P11.6 Não conheço as políticas da minha empresa quanto a este tema

Os resultados das respostas encontram-se na figura 8, verificando-se uma maior frequência de respostas assinaladas na questão P11.1 "Adotam bases de políticas de segurança de dispositivos, como palavras passe, bloqueio remoto e limpeza remota", com 67 respostas, embora apenas 52 e 46 assinalem, respetivamente, as opções P11.2. "Adotam sistemas de gestão de segurança (como *MobileIron* ou *AirWatch*) para garantir a proteção dos dados nos dispositivos" e P11.3 "Infraestrutura de área de trabalho virtual para acesso do utilizador a dados corporativos em *smartphones* e *tablets*".

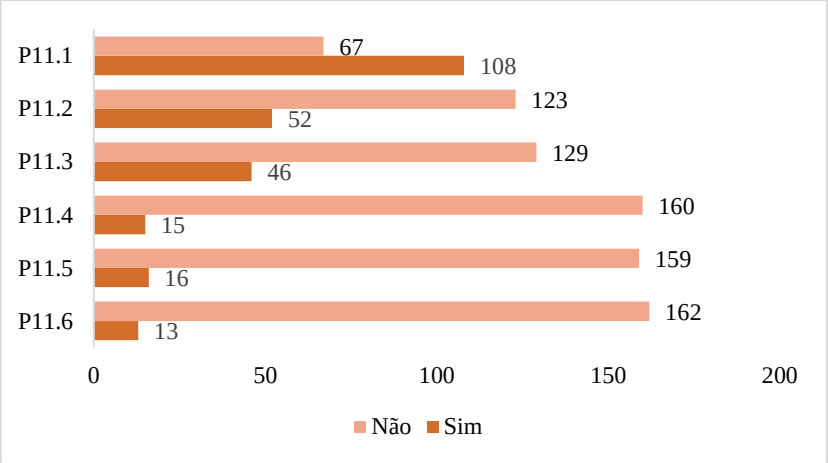


Figura 7: Tipos de tecnologias associadas a segurança de dados em dispositivos

Nesta afirmação, houve indivíduos que assinalaram a opção "Outros" e indicaram que nas SROCs onde trabalham existe presença de tecnologia em questões de segurança de: criptografia de dados e cópias de segurança de informação.

No entanto, de acordo com o entendimento de maioria dos participantes, as SROCs onde trabalham não possuíam tecnologias associadas a PSIs relacionadas a dispositivos móveis, com exceção à P11.1 (palavra passe, bloqueio de tela e limpeza remota).

De forma a obter maior entendimento sobre as dimensões das organizações que indicaram as opções para esta questão, a Tabela 13 foi elaborada com destaque para as principais dimensões representadas nas respostas dos participantes: 1 a 10 colaboradores (56) e 1000+ colaboradores (58). Optou-se, inicialmente, por apresentar os dados das restantes (61) de maneira unificada, tal como na Tabela 12, utilizando-se aqui o mesmo procedimento. No entanto, ao verificar-se o alfa de Cronbach isoladamente para P11.2, P11.3 e P11.4 obteve-se o valor de 0,623, no limar da aceitação para consistência interna dos itens, pelo que a Tabela 14 foi elaborada de modo a perceber as principais diferenças entre as respostas dos participantes de organizações com dimensões diferentes.

Tabela 13: Tecnologias para segurança em dispositivos móveis por dimensão das organizações

	Dimensão das organizações					
Pergunta	1 a 10 Colaboradores	%	1000+ Colaboradores	%	Restantes	%
P11.1	39	70%	37	64%	32	52%
P11.2	5	9%	31	53%	16	26%
P11.3	7	13%	26	45%	13	21%
P11.4	3	5%	8	14%	4	7%
P11.5	10	18%	1	2%	5	8%
P11.6	2	4%	6	10%	5	8%

Verifica-se, portanto, que as respostas para as questões supramencionadas variam, de acordo com a proporção por cada tamanho de organização. Em relação a P11.2, verifica-se maior opção por esta alternativa por parte de colaboradores que desempenham atividades em organizações de grande dimensão, mas que se equipara com a proporção de respostas de participantes de organizações com entre 51 a 100 colaboradores.

Tabela 14: Tecnologias para segurança em dispositivos móveis por dimensão, em detalhes

	Dimensão das organizações (número de colaboradores)											
P11	1 a 10	%	11 a 50	%	51 a 100	%	101 a 500	%	501 a 1000	%	1000+	%
P11.1	39	70%	16	57%	4	67%	8	67%	4	80%	37	64%
P11.2	5	9%	7	25%	3	50%	2	17%	4	80%	31	53%
P11.3	7	13%	5	18%	2	33%	3	25%	3	60%	26	45%
P11.4	3	5%	0	0%	1	17%	1	8%	2	40%	8	14%
P11.5	10	18%	5	18%	0	0%	0	0%	0	0%	1	2%
P11.6	2	4%	2	7%	0	0%	3	25%	0	0%	6	10%

A principal alternativa selecionada por todos os colaboradores, independente da dimensão das organizações está relacionada à P11.1. No entanto, participantes que exercem atividades profissionais em SROCs com 1000+ colaboradores assinalaram mais alternativas em relação ao uso de tecnologia associado aos dispositivos como PSIs implementadas pelas suas organizações, nomeadamente, "Adotam bases de políticas de segurança de dispositivos, como palavras passe, bloqueio remoto e limpeza remota", "Adotam sistemas de gestão de segurança (como *MobileIron* ou *AirWatch*) para garantir a proteção dos dados nos dispositivos" e possuem "Infraestrutura de área de trabalho virtual para acesso do utilizador a dados corporativos em *smartphones* e *tablets*.

A última afirmação (P12) da terceira parte do inquérito diz respeito ao entendimento do participante em relação aos planos para atualizações de políticas de segurança da informação. Diferente das outras afirmações da terceira parte do inquérito, para esta questão, foi apenas possível escolher uma das alternativas, atendendo que se consideram mutuamente exclusivas.

P12. "Quais são os planos da organização onde trabalha em relação a adoção de novas políticas de segurança de dados e informações?"

> i. A organização onde trabalho atualiza, constantemente, as atuais políticas e pretende implementar novas políticas nos próximos 12 meses;
>
> ii. A organização onde trabalho já possui políticas que foram recentemente atualizadas e não pretende implementar novas políticas nos próximos 12 meses;
>
> iii. A organização onde trabalho possui políticas de segurança que não foram atualizadas nos últimos 12 meses;
>
> iv. A organização onde trabalho não possui políticas de segurança;
>
> v. Não conheço as políticas da minha empresa quanto a este tema;
>
> vi. Outro;
>
> vii. S/R – Sem Resposta

A Figura 9 mostra que mais de 70 participantes (41%) afirmou que nas suas organizações fazem atualizações das suas políticas de Segurança da Informação constantemente, o que é um aspeto positivo e deixa a possibilidade do entendimento de que as SROCs investem tempo e capital nesta questão de importância. Apenas 14 (8%) participantes respondem que as SROCs onde trabalham não têm realizado, nos últimos 12 meses, atualizações nas políticas de SI (ii). No entanto, 25 (14%) respondentes assinalaram a opção que diz não ter conhecimento em relação as mesmas. Participantes que selecionaram a opção "Outros" 3 (2%) indivíduos indicaram que as SROCs onde trabalham estão a "*atualizar, neste momento, os todas as suas ferramentas informáticas, incluindo políticas de segurança*" e que, por ser uma SROC recente, "*estão a ser definidas as políticas*". Foram registadas 145 respostas para a P12.

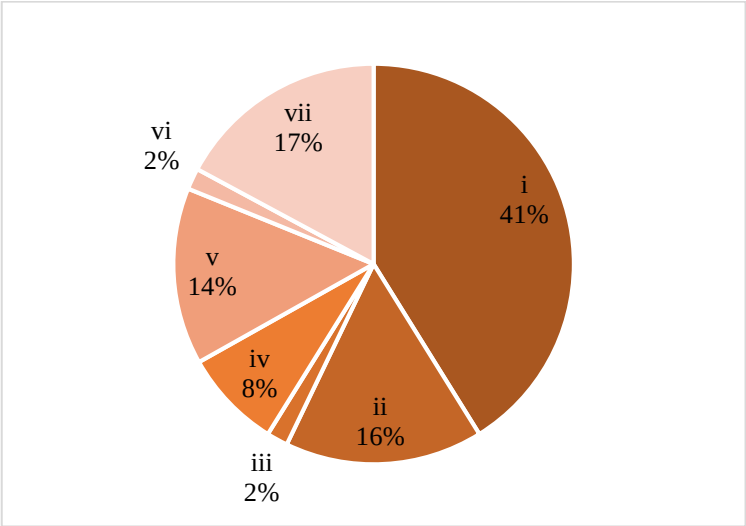


Figura 8: "Quais são os planos da organização onde trabalha em relação a adoção de novas políticas de segurança de dados e informações?"

Adicionalmente, elaborou-se a Tabela 15 onde foi possível perceber, ao nível dimensional das organizações, as afirmações selecionadas pelos participantes. (através da classificação por número de colaboradores em que as organizações se encontram). No que diz respeito a proporção da dimensão por respostas registadas. Foi possível verificar que a proporção de participantes que desempenham atividades em organizações de menor tamanho que assinalam a opção "i" não se distancia da proporção de participantes de organizações maiores, para a mesma opção.

Tabela 15: Dimensão das organizações e planos para novas políticas

Colaboradores	Afirmações disponíveis						
	i.	ii.	iii.	iv.	v.	vi.	Total Respostas
1 a 10 colaboradores	22	13	3	9	4	2	53
11 a 50 colaboradores	10	5	0	4	3	1	23
51 a 100 colaboradores	2	1	0	0	1	0	4
101 a 500 colaboradores	8	1	0	0	2	0	11
501 a 1000 colaboradores	4	0	0	0	0	0	4
1000+ colaboradores	26	8	0	1	15	0	50
Total Respostas	72	28	3	14	25	3	145

Não foi possível obter mais detalhes em relação às organizações onde os participantes trabalham, uma vez que não foi objetivo deste estudo saber com exatidão em que organizações é que os mesmos desempenham suas atividades. O único registo obtido foi através dos *e-mails* registados nas respostas (registado na OROC) e nem todos utilizam correio eletrónico profissional para tal. Ainda assim, foi possível verificar que existem registadas respostas de colaboradores de, pelo menos 60, organizações diferentes.

4.5 Como colaboradores tomam conhecimento sobre as PSIs

Esta quarta e última parte contém afirmações de forma a concluir sobre o entendimento do colaborador no que diz respeito às políticas de segurança adotadas nas SROCs onde trabalham, em especial sobre a forma como toma conhecimento acerca dessas mesmas políticas.com possibilidades de resposta em escala Likert (com as possibilidades 1- Discordo Totalmente, 2- Discordo parcialmente; 3- Não concordo, nem discordo; 4- Concordo parcialmente e 5 - Concordo plenamente).

P13. A organização onde trabalho…

P13.1 realiza formações (sessões presenciais ou através de e-*learning*) de maneira a evidenciar a importância da Segurança da Informação;

P13.2 faz questão de reforçar a importância da confidencialidade, entre outros aspetos de segurança, bem como restrição do uso de câmaras fotográficas (em telemóveis, por exemplo) dentro de suas instalações ou do cliente;

P13.3 faz questão de consciencializar os colaboradores para cuidados com uso de dispositivos vulgarmente designadas "*pendrives*" bem como plataformas de partilha de dados ou conversão de ficheiros (como, por exemplo, PDF em Excel);

P13.4 faz questão de consciencializar os colaboradores para cuidados com o bloqueio de telas de computadores, segurança do equipamento disponibilizado (computadores, mochilas) dentro de suas instalações ou no cliente;

P13.5 faz questão de consciencializar os colaboradores para cuidados ao utilizar fotocopiadoras, scanners e impressoras dentro de suas instalações (como, por exemplo, não deixar nos dispositivos documentos recém impressos, quer fisicamente, quer em memória);

P13.6 faz questão de consciencializar os colaboradores para cuidados com papéis com conteúdos confidenciais em cima da mesa de trabalho;

P13.7 faz questão de consciencializar os colaboradores para cuidados com a eliminação de documentos que contenham informações sigilosas sobre o próprio negócio ou negócios do cliente;

P13.8 A organização onde trabalho faz questão de consciencializar os colaboradores para cuidados com o acesso às suas instalações (como, por exemplo, utilização de cartão de acesso);

A Tabela 16 apresenta as respostas dos participantes em relação as afirmações em escala Likert. Para todas as afirmações foram registadas respostas na opção "concordo plenamente" acima de 50%. Desta maneira, é possível concluir que, de acordo com o entendimento dos participantes, as organizações onde desempenham suas atividades levam aos seus colaboradores o importante assunto relacionado às Políticas de Segurança da Informação (consciencializar os colaboradores). Ainda assim, dos 175 participantes do inquérito, 38 optaram por não responder a esta última parte do questionário, sendo número significativo ao comparar com as opções Discordo plenamente, parcialmente ou nem concordo nem discordo, uma vez que juntas não receberam um total de mais de 30 seleções. Em aspetos quantitativos, foi possível verificar que, entre as principais respostas em "Concordo plenamente", as principais indicações dos participantes estiveram relacionadas a: 1. Cuidados com bloqueio de telas de computadores e segurança do equipamento disponibilizado; 2. Cuidados com papeis que contenham informação confidencial em cima da mesa de trabalho; 3.Cuidados com a eliminação e descarte de documentos que contenham informação sigilosa.

Tabela 16 Perceção dos participantes quanto ao conhecimento das PSIs

Afirmação:	Discordo plenamente	Discordo parcialmente	Nem concordo, nem discordo	Concordo parcialmente	Concordo plenamente	**S/R - Sem Resposta**
P13.1	**9**	**12**	**14**	**29**	**72**	**38**
	7%	9%	10%	21%	53%	
P13.2	**3**	**9**	**12**	**34**	**78**	**38**
	2%	7%	9%	25%	57%	
P13.3	**2**	**7**	**10**	**35**	**82**	**38**
	1%	5%	7%	26%	60%	
P13.4	**2**	**3**	**3**	**39**	**89**	**38**
	1%	2%	2%	29%	65%	
P13.5	**3**	**5**	**11**	**49**	**68**	**38**
	2%	4%	8%	36%	50%	
P13.6	**2**	**3**	**3**	**40**	**88**	**38**
	1%	2%	2%	29%	65%	
P13.7	**0**	**5**	**3**	**41**	**87**	**38**
	0%	4%	2%	30%	64%	
P13.8	**5**	**7**	**15**	**30**	**79**	**38**
	4%	5%	11%	22%	58%	

4.6 Discussão dos Resultados

Do estudo efetuado, verificou-se que cerca de 32% dos participantes desempenham atividades em organizações de pequena dimensão, ou seja, SROCs que possuem entre 1 a 10 colaboradores, e 33% dos participantes indicam que trabalham em organizações de maior dimensão, tendo alguns referido a existência de mais de 1000 colaboradores em seu quadro, através da seleção da opção "1000+ colaboradores". Desta forma, os trabalhos e análises realizados no capítulo anterior foram executados de modo a cumprir com os objetivos definidos e relacionar a dimensão das organizações com o nível de políticas e práticas de segurança implementadas.

Através da revisão da literatura ficou clara a importância da implementação e prática de Políticas de Segurança no âmbito das SROCs de forma a mitigar riscos associados ao tratamento de dados e informação, bem como proteger a atividade e integridade da organização como um todo.

Do trabalho efetuado foi possível verificar que, da perceção dos participantes ao inquérito, as SROCs estão a investir em PSIs, tanto na atualização como implementação de novas PSIs, e fazem como que colaboradores tomem conhecimento das mesmas, para o bom funcionamento do negócio, tanto em organizações de menor, como de maior dimensão Relativamente a este ponto, foi possível constatar que os participantes respondem "Concordo Parcialmente" ou "Concordo Plenamente" relativamente à maioria das questões que foram colocadas, percebendo-se que as SROCs têm a preocupação de elaborar as PSIs, de as transmitir aos seus profissionais e de procurar garantir que esse conhecimento é explicito. Em todas as 8 possibilidades de boas práticas questionadas, os participantes responderam no sentido da concordância (ainda que parcial) entre 74% (relativamente à questão "*realiza formações (sessões presenciais ou através de e-learning) de maneira a evidenciar a importância da Segurança da Informação*") e 94% (correspondente a 3 respostas, nomeadamente, "*faz questão de consciencializar os colaboradores para cuidados com o bloqueio de telas de computadores, segurança do equipamento disponibilizado (computadores, mochilas) dentro de suas instalações ou no cliente*", "*faz questão de consciencializar os colaboradores para cuidados com papéis com conteúdos confidenciais em cima da mesa de trabalho*" e "*faz questão de consciencializar os colaboradores para cuidados com a eliminação de documentos que contenham informações sigilosas sobre o próprio negócio ou negócios do cliente*").

4.7 Políticas de Segurança da Informação: Proposta de boas práticas em SROCs

Tendo como principais objetos de trabalho informação e dados de seus clientes, as SROCs precisam investir conhecimento e realizar levantamentos acerca de seus principais riscos de maneira a definir e atualizar suas políticas de segurança de maneira constante. No âmbito do atual contexto tecnológico e de informação em que a sociedade vive, sabe-se que a segurança da informação é um grande desafio para as SROCs.

Após entendimento de suas vulnerabilidades e avaliação de seus riscos, as entidades definem diversas políticas de segurança de cumprimento obrigatório para um bom funcionamento e para que sua reputação seja mantida.

Através do presente estudo foram obtidos dados acerca das principais PSIs utilizadas por SROCs, de dimensão variada, em Portugal, partindo da perceção dos seus colaboradores. Desta forma, apresenta-se uma "compilação" de boas práticas que podem ser seguidas por organizações (SROCs) e que se encontra descrita abaixo.

a. Segurança Física da Informação

- Cursos de Formação (presenciais ou através de *e-learning*) que sensibilizem acerca de aspetos importantes como: papéis com informação sensível "perdidos" em impressoras bem como em dispositivos *flash USB*;
- Restrição de acesso por parte de terceiros a áreas que contenham dados ou informação sensíveis;
- Segurança associada a transporte, manuseio e utilização de dispositivos fornecidos para trabalho;
- Descarte de informação sensível em depósitos específicos para tal (destruição de material obsoleto ou papeis de trabalho);

b. Segurança Digital da Informação:

- Uso de criptografia em todo o armazenamento e fluxo de dados que estejam fora do perímetro de segurança (dispositivos móveis ou nuvem);
- Uso de VPN (*Virtual Private Network*) em todos os dispositivos móveis conectados a Internet, de maneira a garantir a segurança da conexão e dos dados;
- Limite de acesso a website que representem/apresentem ameaças;
- Utilização de plataformas autorizadas para conversão de ficheiros

- Uso de criptografia em *flash USB* ou plataformas de compartilhamento (*drives*);
- Bloqueio de ecrã de computadores ou telemóveis após um curto período de tempo;

c. Outros Aspetos Importantes

- Comunicação do Código de Conduta e Código de Ética distribuído e do conhecimento de a todos os colaboradores, bem como disponibilizar os mesmos para consultas em caso de eventual necessidade;
- Cláusulas de Confidencialidade na celebração de contratos de trabalho com novos colaboradores ou contratos para prestações de serviços;
- Conversas sobre informação sensível fora do escritório ou sala de reunião apropriada;
- Armazenamento apropriado de informação após projetos ou após utilização;

As SROCs devem estabelecer procedimentos e comunicá-los aos colaboradores de maneira a proteger suas informações físicas e digitais de maneira a mitigar risco de perda, dano ou roubo. Se possível, desenvolver guias ou cursos em *e-learning* para utilizadores de dispositivos disponibilizados como ferramentas de trabalho, nomeadamente, dispositivos móveis, como tablets, telemóveis e computadores portáteis, e dispositivos de armazenamento como *pen drive* (ou *flash USB*) e utilização de armazenamento na *cloud*.

CONCLUSÃO

Este estudo procurou preencher a lacuna da temática no âmbito do conhecimento das atuais Políticas de Segurança da Informação adotadas pelas SROCs no contexto da realização do trabalho dos auditores financeiros em Portugal.

Sendo os dados e a informação os principais ativos e objetos de trabalho do auditor financeiro, as organizações investem em diversos procedimentos que vão desde tecnologias de informação e mecanismos de segurança até formação específica na área da segurança da informação. Os Revisores levam em consideração a inovação tecnológica nas organizações para adaptarem os seus controlos e metodologias de trabalho à necessidade de proteger todo fluxo e conteúdo informacional.

Através da aplicação do inquérito aos profissionais que atuam com auditoria financeira, esta dissertação cumpre com seus objetivos, apresentando seus principais contributos, oportunidades para estudos futuros e limitações no âmbito da realização do trabalho.

Contributos do Estudo

Através da aplicação do questionário foi possível obter dados importantes acerca do atual contexto da Segurança da Informação no âmbito dos profissionais que atuam com auditoria financeira em Portugal, em especial em SROCs: principais políticas adotadas relacionadas ao uso de tecnologia, perspetivas para atualização e melhoria nas políticas de segurança, relação entre dimensão da SROC e suas PSIs, conhecimento e perceção dos profissionais quanto à forma como lhes é transmitido o conhecimento das políticas e da sua atualização. Para além de permitir conhecer a perceção dos respondentes, este estudo debruçou-se também na reflexão sobre a atual prática e situação da Segurança da Informação dentro das organizações do tipo SROCs em Portugal e sugere um conjunto de boas práticas como sugestão de implementação, em especial para as SROC que onde as PSIs estão em fase de implementação.

Estudos Futuros

Estudos relacionados com a segurança da informação no contexto das organizações estão a ser cada vez mais postos em prática, uma vez que o assunto se tem apresentado como muito relevante, principalmente após a implementação da RGPD, em 2018.

Neste sentido, há grandes possibilidades para trabalhos futuros com foco em alguns pontos pertinentes, como os que estão explicitados abaixo:

a. Análise do impacto da implementação do RGPD nas SROCs (o que mudou? O que permanece? Que dificuldades foram sentidas? Que oportunidades foram exploradas?);
b. Análise da evolução das políticas de segurança da informação nas SROCs antes e após o RGPD;
c. Em relação à análise estatística dos dados recolhidos nesta Dissertação, a possibilidade de uma abordagem complexa onde se utilizem técnicas como análise de *clusters* que permita compreender a forma a distribuição dos elementos do grupo.

Ainda, o presente estudo trata apenas das PSIs no âmbito de organizações que prestam determinados tipos de serviços que, no caso, Revisão Oficial de Contas. Portanto, fica como sugestão a seguinte temática:

d. A segurança da informação nas organizações portuguesas;
e. As PSIs dentro de organizações cotadas na bolsa de valores portuguesa;

Por último, o presente estudo trata de recolher dados através de aplicação de inquéritos direcionados a profissionais que trabalham diretamente com auditoria financeira. No sentido de recolher informações externas às SROCs (clientes, por exemplo), a aplicação de um novo inquérito pode ser feita a profissionais que trabalham em organizações que (obrigatoriamente) passam pelo processo de revisão de suas contas.

Limitações do Estudo

Entre as principais limitações deste estudo destacam-se:

a. Dificuldade de obtenção de respostas através de inquéritos para com profissionais que trabalham em auditoria financeira, uma vez que se encontram dispersos e possuem elevado fluxo de trabalho em determinadas épocas do ano, pelo que não se interessam, em grande maioria, em participar de questionários como este. O presente estudo teve uma taxa de resposta de 11%, o que leva a uma amostra reduzida, dificultando realização de modelos de análise dos resultados, como é comum em grande parte dos estudos realizados através de inquéritos;
b. Várias situações de inquiridos que não sabe/não responde, o que invalida o entendimento sobre alguns aspetos importantes.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, B. J. M. D. (2014). Manual de Auditoria Financeira–Uma análise integrada no risco. 1ª Edição, Escolar Editora–Lisboa.

Almeida, B. J. M. D. (2004). Auditoria e sociedade: o diálogo necessário. *Revista Contabilidade & Finanças*, *15*(34), 80-96.

BDO Portugal. RGPD – Audit & Assurance Services Policy Statement (2019). Retrieved from: https://www.bdo.pt/pt-pt/servicos/audit-assurance/rgpd-audit-assurance-services-policy-statement Acesso em 20-10-2019

Bonotto, P. V. (2010). As fraudes contábeis da Enron e Worldcom e seus efeitos nos Estados Unidos. Trabalho de Conclusão de Curso de Graduação (Faculdade de Ciências Econômicas - UFRGS)

Blanch Apostolou, Barbara; (2000); Sampling for internal Auditors; 2ª ed. IIA

Brickey, K. F. (2003). From Enron to WorldCom and beyond: Life and crime after Sarbanes-Oxley. Wash. ULQ, 81, 357.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empi...: EBSCOhost. *Journal of Computer Security*, *11*(11), 431–448. Retrieved from https://web-a-ebscohost-com.libproxy.smu.edu.sg/ehost/pdfviewer/pdfviewer?vid=1&sid=e13ea18f-2e81-45a7-b39f-3dea6201f87c%40sdc-v-sessmgr06 Acesso em 20-10-2019

Center for Audit Quality. 2014. "CAQ Member Alert: Cybersecurity and the External Audit."

CNBC (2019). Nearly three quarters of the world will use just their smartphones to access the internet by 2025. [online] p.1. Available at: https://www.cnbc.com/2019/01/24/smartphones-72percent-of-people-will-use-only-mobile-for-internet-by-2025.html Acesso em 20-10-2019

Clanchy, J. & Ballard, B. (2000). *Como escrever ensaios: um guia para estudantes*. Lisboa: Temas & Debates.

Collis, J., & Hussey, R. (2005). *Pesquisa em administração: um guia prático para alunos de graduação e pós-graduação*. Bookman.

COSO (2017) Enterprise Risk Management Integrating with Strategy and Performance https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

DAVENPORT, Thomas H. Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

Dias, C. (2000). *Segurança e auditoria da tecnologia da informação*. Axcel Books.

Duncan, B., & Whittington, M. (2014, September). Compliance with standards, assurance and audit: does this equal security?. In *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 77). ACM.

ENISA (2010). Threat Landscape Report 2010 – Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2010 Acesso em 20-10-2019

ENISA (2016). Threat Taxonomy – Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view Acesso em 20-10-2019

ENISA (2019). Threat Landscape Report 2018 – Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 Acesso em 20-10-2019

Excel, M. (2017). Excel 2016 da Microsoft – Software de Folhas de Cálculo _ Office. Retrieved September 17, 2019, from https://products.office.com/pt-pt/excel

Fávero, L. P. L., Belfiore, P. P., Silva, F. L. D., & Chan, B. L. (2009). Análise de dados: modelagem multivariada para tomada de decisões.

Grant Thornton (2019), Ataques cibernéticos causaram prejuízo de US$ 280 bilhões. (2019). Retrieved from https://www.grantthornton.com.br/grant-thornton-noticias/press-releases/2017/ataques-ciberneticos/ Acesso em 20-10-2019

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/JCS-2009-0398

Gouveia, L. B. (2016). Gestão Da Segurança Da Informação. *Faculdade de Ciência e Tecnologia Univ Fernando Pessoa*, *1*, 1–52. Retrieved from http://hdl.handle.net/10284/5954

Gouveia, L. B., & Ranito, J. (2007). Sistemas de informação de apoio à gestão.

Guy D., Carmichael D., Whittington R. (2001). Audit sampling: an introduction. 5ªEd John Wiley & Sons

Harris, S. 2006. Alphabet soup: Understanding standards for risk management and compliance. *Information Security Magazine*

Hendriksen, E. S., & Van Breda, M. F. (1999). Teoria da contabilidade; tradução de Antonio Zoratto Sanvicente. São Paulo: Atlas, 277-297.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information and Management*, *52*(3), 337–347. https://doi.org/10.1016/j.im.2014.12.006

IIA (2016). Assessing Cybersecurity Risk – Role of Three Lines of Defense. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/gtag-assessing-cybersecurity-risk.pdf Acesso em 20-10-2019

Iudícibus, S. D. (1995). *Conceitos econômico e contábil de lucro: simetrias e arritmias. RBC*: Revista Brasileira de Contabilidade, 24(96), 12-5.

IT Governance Institute COBIT 4.1 (2007). Retrieved from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Downloads.aspx. Acesso em 20-10-2019

ISACA (2012). CoBIT 5 for Information Security.

ISACA (2013). Leveraging and Securiting the Bring Your Own Device and Technology Approach. Retrieved from https://m.isaca.org/Journal/archives/2013/Volume-1/Documents/jol13v1-BYOD-in-the.pdf Acesso em 20-10-2019

ISACA (2013). BYOD Enterprise – A Holistic Approach. Retrieved from https://m.isaca.org/Journal/archives/2013/Volume-1/Documents/jol13v1-BYOD-in-the.pdf Acesso em 20-10-2019

ISACA (2014). Informatio Security Policies – What´s the point? Retrieved from http://m.isaca.org/chapters10/Lusaka/NewsandAnnouncements/Documents/IT-Security-Policies.pdf Acesso em 20-10-2019

ISACA (2016) Cybersecurity fundamentals glossary. Retrieved from https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf Acesso em 20-10-2019

ISACA (2019) State of Cibersecurity 2019: Current Trends in Attacks, Awareness and Governance. Retrieved from https://www.isaca.org/info/state-of-cybersecurity-2019/index.html Acesso em 20-10-2019

ISO 17799:2005 (2005). Retrieved from https://www.iso.org/standard/39612.html

ISO, A. N. (2005). IEC 17799: 2005: Tecnologia da informação–Técnicas de segurança–Código de prática para a gestão da segurança da informação. *Rio de Janeiro, Associação Brasileira de Normas Técnicas*.

Jamieson, S. (2004). Likert scales: how to (ab)use them. *Medical Education*, *38*(12), 1217–1218. https://doi.org/10.1111/j.1365-2929.2004.02012.x

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*, *84*(11), 6.

Li, H., No, W. G., & Boritz, J. E. (2016). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Ssrn*, 1–55. https://doi.org/10.2139/ssrn.2880928

Lovata, L. M. (1990). Audit Technology and the Use of Computer Assisted Audit Techniques. *Information Systems Journal*, *4*(2), 60–68. Retrieved from http://www.systems.wsu.edu/scripts/wsuall.pl?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=8746957&site=bsi-live

Luz, J. P. G. da. (2010). *Auditoria e Segurança das Informações Geradas por Sistemas Contábeis*. *1*, 1–86.

Martins, A. B., & Santos, C. A. S. (2005). Uma metodologia para implantação de um

sistema de gestão de segurança da informação. *JISTEM: Journal of Information Systems and Technology Management*, 2(2), 121-136.

No, Won Gyun, and Miklos A. Vasarhelyi. "Cybersecurity and continuous assurance." *Journal of Emerging Technologies in Accounting* 14.1 (2017): 1-12.

Nunnally, J.., & Bernstein, I. (1994). *Psychometric theory*. New York: McGraw-Hill.

PADOVEZE, C. L. (2002). A controladoria no planejamento operacional: modelo para determinação da estrutura do ativo. *Revista de Contabilidade do CRC/SP. São Paulo: Ano VI*, (20).

Pedrosa, I., Laureano, R., & Costa, C. J. (2015). Motivações dos auditores para o uso das Tecnologias de Informação na sua profissão: aplicação aos Revisores Oficiais de Contas. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (15), 101-118.

Pedrosa, I (2015). *CAATTs use: Determinants for individual acceptance.* Doctoral dissertation. ISCTE – Instituto Universitário de Lisboa. Retrieved from https://repositorio.iscte-iul.pt/handle/10071/10017

Piattini, M. (2000). *Auditing Information Systems*, Idea Group Publishing

dos Santos Pinheiro, J. M. (2017). Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. *Cadernos UniFOA*, *3*(5), 11-21.

do Prado Gusmão, J. A. (2017). AUDITORIA DOS SISTEMAS DE INFORMAÇÃO COM FOCO NOS CONTROLES DE RISCOS. *QUALIA: a ciência em movimento*, *3*(1), 75-93.

Pirta, R., & Strazdina, R. (2012). Assessing the need of information technology control environment establishment. Information Technology and Management Science, 15(1), 99-104.

Portugal é o segundo país no mundo com mais utilizadores atacados com spam e phishing. (2019). Retrieved from https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/portugal-e-o-segundo-pais-do-mundo-com-mais-utilizadores-atacados-com-spam-e-phishing acesso em 23-05-2019

Proactive Defense: Understanding the 4 Main Threat Actor Types. (2019). Retrieved from https://www.recordedfuture.com/threat-actor-types/

Santos, S. M. (2014). *Práticas de segurança da informação: um estudo de caso num centro hospitalar* (Doctoral dissertation, Instituto Politécnico do Porto. Instituto Superior de Contabilidade e Administração do Porto).

Sousa, Gonçalo V. e. (1998). Metodologia da investigação, redacção e apresentação de trabalhos científicos. 1ª ed. Porto: Civilização Editora.

Revista OROC (Teixeira 2017) acesso em 20-05-2019: http://www.oroc.pt/fotos/editor2/Revista/76/TI7.pdf

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Retrieved from: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN Acesso em 20-10-2019

The Global State of Information Security Survey 2018. Acesso em 03-09-2019. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (1991). Criteria for Scale Selection and Evaluation. In J. P. Robinson, P. R. Shaver, & L. S. B. T.-M. of P. and S. P. A. Wrightsman (Eds.) (pp. 1–16). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-590241-0.50005-8

RGPD - Audit & Assurance Services - Policy Statement. (2019). Retrieved from https://www.bdo.pt/pt-pt/servicos/audit-assurance/rgpd-audit-assurance-services-policy-statement Acesso em 20-10-2019

A proteção de dados ao abrigo do RGPD (2019) Retrieved from: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm Acesso em 20-10-2019

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4

Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems*, *25*(1), 185–211. https://doi.org/10.2308/jis.2011.25.1.185

APÊNDICES

APÊNDICE 1. Estrutura geral do questionário aplicado

1. Questões relacionadas a informação do respondente
   1.1. Número de anos de experiência profissional relacionada a auditoria:
   1.2. Atual cargo na organização onde trabalha;
   1.3. Membro da OROC (S/N);
2. Questões relacionadas a organização onde trabalha
   2.1. Qual segmento de mercado ou área de atuação em que prestam serviços (auditam), por exemplo: *financial services* (banca, seguros), indústrias e outros serviços;
   2.2. Número aproximado de colaboradores que a organização possui;
   2.3. Se a organização em questão está presente em outros países para além de Portugal;
3. Questões acerca das políticas de segurança que da SROC onde o profissional atua
   3.1. Quais são as principais preocupações em relação às fragilidades na segurança em dispositivos móveis;
   3.2. Se existem ferramentas implementadas relacionadas a dispositivos móveis, uso de redes sociais, uso de *"Softwares* como serviços", plataforma de compartilhamento de informações;
   3.3. Tipos de tecnologias presentes em questões de segurança de dados em dispositivos móveis;
   3.4. Quais são os planos da organização em relação adoção de novas políticas e manutenção das atuais implementadas
4. Afirmações acerca do entendimento do colaborador em relação as políticas implementadas (em escala Likert, de 1 a 5, com afirmações seguintes: concordo plenamente, concordo parcialmente, nem concordo e nem discordo, discordo parcialmente, discordo totalmente);
   4.1. "A organização onde trabalho realiza formações (sessões presenciais ou através de e-learning) de maneira a evidenciar a importância da Segurança da informação";
   4.2. "A organização onde trabalho faz questão de reforçar a importância da confidencialidade, entre outros aspetos de segurança, bem como a utilização de câmaras fotográficas (de telemóveis, por exemplo) dentro de suas instalações ou do cliente";

4.3. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com o uso de dispositivos Flash USB bem como plataformas de compartilhamento de dados ou conversão de ficheiros em outras extensões;

4.4. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com o bloqueio de telas de computadores, segurança do equipamento disponibilizados (computadores, mochilas) dentro de suas instalações ou no cliente";

4.5. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados ao utilizar fotocopiadoras, scanners e impressoras dentro de suas instalações";

4.6. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com papeis de conteúdo confidencial em secretárias";

4.7. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com descarte de materiais que contenham informações sigilosas sobre a própria organização ou sobre o cliente";

4.8. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com o acesso às suas instalações (utilização de cartão de segurança, abertura de portas a terceiros sem autorização de superiores)";

4.9. "De maneira geral, acredito ter conhecimento sobre as políticas de segurança da informação que são aplicadas na organização onde trabalho".

APÊNDICE 2. Questionário (versão para impressão)

Bem-vindo ao estudo sobre Segurança da Informação em SROCs. Meu nome é Isadora Lima e desde já agradeço o seu tempo e interesse relativamente a esta pesquisa.

Este inquérito foi elaborado com intuito de recolher dados acerca das práticas e políticas de segurança de informação (incluindo cibersegurança) adotadas por SROCs em Portugal, no âmbito da dissertação de Mestrado em Auditoria Empresarial e Pública do Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra.

Irá encontrar uma série de questões de carácter profissional e também sobre a organização em que atua profissionalmente. É muito importante que as responda com a intenção de fornecer informações que remetam ao máximo a realidade do assunto em questão.

O inquérito estará disponível até o dia 12 de agosto. A sua participação é muito importante para este estudo!

Os dados recolhidos serão utilizados apenas no âmbito deste estudo. Não serão efetuadas referências a dados considerados individualmente, nomeadamente, dados pessoais, profissionais ou organizacionais.

Agradeço também o preenchimento completo do questionário de forma a garantir a coerência da análise. As questões tomarão cerca de 7 minutos do seu tempo.

Muito obrigada pela sua Participação!

Isadora Lima
Aluna do 2.º Ano
Mestrado em Auditoria Empresarial e Pública do Instituto Superior de Contabilidade e Administração de Coimbra
Instituto Politécnico de Coimbra

Existem 15 perguntas neste inquérito

Um pouco mais sobre si...

Estas primeiras questões estão direcionadas para obtenção de informações de carácter profissional do Revisor Oficial de Contas (ROC) ou profissional que trabalha com auditoria financeira em uma SROC.

1 [1]Número de anos de experiência profissional relacionada com auditoria financeira: *

Por favor, escreva aqui a sua resposta:

Responder com números a quantidade de anos de experiência profissional relacionada a auditoria financeira

2 [4]Idade, em anos *

Por favor, escreva aqui a sua resposta:

Responder com números anos completos em 31-12-2018

3 [5]Género

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Feminino
- ○ Masculino

4 [2]Atual posição hierárquica na organização onde desempenha suas atividades profissionais* *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Assistente (estagiário) ou equivalente
- ○ Auditor junior ou equivalente
- ○ Auditor senior ou equivalente
- ○ Gerente (supervisor) ou equivalente
- ○ Diretor ou equivalente
- ○ Sócio

Baseado em uma estrutura hierárquica típica de uma sociedade de auditores, de acordo com Almeida (2014) em *Manual de Auditoria Financeira: Uma análise integrada baseada no risco. Portugal: Escolar Editora.*

5 [3]É Revisor Oficial de Contas (ROC)? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sim
- ○ Não

Um pouco mais sobre a organização onde trabalha...

Algumas questões sobre a organização onde trabalha relacionadas a dimensão e segmento de negócios

6 [1]Qual segmento de mercado ou áreas para as quais a organização onde trabalha presta serviços de auditoria / revisão oficial de contas? *

Por favor, seleccione **todas** as que se aplicam:

- ☐ Serviços Financeiros (como, por exemplo, banca ou seguradoras)
- ☐ Indústria de Produção (como, por exemplo, químicos, papel e celulose, tecnologia, informática)
- ☐ Outros Serviços (como, por exemplo energia, turismo, entretenimento)
- ☐ Outro: _____

7 [2]Quantos colaboradores (aproximadamente) a organização onde realiza suas atividades profissionais possui? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ 1 - 10 colaboradores
- ○ 11 - 50 colaboradores
- ○ 51 – 100 colaboradores
- ○ 101 - 500 colaboradores
- ○ 501 - 1000 colaboradores
- ○ 1000+ colaboradores

8 [3]A organização onde realiza atividades profissionais está presente em outros países, para além de Portugal? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ Sim
- ○ Não

Em relação as Políticas de Segurança da Informação na organização onde trabalha

Selecione as alternativas das questões de acordo com o seu entendimento em relação às políticas de segurança da informação adotadas pela organização onde trabalha:

9 [1]Fazem parte das principais preocupações da organização onde trabalha (em relação a fragilidades na segurança em dispositivos móveis) aspectos como: *

Por favor, seleccione **todas** as que se aplicam:

- ☐ Perda de dados relacionada com perda ou roubos de dispositivos
- ☐ Software malicioso em dispositivos
- ☐ Inconsistência nas soluções para proteção de dados em diferentes plataformas móveis
- ☐ Ausência de soluções para proteção ou perda de dados através de dispositivos móveis
- ☐ Ausência de segregação entre informações corporativas e utilizadores
- ☐ Não possuem qualquer tipo de preocupação em relação as fragilidades em dispositivos móveis
- ☐ Não conheço as políticas da minha empresa quanto a este tema
- ☐ Outro: _____

10 [2]A SROC onde trabalha possui políticas de segurança e ferramentas implementadas relacionadas a: *

Por favor, seleccione **todas** as que se aplicam:

- ☐ Telemóveis disponibilizados aos colaboradores
- ☐ Tablets disponibilizados aos colaboradores
- ☐ Computadores disponibilizados aos colaboradores
- ☐ Uso pessoal de redes sociais (como, por exemplo, Instagram, Facebook ou Twitter)
- ☐ Uso profissional de plataformas de partilha de informações e sincronização (como, por exemplo, Google Drive ou Dropbox)
- ☐ Uso profissional de ferramentas tipo Software as a Service - SaaS (como, por exemplo, G-Suite ou Microsoft Office 365)
- ☐ Não conheço as políticas da minha empresa quanto a este tema
- ☐ Outro: ____

11 [3]Que tipos de tecnologias estão presentes em questões de segurança de dados em dispositivos móveis (telemóveis, por exemplo): *

Por favor, seleccione **todas** as que se aplicam:

- ☐ Adotam bases de políticas de segurança de dispositivos, como palavras passe, bloqueio remoto e limpeza remota
- ☐ Adotam sistemas de gestão de segurança (como MobileIron ou AirWatch) para garantir a proteção dos dados nos dispositivos
- ☐ Infraestrutura de área de trabalho virtual para acesso do utilizador a dados corporativos em smartphones e tablets
- ☐ Aplicações do tipo Sandbox para separar, nos dispositivos, informação corporativa da informação pessoal
- ☐ Não adotam qualquer tipo de política para proteção de dados em dispositivos móveis
- ☐ Não conheço as políticas da minha empresa quanto a este tema
- ☐ Outro: ____

12 [4]Quais são os planos da organização onde trabalha em relação a adoção de novas políticas de segurança de dados e informações? *

Por favor, seleccione **apenas uma** das seguintes opções:

- ○ A organização onde trabalho atualiza, constantemente, as atuais políticas e pretende implementar novas políticas nos próximos 12 meses
- ○ A organização onde trabalho já possui políticas que foram recentemente atualizadas e não pretende implementar novas políticas nos próximos 12 meses
- ○ A organização onde trabalho possui políticas de segurança que não foram atualizadas nos últimos 12 meses.
- ○ A organização onde trabalho não possui políticas de segurança
- ○ Não conheço as políticas da minha empresa quanto a este tema
- ○ Outro ____

Em relação as políticas de segurança adotadas pela organização onde trabalha

Selecione as alternativas com as quais mais se identifica de acordo com as afirmações abaixo de tomando como base seu entendimento em relação às políticas de segurança da informação adotadas pela organização onde trabalha:

13 [1]A organização onde trabalho... *

Por favor, seleccione uma resposta apropriada para cada item:

	Concordo plenamente	Concordo parcialmente	Nem concordo, nem discordo	Discordo parcialmente	Discordo plenamente
realiza formações (sessões presenciais ou através de e-learning) de maneira a evidenciar a importância da Segurança da Informação	○	○	○	○	○
faz questão de reforçar a importância da confidencialidade, entre outros aspetos de segurança, bem como restrição do uso de câmaras fotográficas (em telemóveis, por exemplo) dentro de suas instalações ou do cliente	○	○	○	○	○
faz questão de consciencializar os colaboradores para cuidados com uso de dispositivos vulgarmente designadas "pen drives" bem como plataformas de partilha de dados ou conversão de ficheiros (como, por exemplo, PDF em Excel)	○	○	○	○	○
faz questão de consciencializar os colaboradores para cuidados com o bloqueio de telas de computadores, segurança do equipamento disponibilizado (computadores, mochilas) dentro de suas instalações ou no cliente	○	○	○	○	○

	Concordo plenamente	Concordo parcialmente	Nem concordo, nem discordo	Discordo parcialmente	Discordo plenamente
faz questão de consciencializar os colaboradores para cuidados ao utilizar fotocopiadoras, scanners e impressoras dentro de suas instalações (como, por exemplo, não deixar no dispositivo documentos recém fotocopiados ou impressos, quer fisicamente, quer em memória)	○	○	○	○	○
faz questão de consciencializar os colaboradores para cuidados com papéis com conteúdos confidenciais em em cima da mesa de trabalho	○	○	○	○	○
faz questão de consciencializar os colaboradores para cuidados com a eliminação de documentos que contenham informações sigilosas sobre o próprio negócio ou negócios do cliente	○	○	○	○	○
A organização onde trabalho faz questão de consciencializar os colaboradores para cuidados com o acesso às suas instalações (como, por exemplo, utilização de cartão de acesso)	○	○	○	○	○

14 [2]De maneira geral, acredito ter conhecimento sobre as políticas de segurança da informação que são aplicadas na organização onde trabalho *

Por favor, seleccione **apenas uma** das seguintes opções:

○ Sim

○ Não

APÊNDICE 3. Convite de participação

Exmo Sr. (a) Dr. (a) {FIRSTNAME},

Desde já agradeço a sua atenção e disponibilidade para a leitura deste, bem como para a resposta a este questionário.

Esta mensagem surge na sequência do seu endereço de correio eletrónico pertencer aos registos da Ordem dos Revisores Oficiais de Contas, na seção de informações sobre Revisores Oficiais de Contas em atividade.

O inquérito é intitulado de:

"{SURVEYNAME}"

Clique aqui para aceder ao inquérito:
{SURVEYURL}

Enquadramento do trabalho efetuado para a dissertação

O meu projeto de dissertação envolve um estudo sobre a Segurança da Informação nas SROCs, de maneira a verificar a prática e políticas de segurança dentro das organizações, em vias de garantir a segurança necessária e a mínima exposição ao risco. Ainda, com este estudo pretende-se evidenciar aspetos positivos consequentes da implementação da gestão de segurança da informação dentro das SROCs.

Assim, este inquérito destina-se a colaboradores que exerçam atividade profissional em auditoria financeira, e serve de base para recolha de dados relacionados às políticas de segurança adotadas no atual contexto das SROCs.

Neste sentido, o seu contributo, o qual desde já muito agradeço, é fundamental.

Com os melhores cumprimentos,

Isadora Lima, aluna 2º ano do mestrado em Auditoria Empresarial e Pública no ISCAC-IPC.

Nota sobre a privacidade do processo de recolha de dados

Não serão efetuadas referências a dados considerados individualmente, nomeadamente, dados pessoais, profissionais ou organizacionais. Embora alguns questionários possuam um código associado, esta funcionalidade é apenas utilizada para a gestão das respostas já efetuadas e não para qualquer análise individual.

Se não quer participar deste inquérito e não deseja receber mais convites clique p.f. na seguinte ligação:

{OPTOUTURL}

APÊNDICE 4. Lembrete para participação no inquérito

Caro(a) {FIRSTNAME}

Recentemente, foi convidado a participar num inquérito e gostaríamos de relembrar que o mesmo ainda se encontra disponível, caso queira tomar parte dele. A sua resposta é fundamental para a prossecução deste estudo. O tempo médio de resposta é de 8 minutos.

Clique aqui para aceder ao inquérito:
{SURVEYURL}

Breve descrição do estudo

O meu projeto de dissertação envolve um estudo sobre a Segurança da Informação nas SROCs, de maneira a verificar a prática e políticas de segurança dentro das organizações, em vias de garantir a segurança necessária e a mínima exposição ao risco. Ainda, com este estudo pretende-se evidenciar aspetos positivos consequentes da implementação da gestão de segurança da informação dentro das SROCs.

Assim, este inquérito destina-se a colaboradores que exerçam atividade profissional em auditoria financeira, e serve de base para recolha de dados relacionados às políticas de segurança adotadas no atual contexto das SROCs.

Neste sentido, o seu contributo, o qual desde já muito agradeço, é fundamental.

Com os melhores cumprimentos,

Isadora Lima, aluna do 2º ano do Mestrado em Auditoria Empresarial e Pública no ISCAC-IPC

Nota sobre a privacidade do processo de recolha de dados

Não serão efetuadas referências a dados considerados individualmente, nomeadamente, dados pessoais, profissionais ou organizacionais. Embora alguns questionários possuam um código associado, esta funcionalidade é apenas utilizada para a gestão das respostas já efetuadas e não para qualquer análise individual.

Se não quer participar deste inquérito e não deseja receber mais convites clique p.f. na seguinte ligação:
{OPTOUTURL}

APÊNDICE 5. Confirmação de participação

Caro(a) {FIRSTNAME},

Este email confirma que completou o inquérito
intitulado {SURVEYNAME} e que as suas respostas foram gravadas.
Agradecemos a sua participação.

Se tiver outras perguntas relacionadas com este email, por favor,
contacte {ADMINNAME} através do endereço
electrónico {ADMINEMAIL}.

Com os melhores cumprimentos,

{ADMINNAME}