A Segurança da Informação nas Sociedades de Revisores Oficiais de Contas Portuguesas

Information Security on Portuguese Statutory Auditors firms

Isadora Lima
Coimbra Business School | ISCAC, Polytechnic of Coimbra
Coimbra, Portugal
isadorarclima@gmail.com

Isabel Pedrosa
Coimbra Business School | ISCAC, Polytechnic of Coimbra
Instituto Universitário de Lisboa (ISCTE-IUL) ISTAR-IUL, Portugal
ipedrosa@iscac.pt

Sónia Rito
Coimbra Business School | ISCAC, Polytechnic of Coimbra
Coimbra, Portugal
srito@iscac.pt

Resumo — **Sendo a informação gerada pelos clientes de Sociedades de Revisores Oficiais de Contas (SROCs) um dos principais objetos de trabalho do auditor financeiro, é importante que existam Políticas de Segurança da Informação (PSIs) eficientes, dada a necessidade da confidencialidade e sigilo no âmbito de seu tratamento. Através de um inquérito, este estudo aborda esta importante questão, cumprindo objetivos definidos através da avaliação do atual cenário das SROCs no âmbito das PSIs aplicadas, independente da dimensão das organizações. O presente estudo apresenta contribuições significativas acerca do atual contexto da Segurança da Informação no âmbito de profissionais que atuam diretamente com auditoria financeira: principais políticas adotadas relacionadas com o uso da 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 de Segurança da Informação; Auditoria Financeira; SROC.

Abstract — **Since clients' information used by audit firms 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. Using an online questionnaire, this study addresses this important question by assessing the current scenario of the audit firms within the scope of applied PSIs, regardless of the size of the organizations. This study 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: main policies adopted related to the use of technology, perspectives for updates and improvement in information security policies and the relationship between the dimension of Statutory Auditors' firms and PSIs.**

Keywords – Audit, Information Scurity, Cybersecurity, Information Security Policies, Financial Audit; Statutory Auditors Firms.

I. INTRODUÇÃO

A qualidade da informação e a amplitude de conhecimentos pessoais e organizacionais são decisivos no futuro dos negócios das organizações [1]. No âmbito do processo de globalização, o qual ganhou 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 a adoção de Políticas de Segurança da Informação (PSIs) revelam-se de extrema importância para todas as organizações devido ao aumento do fluxo informacional consequente desta globalização. Um dos fatores mais importantes na proteção da informação e seus elementos básicos assenta na definição de boas bases de uma gestão eficaz da segurança da informação.

No âmbito das Sociedades de Revisores Oficiais de Contas (SROCs) o tema acaba ainda por ser mais delicado, dado que os profissionais desta área trabalham com informação confidencial e sensível dos seus clientes, cuja divulgação indevida pode ter consequências nocivas. A importância da segurança da informação proporcionou novos desafios para auditores financeiros [2]. Para garantir que todo o conteúdo informacional gerado e adquirido junto das organizações se encontra protegido de diferentes tipos de ataques ou acontecimentos adversos, os auditores financeiros investem numa série de procedimentos que vão desde a utilização de tecnologias de informação e mecanismos de segurança até à formação específica na área da segurança da informação.

Através de um inquérito aplicado a profissionais que atuam diretamente em auditoria financeira, foram obtidas informações acerca da atual prática relacionada com PSIs no contexto das SROCs. Sendo a abordagem principal deste estudo um tema de extrema importância para o cotidiano de entidades de auditoria financeira, o resultado deste estudo por si só acaba por se tornar um contributo significativo para o tema em Portugal.

Na próxima seção será apresentada uma breve revisão de literatura, de maneira a contextualizar aspetos da profissão de auditor financeiro e atual realidade da Segurança da Informação. A terceira seção trata sobre a metodologia de trabalho e elaboração do inquérito aplicado. Os resultados serão discutidos e analisados na quarta seção, seguidos de alguns exemplos de

boas práticas e sugestões de PSIs para entidades de auditoria financeira.

II. Revisão da literatura

A. A auditoria financeira

A auditoria surge como 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 [3]. Ao longo do tempo, a finalidade e procedimentos de trabalho sofreram alterações. Até finais do século XIX, a deteção de fraude era aceite como o principal objetivo da realização de auditoria sendo requerido aos auditores que conduzissem seus trabalhos com razoável destreza para atingir esse fim [4]. Posteriormente, normas de auditoria passaram a dar suporte aos profissionais, de modo que a finalidade do seu trabalho passou a ser assegurar e garantir (*assurance*) a credibilidade dos relatórios financeiros emitidos pela gestão de uma organização. Já no século XXI, uma quebra de confiança no mercado de capitais em consequência de falência de grandes organizações devido a fraudes financeiras leva o Governo norte-americano a publicar a Lei Sarbanes Oxley (SOX), a qual reforça a necessidade de independência e discernimento crítico entre os profissionais de auditoria e as organizações para as quais prestam serviços. Apesar da SOX ser aplicada apenas a organizações com valores mobiliários admitidos à cotação nos Estados Unidos, teve um forte impacto global na profissão de auditor financeiro a qual se tornou muito mais regulamentada e sujeita a supervisão de organismos quasi-governamentais [4].

Nos dias atuais, os auditores utilizam tecnologias de informação na realização de tarefas anteriormente manuais, aumentando deste modo a eficiência do seu trabalho [5]. A utilização de instrumentos informatizados tornou-se hoje essencial para o processo de auditoria, sendo indispensável para o desempenho da profissão. Podemos ver a sua influência a diferentes níveis, tais como, no processo de amostragem muitas vezes fundamental numa abordagem substantiva [6] [7], ou mesmo no suporte aos processos de gestão e estratégico das organizações produzindo informações vitais para as organizações [8]. As CAATTs (*Computer-assisted Audit Tools and Techniques*) são ferramentas que auxiliam o trabalho de auditoria e, desde que utilizadas de forma correta, podem aumentar a eficiência, a eficácia, a produtividade e o trabalho colaborativo, diminuindo não só o tempo gasto com uma tarefa como também a ocorrência de erros [9]. Como ferramentas deste género: folhas de cálculo ou planilhas eletrónicas, DRAI (Dossier de revisão/auditoria informatizado), IDEA (*Interactive Data Extraction and Analysis)* e ACL (*Audit Command Language*).

No entanto, a tecnologia da informação está também relacionada a novos riscos no âmbito do armazenamento de informação confidencial que acrescentam novas variáveis ao planeamento e execução de um trabalho de auditoria: os riscos associados à produção de informação em computadores criam a necessidade dos auditores pesquisarem como identificar os riscos nos ambientes organizacionais de forma a conseguirem mitigá-los e comunicá-los a sua própria gestão [2].

B. A segurança da informação

Sendo a informação um pilar para a continuidade de qualquer organização, nomeadamente SROCs, é preciso garantir a segurança desse ativo, estabelecendo-se controlos cada vez mais sofisticados para preservar a informação contra situações adversas, quer as mesmas aconteçam intencionalmente ou não [10]. O ISACA (*Information Systems Audit and Control Association*) realça que a segurança da informação "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)"* [11]. Adicionalmente pode também ser considerada como o conjunto de medidas que protege não só a informação das organizações, mas também os sistemas de informação de acessos não autorizados, divulgação, interrupção e modificação [12]. Assim, o objetivo da segurança da informação é proteger de forma adequada os ativos de informação de modo a assegurar a continuidade do negócio, minimizando potenciais perdas que possam vir a ocorrer [13]. A correta apresentação e aplicação de controlos para a segurança da informação garante a credibilidade da mesma e das organizações sendo, na atualidade, um requisito praticamente obrigatório para tal.

A política de segurança deve ser apoiada em recursos tecnológicos em complemento de conscientização e formação de colaboradores no âmbito do uso eficiente e responsável das componentes da informação [1]. Note-se que, no âmbito das organizações atuais, incluindo SROCs, é muito comum o uso de correio eletrónico, redes sociais, e dispositivos como *Flash* USB que permitem partilha rápida e "despreocupada" de informação sensível e relevante para as organizações [13], assim como a utilização dos seus próprios dispositivos (computadores e *smartphones*) pelos colaboradores [14]. Estas rotinas reforçam a necessidade de definição de PSIs que lidem com estes desafios, assim como uma forte sensibilização dos envolvidos.

Note-se que, em 2010, o Relatório de Cenários de Ameaças à Segurança da Informação, emitido pelo ENISA (European Union Agency for Network and Information Security), organismo que tem por objetivo garantir alto nível de segurança em redes de informação da Europa, realçava que "os *smartphones* serão os dispositivos mais comuns para acesso à *internet*" [15]. Passados 10 anos, é possível comprovar essa estimativa. No Relatório de Cenários Ameaças à Segurança da Informação de 2018 [16], a ENISA listou ações de mitigação das principais ameaças, com destaque para: (1) Uso de encriptação em todo armazenamento e fluxo de informação que se encontram fora do perímetro de segurança (dispositivos móveis, serviços na nuvem); (2) Imposição de limite de acesso à áreas com informação ou equipamentos sensíveis; (3) Implementação de políticas de segurança física, integrada com dispositivos móveis; (4) Elaboração de guias de boas práticas.

C. A segurança da informação nas SROCs

O processo de definição das PSIs no âmbito das SROCs não se diferencia em relação ao das demais entidades. De maneira a determinar quais são as PSIs mais adequadas à sua organização, o órgão de gestão deve procurar identificar as vulnerabilidades a que a mesma está exposta. Para tal pode apoiar-se em análises de risco [13] e investigações cuidadosas aos sistemas e ambientes, procurando conhecer o que poderá ser danoso ao fluxo informacional. Depois de identificados os riscos e definidas as PSIs, torna-se imperativo definir a sua correta implementação através de um manual ou guia corporativo [17].

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. Sendo a informação gerada pelos clientes das SROCs um dos principais *inputs* do trabalho de auditores financeiros, é de grande importância a existência de PSIs eficientes que garantam o cumprimento dos deveres de confidencialidade e privacidade a que os ROC estão obrigados [18].

A proteção de informação nas SROCs não é só uma preocupação, mas uma obrigação prevista no normativo de auditoria. A ISQC 1 (*International Standard on Quality Control)*, que visa assegurar a garantia de qualidade no trabalho das empresas de auditoria em conjunto com as normas internacionais de auditoria, refere expressamente que "a firma deve estabelecer políticas e procedimentos concebidos para manter a confidencialidade, custódia segura, integridade, acessibilidade e recuperabilidade da documentação do trabalho" [19]. Ou seja, o sistema de controlo de qualidade a implementar nas SROCs deve abranger impreterivelmente políticas relacionadas com a segurança da informação.

Na Tabela 1 apresentam-se quatro tipos de cibercrime que podem ameaçar as organizações e os seus possíveis impactos numa SROCs (baseado no estudo do Record Future, 2016) [20].

Tabela 1: Tipos de ameaça e consequências para SROC

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.
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.
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, existe o risco de que colaboradores insatisfeitos com as organizações realizem esquemas para prejudicar as mesmas.

Em Portugal, estão a crescer os ataques com intenção de obter vantagens económicas, tendo-se verificado um aumento exponencial dos casos relacionados com extorsão cibernética (*ransomware)* que tomam poder de bases de dados e/ou de informação confidencial dos Revisores Oficiais de Contas (ROCs) e realizam pedidos de resgate ou outras exigências de pagamento para a sua recuperação [19]. 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 [21] [22] [23] [24] [25].

III. METODOLOGIA DE TRABALHO

A metodologia de investigação definida para o estudo foi a aplicação de um inquérito por questionário aos profissionais que trabalham em SROCs, sejam eles ROCs ou não, de maneira a obter dados sobre as PSIs adotadas dentro do atual contexto dessas 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. Os principais objetivos a serem atingidos com o inquérito foram:

1. Analisar a prática das políticas de segurança aplicadas nas SROCs, de maneira a garantir mínima exposição ao risco;
2. Identificar as tecnologias utilizadas pelas organizações bem como as fragilidades no contexto da segurança da informação das organizações;
3. Relacionar a dimensão das SROCs com as políticas de segurança aplicadas.

A. Definição do questionário

Com base no conhecimento adquirido através da revisão bibliográfica deste estudo, o questionário foi elaborado com um total de 14 questões. A versão final do mesmo foi obtida após validação por especialistas em auditoria que puderam verificar se as questões estavam adequadas ao contexto da pesquisa. Foi ainda realizado um pré-teste *online* junto de alunos do Mestrado em Auditoria que se encontravam em Estágio ou a desenvolver trabalho em SROCs. O questionário foi dividido em quatro grupos de questões, tal como apresentado na Tabela 2.

O inquérito foi introduzido na plataforma *Lime Survey*, disponibilizada pelo Instituto Politécnico de Coimbra, de forma a possibilitar a criação de *tokens* para os *e-mails* dos participantes.

Foi efetuada uma avaliação da fiabilidade das variáveis do estudo, na dimensão de consistência interna, através da análise dos itens, na qual foram ponderadas as correlações por intermédio do Alfa de Cronbach [26], 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. Aceita-se como limite inferior de adequada consistência interna o valor de 0,70. 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 âmbito da perceção dos colaboradores em relação às PSIs das SROCs fez sentido efetuar-se a ponderação.

Tabela 2: Estrutura do questionário

Parte 1: Características do respondente
P.1. Experiência profissional em auditoria (Número de anos)
P.2. Idade
P.3. Género
P.4. Atual cargo na organização onde trabalha
P.5. Membro da OROC (S/N)
Parte 2: Caraterísticas da organização onde trabalha
P.6. Principal segmento de mercado ou área de atuação em que prestam serviços de auditoria
P.7. Número aproximado de colaboradores
P.8. Presença em outros países para além de Portugal
Parte 3: PSIs implementadas na organização onde trabalha
P.9. Principais preocupações percetíveis em relação às fragilidades na segurança em dispositivos móveis
P.10. Existência de PSIs implementadas relacionadas a dispositivos móveis, uso de redes sociais, uso de *"Softwares* como serviços", plataforma de compartilhamento de informações
P.11. Tipos de tecnologias presentes em questões de segurança de dados em dispositivos móveis
P.12. Planos da organização em relação à adoção de novas políticas e manutenção das atuais implementadas
Parte 4: Perceção do colaborador em relação às PSIs implementadas (em escala *Likert*)
P.13.1. "A organização onde trabalho realiza formações (sessões presenciais ou através de e-learning) de maneira a evidenciar a importância da Segurança da informação"
P.13.2 "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"
P.13.3. "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
P.13.4. "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"
P.13.5. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados ao utilizar fotocopiadoras, scanners e impressoras dentro de suas instalações"
P.13.6. "A organização onde trabalho faz questão de conscientizar os colaboradores para cuidados com papeis de conteúdo confidencial em secretárias"
P.13.7. "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"
P.13.8. "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)"
P.13.9. "De maneira geral, acredito ter conhecimento sobre as políticas de segurança da informação que são aplicadas na organização onde trabalho"

B. Definição da amostra

Numa primeira fase foram enviados e-mails personalizados para os 1470 ROCs registados na Ordem dos Revisores Oficiais de Contas (OROC) com endereço eletrónico ativo. Uma vez que não foi objetivo de trabalho obter informações apenas de ROCs, posteriormente foram enviadas mensagens a 204 SROCs registadas no *website* da ordem com intenção de solicitar a participação de colaboradores não ROCs que trabalham com auditoria financeira. Por esta via foi possível obter 138 endereços de e-mail de colaboradores não ROCs, aos quais também foi endereçado convite à participação no estudo por e-mail. 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.

Do total de 1470 ROCs contactados, 11 profissionais optaram por clicar na opção de não participar da pesquisa e 6 profissionais responderam que não exerciam atividade de auditoria logo não participariam no estudo. Desta maneira, a população total do estudo foi de 1591 endereços eletrónicos, tendo-se obtido 175 registos de respostas considerados válidos para a análise, representando uma proporção de 11%.

IV. Apresentação e Discussão dos Resultados

A. Caracterização dos Respondentes e das organizações

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 mais velho possui 76 anos de idade e o mais novo 23. Cerca de 65% dos trabalhadores trabalham com auditoria financeira há, pelo menos, 5 anos, sendo a média de anos com experiência na área de, aproximadamente, 15 anos. 61% dos respondentes são ROCs. 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%). 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 na SROC. 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.

B. As PSIs nas SROCs e a perceção dos colaboradores

Através das respostas da terceira e quarta parte do questionário foi possível identificar características sobre as PSIs das SROCS e sobre o entendimento dos participantes sobre as mesmas. As respostas à última questão da quarta parte do inquérito revelam que grande parte dos colaboradores, independente da dimensão da organização onde trabalha, tem conhecimento sobre o atual contexto das PSIs que estão a ser aplicadas (130 indivíduos indicaram ter conhecimento, 7 indicaram não ter conhecimento e 38 optaram por não responder).

No âmbito da P.9., 73% dos participantes indicaram fazer parte das principais preocupações das organizações onde trabalham os seguintes temas: perda de dados relacionadas a perdas ou roubos de dispositivos e existência de *software* malicioso em dispositivos.

De acordo com o entendimento de maioria dos participantes, as SROCs onde trabalham possuíam PSIs relacionadas aos computadores disponibilizados aos colaboradores. No entanto, as respostas dividem-se ou são negativas no que respeita aos dispositivos móveis (telemóveis ou *tablets*), aos SaaS utilizados e também em relação ao uso de redes sociais. Explorando a dimensão da organização, é possível perceber que grande parte dos participantes envolvidos em organizações de maiores dimensões (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.

No que diz respeito ao tipo de tecnologia associados à segurança de dados em dispositivos, verificou-se um maior número de observações, independente da dimensão das organizações, na adoção de palavras passes, bloqueio remoto e limpeza remota de dispositivos (108 observações). No entanto, participantes que exercem atividades profissionais em SROCs com 1000+ colaboradores assinalaram mais alternativas como PSIs implementadas pelas suas organizações, nomeadamente, "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"*.

Mais de 70 participantes (41%) afirmou que nas suas organizações fazem atualizações das PSIs 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. A quarta parte do inquérito inclui um conjunto de afirmações que pretende aferir sobre a forma como as firmas dão conhecimento aos colaboradores relativamente às PSIs implementadas. As opções de resposta foram desenhadas em escala *Likert* com 5 níveis (1-Discordo Totalmente, 2- Discordo parcialmente; 3- Não concordo, nem discordo; 4- Concordo parcialmente e 5 - Concordo plenamente).

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 as suas atividades levam aos seus colaboradores o importante assunto relacionado às PSIs, ou seja, procuram consciencializar os colaboradores. Ainda assim, dos 175 participantes, 38 optaram por não responder a esta última parte do questionário, sendo número algo significativo. (as opções "Discordo plenamente", "parcialmente" ou "nem concordo nem discordo" 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 o 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.

C. Discussão dos Resultados

Os trabalhos e análises realizados nos pontos anteriores 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 PSIs 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 com que os 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" 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 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*").

D. PSIs:Proposta de boas práticas em SROCs

Através do presente estudo foram obtidos dados acerca das principais PSIs utilizadas em SROCs de dimensão variada, em Portugal, partindo da perceção de seus colaboradores. Assim, apresenta-se uma breve "compilação" de boas práticas que podem ser seguidas por firmas de auditoria:

1. Segurança Física da Informação:
   a. 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*;
   b. Restrição de acesso por parte de terceiros a áreas que contenham dados ou informação sensíveis;
   c. Segurança associada a transporte, manuseio e utilização de dispositivos fornecidos para trabalho;
   d. Descarte de informação sensível em depósitos específicos para tal (destruição de material obsoleto ou papéis de trabalho);

2. Segurança Digital da Informação:
   a. Uso de criptografia em todo o armazenamento e fluxo de dados que estejam fora do perímetro de segurança (dispositivos móveis ou nuvem);
   b. 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;
   c. Limite de acesso a website que representem/apresentem ameaças;
   d. Utilização de plataformas autorizadas para conversão de ficheiros;
   e. Uso de criptografia em *flash USB* ou plataformas de compartilhamento (*drives*);
   f. Bloqueio de ecrã de computadores ou telemóveis após um curto período de tempo;

3. Outros aspetos importantes:
   a. 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;
   b. Cláusulas de Confidencialidade na celebração de contratos de trabalho com novos colaboradores ou contratos para prestações de serviços;
   c. Conversas sobre informação sensível fora do escritório ou sala de reunião apropriada;
   d. 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*.

V. Conclusões

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. 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 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 do Regime Geral de Proteção de Dados (RGPD), em 2018. Neste sentido, há grandes possibilidades para trabalhos futuros com foco em alguns pontos pertinentes, como: análise do impacto da implementação do RGPD nas SROCs (e outras organizações); análise da evolução das PSIs nas SROCs antes e depois do RGPD; Segurança da Informação nas organizações portuguesas; as PSIs dentro das organizações cotadas na bolsa de valores portuguesa. Em relação a análise estatística dos dados recolhidos, a possibilidade de uma abordagem complexa onde se utilizem técnicas como análise de *clusters* que permita compreender a forma e distribuição dos elementos do grupo.

Entre as principais limitações deste estudo, destacam-se: 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; várias situações de inquiridos que não sabe/não responde, o que invalida o entendimento sobre alguns aspetos importantes.

Referências Bibliográficas

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

[2] 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).

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

[4] Almeida, B. J. M. D. (2019). Manual de Auditoria Financeira–Uma análise integrada no risco. 3ª Edição, Escolar Editora–Lisboa.

[5] Dias, C. (2000). Segurança e auditoria da tecnologia da informação. Axcel Books.

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

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

[8] 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.

[9] 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

[10] 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).

[11] ISACA (2012). CoBIT 5 for Information Security.

[12] 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

[13] 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

[14] 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

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

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

[17] ISACA (2014). Information 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

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

[19] IFAC (2009) International Standard on Quality Control 1 – Quality Control for Firms that Perfom Audit and Reviews of Financial Statements, and Other Assurance and Related Services Engagements, *2009.*

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

[21] 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

[22] 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.

[23] 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

[24] 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

[25] 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

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