Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO

CONTABILIDADE, FISCALIDADE E FINANÇAS EMPRESARIAIS

TRABALHO DE FINAL DE MESTRADO

DISSERTAÇÃO

A EFICÁCIA DA AUDITORIA DE CIBERSEGURANÇA EM PORTUGAL

MATILDE DE JESUS GOMES COSTA

Lisbon School of Economics & Management
Universidade de Lisboa

OUTUBRO - 2024

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO
CONTABILIDADE, FISCALIDADE E FINANÇAS EMPRESARIAIS

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

A EFICÁCIA DA AUDITORIA DE CIBERSEGURANÇA EM PORTUGAL

MATILDE DE JESUS GOMES COSTA

ORIENTAÇÃO:
PROFESSOR NUNO MIGUEL MENDES MORUJÃO

OUTUBRO - 2024

À Benedita, a minha sobrinha
e afilhada.

1 LISTA DE ABREVIATURAS

AI – Auditoria Interna

AICPA – American Institute of Certified Public Accountants

CI – Controlo Interno

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

COSO – Committee of Sponsoring Organizations

CSAM – Cybersecurity Audit Model

IIA – Institute of Internal Auditors

IPAI – Instituto Português de Auditoria Interna

ISA – International Standard on Auditing

ISACA – Information Systems Audit and Control Association

ISO – International Organization for Standardization

SI – Sistemas de Informação

NIST – National Institute of Standards and Technology

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

2 RESUMO

O principal objetivo desta dissertação consiste em avaliar a eficácia da auditoria de cibersegurança em Portugal, em 2024, através do cálculo do Índice de Eficácia da Auditoria de Cibersegurança, desenvolvido por Slapničar et al. (2022).

Adicionalmente, foi analisado o impacto das competências dos recursos humanos e da sua formação no índice, bem como o impacto da presença de um especialista em Sistemas de Informação no Conselho de Administração. Os resultados mostram que todos estes indicadores afetam positivamente o índice.

A escolha deste tema foi devida à importância da cibersegurança na prevenção dos ataques cibernéticos e das suas consequências para organizações e sociedade no geral. Como tal, este estudo fornece dados importantes para as organizações portuguesas, incentivando o investimento nesta área.

Relativamente à eficácia da auditoria de cibersegurança, concluiu-se que o índice médio de Portugal é superior ao de um estudo que abrange diversos países europeus, Israel, Austrália e Nova Zelândia, sugerindo uma maior eficácia no contexto português.

No entanto, o estudo apresenta algumas limitações, nomeadamente o reduzido número de respostas ao questionário, comprometendo a representatividade dos resultados. Além disso, o número de respostas por sector não é suficiente para efetuar uma análise setorial.

Para além do seu contributo para a comunidade científica, este estudo permite também uma avaliação da eficácia da cibersegurança em Portugal, bem como a obtenção de referências úteis para trabalhos de auditoria.

PALAVRAS-CHAVE: Auditoria Interna; Cibersegurança; Segurança da Informação; Eficácia; Controlo Interno; Auditoria de Segurança de Informação

JEL CODES: L86; M15; M40; M42; M53.

3 ABSTRACT, KEYWORDS AND JEL CODES

The main objective of this dissertation is to evaluate the effectiveness of cybersecurity auditing in Portugal, in 2024, through the calculation of the Cybersecurity Auditing Effectiveness Index, developed by Slapničar et al. (2022).

Additionally, the impact of human resources skills and their training on the index was analyzed, as well as the impact of the presence of an Information Systems specialist on the Board of Directors. The results show that all these indicators positively affect the index.

The choice of this topic was due to the importance of cybersecurity in preventing cyber-attacks and their consequences for organizations and society in general. As such, this study provides important data for Portuguese organizations, encouraging investment in this area.

Regarding the effectiveness of the cybersecurity audit, it was concluded that Portugal's average index is higher than that of a study covering several European countries, Israel, Australia and New Zealand, suggesting greater effectiveness in the Portuguese context.

However, the study has some limitations, namely the small number of responses to the questionnaire, compromising the representativeness of the results. Furthermore, the number of responses per sector is not sufficient to carry out a sectoral analysis.

In addition to its contribution to the scientific community, this study also allows an assessment of the effectiveness of cybersecurity in Portugal, as well as obtaining useful references for audit work.

KEYWORDS: Internal Audit; Cybersecurity; Information Security; Efficiency; Internal Control; Information Systems Audit

JEL CODES: L86; M15; M40; M42; M53.

4 Índice

5 ÍNDICE DE TABELAS

6 AGRADECIMENTOS

Aos meus pais, por todo o amor, carinho e apoio incondicional ao longo de toda a minha vida. Pela educação que me deram, pela capacidade de lutar e de não desistir. Por serem as pessoas mais importantes da minha vida. Tenho um orgulho imenso em ser vossa filha.

À minha irmã, por me ter acompanhado nos momentos mais difíceis da minha vida. Por ser a minha melhor amiga. Obrigada, por todas as vezes que me aturaste e continuas a aturar.

À minha querida sobrinha e afilhada, Benedita, que escreveu esta investigação comigo, sentada no meu colo. Provaste-me que o amor e a família são os pilares mais importantes da vida humana.

Aos meus tios, Palmira e Isidro, que se tornaram os meus segundos pais, acolhendo-me como filha durante toda a minha vida académica. Conseguiram fazer com que a distância ao Norte nunca fosse um obstáculo.

Ao meu namorado, Miguel, que acompanhou de perto todo o processo de escrita deste trabalho bem como todas as minhas dificuldades. Obrigada por me apoiares, por me manteres com os pés no chão, por me levares a passear sempre que alguma coisa não corria como eu queria.

Aos meu avôs e avós, Estevão e Amélia, Isaura e Alcino.

Ao meu tio Bernardo.

Um agradecimento ao meu orientador, Professor Nuno M. Morujão, por todo o acompanhamento, compreensão, dedicação e apoio.

À Professora Inês Pinto, pela compreensão e ajuda.

A todos os inquiridos que responderam ao questionário, obrigada! Pela paciência, compreensão e ajuda! Este trabalho nunca seria possível sem vocês.

7 DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICAL

Eu, Matilde de Jesus Gomes Costa, venho por este meio declarar que no âmbito da elaboração do presente trabalho final de mestrado, usei ferramentas de Inteligência Artificial Generativa para sugerir como utilizar o programa SPSS.

1 INTRODUÇÃO

A digitalização é um fator crucial para todas as organizações, desempenhando um papel estratégico em termos de produtividade, otimização de tarefas e eficácia operacional. No entanto, com a informatização dos processos das empresas surgem desafios que necessitam de respostas rápidas e eficazes, como é o caso dos ataques cibernéticos.

Várias empresas têm sido vítimas deste tipo de ataques (CNCS, 2023; Correia, 2019; Cowley, 2019; Litt et al., 2023) , sofrendo consequências como perda de riqueza para acionistas, custos de reputação, perda de confiança dos seus clientes, indisponibilidade de serviços de Tecnologia de Informação e Comunicação (TIC), divulgação de dados confidenciais, entre outros (Kamiya et al., 2020; Spanos & Angelis, 2016). Uma das soluções para mitigar estes riscos consiste na cibersegurança pois, através da proteção do ciberespaço e dos sistemas informáticos das organizações, permite evitar a ocorrência de ataques cibernéticos e suas consequências.

Com a complexidade do mundo corporativo, a auditoria interna (AI) é fundamental, na medida em que é uma ferramenta de apoio que abrange a toda a organização. Além disso, a AI tem um papel importante na proteção dos ativos da empresa, garantia da integridade dos dados e na confirmação sobre se a tecnologia atual suporta o plano de negócios existente (Al-Matari et al., 2021). Posto isto, a auditoria de cibersegurança relaciona estas duas áreas imprescindíveis para assegurar o futuro das organizações.

O principal objetivo deste estudo consiste em analisar a eficácia da auditoria de cibersegurança em Portugal, em 2024, através do cálculo do Índice de Eficácia da Auditoria de Cibersegurança (IEAC) proposto por Slapničar et al. (2022).

Posteriormente, foi realizada uma comparação entre o IEAC nacional e o índice calculado por Slapničar et al. (2022). Foram também testadas hipóteses que permitem compreender o impacto da avaliação das competências dos Recursos Humanos (RH), das ações de formação e sensibilização em matérias de cibersegurança dos RH e a presença de um especialista de Sistemas de Informação (SI) no Conselho de Administração das organizações no IEAC.

A metodologia adotada foi baseada no estudo de Slapničar et al. (2022), tendo sido alvo de adaptações que podem influenciar a comparabilidade do estudo.

Desta forma, foi elaborado um questionário que, posteriormente, foi distribuído aos profissionais de AI através do Instituto Português de Auditoria Interna (IPAI). Além disso, o questionário foi ainda enviado individualmente a auditores internos através da rede social Linkedin.

Este estudo foi realizado com dados relativos à cibersegurança das organizações nacionais, permitindo identificar as áreas mais fortes e mais vulneráveis. As conclusões deste estudo permitem identificar algumas áreas que afetam positivamente o IEAC, sendo um apoio para as organizações. O contributo para a comunidade científica deve também ser valorizado pois, em Portugal, não existem muitos estudos sobre o tema.

A realização da tese de mestrado concretiza um capítulo importante da vida académica da autora, contribuindo para o seu desenvolvimento pessoal, académico e profissional. A escolha do tema decorre da sua atualidade e impacto na sociedade, sendo suscetível de gerar resultados relevantes e contribuir para o avanço significativo na área.

O presente documento está estruturado em 5 capítulos. O primeiro consiste na introdução; o segundo na revisão de literatura, onde são abordados os conceitos em estudo e as relações entre os mesmos. O terceiro capítulo descreve a metodologia, caracterização da amostra e instrumentos de medida. O quarto capítulo é dedicado à análise de resultados do estudo da evidência empírica. Por fim, o quinto capítulo é destinado à conclusão, englobando as contribuições do estudo, limitações e sugestões para investigações futuras.

2 REVISÃO DE LITERATURA

2.1 Digitalização nas Organizações

Nos últimos anos, a tecnologia tem sido alvo de avanços exponenciais com impacto na sociedade nos mais diversos domínios. No caso do mundo empresarial, a digitalização foi crucial para a melhoria da eficiência operacional, nomeadamente em termos de produtividade e otimização de tarefas.

Existem evidências de que a adoção de TIC nas empresas portuguesas afetam positivamente a produtividade por trabalhador, os salários e a intensidade exportadora (Amador & Silva, 2023). Para Brodny & Tutak (2022), a adoção de tecnologias digitais nos processos das organizações é sinónimo de modernidade e inovação, contribuindo para um ambiente competitivo e inovador.

Recentemente, a Pandemia "Covid-19" afetou significativamente as organizações a um nível mundial. Em consequência, foi exigida uma elevada capacidade de resiliência ao mundo corporativo, que se adaptou no sentido de aumentar o recurso à telemática, uma vez que o trabalho presencial tornou-se impossível na maioria dos seus casos. Neste contexto, o uso do teletrabalho emergiu como uma ferramenta essencial para a continuidade dos negócios, gerando vantagens como a redução de custos financeiros para funcionários e empresas, o aumento da satisfação do trabalho, entre outros (Kähkönen, 2023).

Embora seja de domínio público que o uso de TIC e a digitalização proporcionam inúmeras vantagens, existem desvantagens que devem ser consideradas pelas organizações, nomeadamente a desconexão social, perda de postos de trabalho, redução da atividade física e interação *face-to-face*. No âmbito deste estudo, é particularmente relevante mencionar riscos de segurança e perda de privacidade, sendo um dever garantir que os dados estão armazenados de forma segura e protegida de ataques e outros *malwares* que ocorrem diariamente (Prakashbhai Bosamia, 2013).

2.2 Cibersegurança: Conceitos, Importância e Evolução

Um ciberataque consiste num ataque realizado via ciberespaço que visa o uso do último a fim de perturbar, incapacitar, destruir ou controlar maliciosamente um ambiente

ou infraestrutura computacional, podendo envolver a destruição da integridade dos dados ou roubo de informações controladas (NIST, 2019).

Um ataque deste tipo pode ter consequências devastadoras. De acordo com a Presidente do Banco Central Europeu, Christine Lagarde, um ataque bem-sucedido pode potenciar uma grave crise mundial (Maurer & Nelson, 2021).

Em particular, ao nível empresarial, um ciberataque pode resultar em perdas de riqueza para os acionistas e custos de reputação economicamente elevados (Kamiya et al., 2020). Como exemplo, pode ser recordada a violação de dados que vitimizou a *Equifax*, em 2017, expondo os dados confidenciais de 147 milhões de consumidores resultando em custos superiores a 650 milhões de dólares (Cowley, 2019). O estudo de Litt et al. (2023) refere o ataque realizado à *Deloitte* em 2017, confirmando que a empresa sofreu danos de reputação significativos após a violação e que cobraram honorários de auditoria mais baixos após o incidente, provavelmente como estratégia de recuperação. Além disso, os seus clientes de auditoria também sofreram com o incidente, tendo sido verificadas reações negativas no mercado.

O Centro Nacional de Cibersegurança (CNCS), tem registo de vários ataques recentes a organizações portuguesas dos mais diversos setores de atividade, nomeadamente o ataque ao Grupo Imprensa, do setor da comunicação social; à Vodafone, do setor das telecomunicações; à Sonae do setor de comércio grosso e a retalho e à TAP, no setor dos transportes (CNCS, 2023). A sociedade de advogados PLMJ foi também vítima de um ataque informático que resultou na divulgação de dados confidenciais de processos como a "Operação Marquês", o banco BES e o "E-Toupeira" (Correia, 2019).

Foi também comprovado, por Juma'h & Alnsour (2020) que o desempenho geral de uma empresa também é afetado por uma violação de dados, salientando que a ocorrência destes eventos indica a existência de deficiências internas.

No que diz respeito ao mercado de capitais, existem evidências de que os eventos positivos relacionados com segurança de informação, como investimento nesta área, são refletidos de forma positiva no preço das ações, enquanto a divulgação de uma violação de dados é incorporada de forma negativa no preço das ações (Spanos & Angelis, 2016).

Num contexto europeu, os dados de 2021 indicam que 22,2% das empresas vítimas de incidentes de cibersegurança sofreram consequências como a indisponibilidade dos

serviços de TIC, destruição ou corrupção de dados ou divulgação de dados confidenciais (Eurostat, 2023). No caso português, este indicador foi de 11,5%, sendo inferior ao valor da União Europeia (UE). Este facto indica que o impacto dos incidentes de cibersegurança em Portugal é inferior ao da média europeia, podendo justificar-se devido à ocorrência de menos ataques, à implementação de medidas de cibersegurança eficazes ou uma menor exposição ao risco.

Em 2022, foram registadas 367 violações de dados pessoais em Portugal, comprometendo os princípios de confidencialidade, integridade e disponibilidade (CNPD, 2022). Estas ocorrências colocam em causa a informação, que constitui um ativo valioso das empresas e que deve ser igualmente considerada relativamente aos outros importantes ativos, uma vez que é essencial para o negócio (ISACA, 2024).

A título de exemplo, podemos observar na Tabela I o número de incidentes registados em Portugal entre 2016 e 2022, sendo de salientar a tendência de crescimento acentuado. O contexto pandémico, observado em 2020[1], foi um fator que influenciou este indicador, tendo contribuído para o aumento e sofisticação dos incidentes de cibersegurança (Carreiras et al., 2020).

Tabela I - N.º de Incidentes de Cibersegurança em Portugal, entre 2016 e 2022

Ano	N.º de Incidentes de Cibersegurança
2016	413
2017	501
2018	599
2019	754
2020	1418
2021	1781
2022	2023

Fonte: CNCS

Na atual era digital, os ataques cibernéticos estão cada vez mais presentes. Assim sendo, a segurança da informação é necessária para a proteção dos recursos da organização, mas também para garantir a fiabilidade das demonstrações financeiras e outros relatórios de gestão (Steinbart et al., 2012).

[1] É importante notar que foram realizadas alterações na taxonomia utilizada a partir de 2020, passando a considerar vulnerabilidades como incidentes.

Neste contexto, a cibersegurança emerge como uma ferramenta fundamental na mitigação dos crimes cibernéticos. Por definição, a cibersegurança consiste na "capacidade de proteger ou defender o uso do ciberespaço de ataques cibernéticos" (NIST, 2019). Com o aumento mundial dos fluxos de tráfego e dos utilizadores de internet, a cibersegurança emergiu como uma questão de grande relevância mundial (Gunasegaran et al., 2021).

Posto isto, as organizações devem priorizar os seus recursos limitados, de forma a obter o melhor nível de segurança possível, dentro dos seus orçamentos (Al-Matari et al., 2021).

2.2.1 Tipos de Incidentes de Cibersegurança mais frequentes em Portugal

Neste capítulo, são mencionados os tipos de incidentes de cibersegurança com maior frequência em Portugal.

Tabela II - Tipos de Incidentes de Cibersegurança mais registados em Portugal, em 2022

Lugar no Ranking	Tipo de Incidente	N.º de Incidentes Registados
1	Phishing/Smishing	742
2	Engenharia Social	285
3	Distribuição de Malware	214
4	Utilização ilegítima de nome de terceiros	126
5	Comprometimento de conta não privilegiada	115

Fonte: CNCS

Conforme a Tabela II, o "*phishing/smishing"* foi o incidente mais frequente, com 742 casos registados. De acordo com o estudo de Yeboah-Boateng & Amanor (2014), *phishing* consiste numa forma de levar um utilizador final a revelar a sua informação sensível a um atacante em linha como, por exemplo, palavras-passe ou outras informações pessoais e dados sensíveis. O *smishing* tem o mesmo objetivo, mas em vez de ocorrer através de mensagens de correio eletrónico surge através de mensagens curtas ou mensagens de texto (Yeboah-Boateng & Amanor, 2014).

O segundo tipo mais frequente é a "Engenharia Social", sendo responsável por 285 incidentes. De acordo com Mouton et al. (2014), Engenharia Social trata-se da "ciência de utilização da interação social como meio de persuadir um indivíduo ou uma organização a cumprir um pedido específico de um atacante, em que a interação social, a persuasão ou o pedido envolve uma entidade informática".

Em seguida, a "Distribuição de *Malware"* é responsável por 214 ocorrências. Conforme o estudo de Aslan & Samet (2020), é considerado *malware* a utilização de qualquer *software* que execute intencionalmente "*malicious payloads*[2]" nas máquinas das vítimas, tais como computadores, *smartphones*, redes de computador, entre outros.

Por fim, o quarto e quinto tipo de incidente mais frequente são a "Utilização ilegítima de nome de terceiros" e o "Comprometimento de conta não privilegiada", tendo registado 126 e 115 ocorrências, respetivamente. É de notar que o relatório elaborado pelo CNCS, inclui uma análise aprofundada com dados de diferentes entidades.

2.2.2 Consequências dos Incidentes de Cibersegurança para as Organizações

Os incidentes cibernéticos e violações de segurança relacionadas com a acessibilidade, integridade e confidencialidade da informação envolvem custos explícitos e implícitos para as organizações (Brogi et al., 2018). Vários autores evidenciam os impactos dos incidentes cibernéticos no mercado bolsista (Brogi et al., 2018; Kamiya et al., 2020).

Kamiya et al. (2020) mostra que os incidentes de cibersegurança resultam em perda de riqueza para os acionistas e custos de reputação elevados para as organizações. Brogi et al. (2018) conclui que os retornos negativos substanciais resultantes dos ataques são mais elevados nas empresas do setor financeiro.

Além de afetar diretamente o mercado bolsista, um ataque cibernético bem-sucedido resulta em perda de confiança por parte dos clientes. Como tal, esta perda é especialmente significativa em negócios cuja confiança é fundamental como, por exemplo, sociedades de advogados ou empresas do setor financeiro.

Num estudo elaborado pelo Eurostat (2023) em que foram analisadas as consequências por incidentes de segurança nas TIC, em Portugal e na UE, em empresas com mais de 10 trabalhadores, concluiu-se que a consequência que mais afeta as organizações é a indisponibilidade de serviços de TIC, seguida da distribuição ou corrupção de dados e, por fim, a divulgação de dados confidenciais. Contudo, é importante reconhecer que este estudo apresenta limitações como a exclusão do setor

[2] "*malicious payloads*" é definido como a componente de um vírus de computador que executa uma atividade maliciosa (Rouse, 2016).

financeiro e a ausência de um termo de comparação com períodos anteriores, uma vez que foram realizadas alterações às questões (CNCS, 2023).

Assim, é de salientar que uma das consequências poderá ser a manipulação de dados, nomeadamente financeiros. Neste sentido, a qualidade dos dados que constam na informação financeira e, em consequência, na auditoria, pode ser comprometida. Devem ainda ser considerados outros riscos inerentes, como as falhas dos SI das organizações, essenciais para a realização da atividade das empresas.

Alguns impactos podem ser refletidos diretamente nas demonstrações financeiras, como, por exemplo, os ativos intangíveis, nomeadamente a confiança dos clientes, reputação da organização e a perda de propriedade intelectual, sendo a sua proteção essencial.

Em suma, ao analisar estas consequências, é relevante considerar que os ataques de cibersegurança podem afetar a operacionalidade das organizações, assim como a integridade dos seus dados, incluindo a informação financeira (pois pode ser manipulada), e perda de dados confidenciais, como, por exemplo, bases de dados de consumidores.

2.3 A Auditoria como ferramenta aliada à Cibersegurança

Num mundo corporativo cada vez mais complexo e competitivo, a auditoria assume um papel fundamental, pois tem como objetivo aumentar o grau de confiança dos destinatários das demonstrações financeiras (ISA 200, 2009).

A literatura existente não define o conceito de auditoria de forma única. O ISACA (2024), considera a auditoria como uma inspeção e verificação formal, que tem como objetivo verificar se uma norma ou um conjunto de diretrizes está a ser aplicado corretamente, garantindo a precisão dos registos e o cumprimento da eficiência e eficácia das metas. No estudo de Antunes (2021), a auditoria é entendida como a "atividade de recolha, exame e avaliação de informação (financeira, contabilística, operacional, legal) com vista a atestar a sua conformidade com determinados critérios preestabelecidos".

A auditoria pode assumir diversos tipos, dependendo da sua finalidade e incidência. No entanto, no âmbito deste estudo, é dado enfâse à AI.

De acordo com o IPAI (2024), a AI é uma "atividade independente, de garantia e de consultoria, destinada a acrescentar valor e melhorar as operações de uma organização.

Assiste a organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação dos processos de gestão de risco, de controlo e de governação".

Conforme Alqudah et al. (2023), "uma AI ativa pode sustentar uma organização para alcançar seus propósitos através de várias funções". Posto isto, é possível destacar alguns objetivos da AI nomeadamente, o apoio no alcance dos propósitos da organização, garantia de conformidade, avaliação do processo de gestão de riscos, controlo e de governação, entre outros. Adicionalmente, de acordo com (Stafford et al., 2018), os objetivos da auditoria centram-se em comprovar que existem controlos internos para minimizar o risco empresarial e que estes estejam a funcionar conforme o esperado.

Como anteriormente mencionado, para Juma'h & Alnsour (2020), um ataque de cibersegurança pode revelar deficiências internas. Diante isto, a AI pode desempenhar um forte papel na cibersegurança das organizações, na medida em que é responsável pela avaliação, monitorização, melhoria e consequentemente eficácia do controlo interno (CI).

De acordo com o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), o CI trata-se de um processo efetuado pelos trabalhadores da empresa, delineado para o fornecimento de garantia razoável relativamente ao alcance de objetivos relacionados a operações, relatórios e conformidade. Ou seja, o CI é "a resposta do órgão de gestão para mitigar um risco identificado ou atingir um objetivo de controlo"(IFAC, 2018).

No ambiente cibernético, o principal objetivo do CI é mitigar os riscos relacionados com a segurança da informação e com a cibersegurança. Assim sendo, a eficácia de um controlo consiste na capacidade de deteção, prevenção e mitigação de um risco de cibersegurança.

Neste sentido, o CI é fundamental pois contribui para a proteção contra ameaças cibernéticas através da implementação de controlos que protejam os SI das empresas de potenciais ataques. É de salientar que a deteção destes incidentes é crucial para a correção de fraquezas de CI, que representam vulnerabilidades que os criminosos podem aproveitar (Steinbart et al., 2018). Por isso, Stafford et al., (2018) considera "a prevenção, deteção e correção" de eventos indesejáveis como substância do processo de auditoria.

Complementarmente, o CI é responsável pela implementação de medidas que evitem o crescimento de ataques de cibersegurança, nomeadamente a consciencialização de colaboradores, uma vez que o fator humano é considerado um importante vetor na proteção de SI (Medeiros, 2023).

Por outro lado, Nobles (2018) afirma que 95% dos incidentes de cibersegurança são de origem humana. Pelo que, acredita-se que uma boa avaliação das competências dos RH pode influenciar positivamente a eficácia da auditoria de cibersegurança, sendo esta a primeira hipótese deste estudo:

H1: A avaliação das competências dos Recursos Humanos da organização em matérias de Cibersegurança está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

Da mesma forma, prevê-se que a formação e sensibilização dos RH nos assuntos de cibersegurança melhore o Índice de Eficácia de Auditoria de Cibersegurança, surgindo a hipótese H1a.

H1a.: A formação dos Recursos Humanos da organização em matérias de Cibersegurança está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

Assim, a Auditoria de Cibersegurança emerge como uma ferramenta aliada para o combate a riscos e criminalidade cibernética. A Auditoria de Cibersegurança consiste na avaliação dos sistemas e controlos em vigor, de forma a garantir a segurança das atividades cibernéticas, com o objetivo de avaliar a tecnologia, políticas e procedimentos atuais para determinar se as normas e regulamentos aplicados estão a ser cumpridos de forma eficaz e eficiente (Chimwanda, 2022). Por outro lado, Stafford et al. (2018), refere que a auditoria das funções de segurança de informação visa determinar a qualidade dos regimes preventivos e a identificação de erros nas medidas corretivas adotadas contra infrações às políticas de segurança. É ainda pertinente referir a Auditoria de SI que engloba o conjunto de etapas para a avaliação do status dos controlos de segurança das organizações, ou seja, um exame dos controlos de gestão dentro de uma infraestrutura de tecnologia de informação (TI) (Al-Matari et al., 2021).

Neste sentido, a auditoria auxilia o processo de identificação de pontos fracos numa organização de forma geral, ou especificamente em sistemas onde a segurança é essencial (Toapanta et al., 2019). No estudo de Toapanta et al. (2019) concluiu-se que

uma organização pode evitar muitos riscos através da realização de uma boa auditoria e evitar milhões de dólares em ataques cibernéticos.

Complementarmente, para Stafford et al. (2018), os auditores com julgamento estratégico e abordagem consultiva são essenciais para enfrentar os desafios de cibersegurança.

No que diz respeito aos interesses dos *stakeholders*, tem sido dada importância à divulgação de fatores de risco de cibersegurança, independentemente da ocorrência de um ataque cibernético ou não, uma vez que estes têm aumentado em empresas que sofreram e que não sofreram uma violação de dados (Chen et al., 2023).

2.4 Fatores que influenciam a eficácia da Auditoria

Atualmente, a definição de medidas de eficácia de auditoria ainda é um desafio. Turetken et al. (2020) sugere que não há consenso acerca dos fatores que contribuem para a eficácia da AI. No entanto, existem na literatura diversos estudos que permitem identificar indicadores que influenciam a eficácia da auditoria.

No estudo Steinbart et al. (2018), foi evidenciado que a qualidade do relacionamento entre a AI e as funções de segurança de informação tem um efeito positivo no número de fraquezas de CI e incidentes de não conformidade divulgados, bem como no número de incidentes de cibersegurança detetados antes e depois de causarem danos materiais à organização.

Bozkus Kahyaoglu & Caliyurt (2018) defendem que o auditor deve ter um forte conhecimento acerca das alterações regulamentais e tendências do setor, bem como garantir um alinhamento entre a auditoria e esses fatores. Em contradição, Vuko et al. (2021) não observaram que a regulamentação e as tendências do setor influenciam significativamente a auditoria de cibersegurança. No entanto, estes fatores não podem ser ignorados uma vez que, Vuko et al. (2021) salientam a possibilidade de dificuldades de medição da importância da regulamentação.

A compreensão do impacto total das ameaças cibernéticas para a organização, a identificação dos riscos cibernéticos de forma proativa, o entendimento do apetite ao risco da organização e a cooperação entre a função de AI e a Segurança da Informação, são fatores também fatores relevantes (Bozkus Kahyaoglu & Caliyurt, 2018).

Várias entidades reconhecidas desenvolveram *frameworks*[3] que contribuem para a eficácia da auditoria, nomeadamente o *Control Objectives for Information Technologies* (COBIT), *International Organization for Standardization* (ISO), *American Institute of Certified Public Accountants* (AICPA) e *National Institute of Standards and Technology* (NIST) (Bozkus Kahyaoglu & Caliyurt, 2018).

Com o objetivo de criar um modelo adaptável a qualquer organização e que inclua todas as áreas funcionais, Sabillon et al. (2017) desenvolveu o Modelo de Auditoria de Segurança Cibernética (CSAM). Este modelo é composto por 18 domínios, em que o primeiro é específico para cada Estado-Nação e os restantes podem ser adaptados a qualquer organização (Sabillon et al., 2017). No entanto, Slapničar et al. (2022) argumentam que esse modelo não é claro acerca da divisão dos domínios, não apresenta um controlo específico e fornece uma avaliação de diretrizes aplicáveis, não sendo por isso fiável.

De acordo com Stafford et al. (2018), a sensibilização em matérias de SI deve fazer parte de um plano global de segurança cibernética das organizações, destacando que os programas de sensibilização bem-sucedidos exigem auditores competentes na identificação de utilizadores que necessitam de aconselhamento. É ainda salientado que um utilizador instruído é o meio de dissuasão mais eficaz contra ameaças.

Vuko et al. (2021) refere que empresas mais digitalizadas são mais propensas a nomear membros do Conselho de Administração com competências de Cibersegurança. Destaca ainda os fatores humanos, o apoio e competências do Conselho de Administração como muito significativos.

Neste sentido, considera-se que a presença de especialistas em SI na chefia da organização pode estar positivamente relacionada com o IEAC.

Portanto:

H2: A presença de um especialista em Sistemas de Informação na chefia da organização está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

[3] *Framework* consiste numa estrutura conceptual básica utilizada para resolver ou abordar questões de maior complexidade (ISACA, 2024).

Al-Matari et al. (2021) sugere que os auditores de segurança de informação e os profissionais de cibersegurança devem estar familiarizados com os sistemas da organização, nomeadamente com a segurança da rede, bases de dados e sistemas operacionais.

No que diz respeito ao CI, podem surgir benefícios adicionais quando a monitorização dos controlos de segurança da informação é realizada pela função de segurança da informação e pela AI. No entanto, esses benefícios dependem do conhecimento de TI dos auditores internos, das suas atitudes em relação à cooperação com o pessoal de segurança de informação, do apoio da gestão de topo para a colaboração destes profissionais e das características organizacionais (Steinbart et al., 2012).

3 ESTUDO EMPÍRICO

3.1 Métodos e Procedimentos

Para Slapničar et al. (2022) a AI é constituída por três dimensões fundamentais: Planeamento, Desempenho e Relato.

A presente dissertação adota uma metodologia adaptada do estudo de Slapničar et al. (2022) permitindo, por um lado a consistência e comparabilidade entre os resultados e, por outro, a análise diferenciada pelas questões adicionais que foram incluídas pela autora.

A população alvo deste estudo abrange os profissionais de AI que realizem a sua atividade em Portugal. Pelo que, este estudo baseia-se em questionário feito a uma amostra de profissionais de AI, que exercem atividade profissional em Portugal, recorrendo para o efeito ao Instituto Português de Auditoria Interna (IPAI) e à rede social Linkedin. Assim, a amostra é não probabilística (não representativa), pela conveniência de conseguir maior número de respostas.

As questões inseridas foram baseadas nas utilizadas por Slapničar et al. (2022) pois, uma vez já testadas, contribuem para a qualidade deste estudo. De acordo com Maroco & Garcia-Marques (2013), um instrumento possui fiabilidade apropriada se o alpha de Cronbach for pelo menos de 0,7, sendo 0,6 suficiente para ciências sociais. Slapničar et al. (2022) refere, no seu estudo, que o alpha de Cronbach foi de 0,952 no primeiro teste de escala e de 0,955 no segundo teste de escala, evidenciando a fiabilidade do estudo.

As questões utilizadas nesse estudo foram traduzidas para língua portuguesa, tendo sido realizado um pré-teste que consistiu na distribuição do questionário a profissionais de várias áreas, permitindo a análise de formas de interpretação e identificação de erros. Não foram detetados erros que justificassem alterações no questionário, na sua versão final.

O período de recolha decorreu entre 11 e 25 de junho de 2024, o que resultou num total de 100 respostas. Destas 100 respostas, 83 são válidas (os demais inquiridos não se identificaram como profissionais de AI).

3.1.1 Índice de Eficácia de Auditoria de Cibersegurança

À semelhança da metodologia de Slapničar et al. (2022), neste estudo é desenvolvido um Índice de Eficácia de Auditoria de Cibersegurança (IEAC). Este índice trata-se de uma variável composta, uma vez que é construído através de três dimensões (Planeamento, Desempenho e Relato), sendo que cada dimensão contribui para a formação de um construto total, o IEAC.

O índice é função destas variáveis, pelo que qualquer alteração nelas será refletida no IEAC.

A primeira dimensão, Planeamento, é representada por 3 conjuntos de indicadores, presentes na Tabela III. O indicador PROACT envolve nove questões sobre a proatividade da AI no que diz respeito ao planeamento. O segundo indicador, RISK, é calculado através das quatro questões sobre as atividades reais de avaliação de risco. Ambos os indicadores (PROACT e RISK) foram respondidos numa escala de Linkert, em que 1 representa “Nada” e 5 “Totalmente. Por fim, o terceiro indicador avalia a utilização de *frameworks* de cibersegurança pela AI.

Tabela III - Indicadores da Dimensão Planeamento

Abreviatura	Planeamento	Peso	Descrição
PROACT	Proatividade de planeamento da AI	0,3	Nove itens sobre a proatividade da AI no planeamento (medidos numa escala de Linkert de 1 a 5, em que 1 significa "Nada" e 5 significa "Totalmente")
RISK	Avaliação de risco da AI	0,3	Quatro itens sobre as atividades reais da AI na avaliação de risco (medidos numa escala de Linkert de 1 a 5, em que 1 significa "Nada" e 5 significa "Totalmente"))
FRAMEW	Framework de cibersegurança utilizado	0,4	1 - se o inquirido utiliza algum framework; 0 - caso contrário

Fonte: SPSS

A dimensão Desempenho é constituída por dois indicadores (Tabela IV). O primeiro, PROCED, traduz os procedimentos de auditoria que são utilizados em cada uma das doze áreas de risco de cibersegurança, em cada ciclo. O segundo indicador, TOOLS, representa as ferramentas de cibersegurança utilizadas.

Tabela IV - Indicadores da dimensão Desempenho

Abreviatura	Desempenho	Peso	Descrição
PROCED	Procedimentos de auditoria que têm sido desempenhados para verificar 12 áres de cibersegurança em cada ciclo de auditoria	0,8	Procedimentos de auditoria utilizados em cada uma das 12 áreas de risco de cibersegurança (Não é verificado, Inquéritos/Questionários, Observação, Inspeção, Procedimentos Analiticos e Reexecução)
TOOLS	Utilização de ferramentas de cibersegurança pela AI	0,2	14 ferramentas de cibersegurança

Fonte: SPSS

A última dimensão, Relato, é constituída também por dois indicadores (Tabela V), FREQ, que revela a frequência de comunicação entre a AI e o Conselho de Administração e OPINION, que representa a independência da opinião da AI.

Tabela V - Indicadores da dimensão Relato

Abreviatura	Desempenho	Peso	Descrição
FREQ	Frequência de relato	0,8	Frequência de comunicação ao Conselho (1-Nunca; 2-Periodos inferiores a 2 anos; 3 - Períodos de 2 anos; 4 - Anualmente; 5 - Trimestralmente ou em todas as reuniões do Conselho de Auditoria)
OPINION	Fornecimento de uma opinião independente	0,2	1- se a AI emite uma opinião independente ao Conselho sobre a governance de cibersegurança, gestão de riscos e CI; 0-caso contrário

Fonte: SPSS

É de salientar que o peso de cada indicador corresponde ao utilizado por Slapničar et al. (2022) garantindo a semelhança do cálculo do IEAC e, consequentemente, a comparabilidade entre índices e geografias.

Para o cálculo da dimensão planeamento, foi utilizada a seguinte fórmula:

$$Planeamento = \left(\frac{\sum_{PROACT_i - PROACT_{min}}}{PROACT_{max} - PROACT_{min}} \right) 0,3 + \left(\frac{\sum_{RISK_i - RISK_{min}}}{Risk_{max} - RISK_{min}} \right) 0,3 + FRAMEW 0,4$$

$\sum PROACT_i$, representa o somatório das ponderações de 1 a 5, das nove questões relativas à proatividade da AI no que diz respeito ao planeamento (medidas através da escala de Linkert). Por isso, o valor mínino ($PROACT_{min}$) corresponde a 9 e o valor máximo ($PROACT_{max}$) é 45. O peso deste indicador na dimensão é de 0,3.

À semelhança do primeiro indicador mencionado, $\sum RISK_i$ indica a classificação total obtida nas quatro questões sobre as atividades reais de avaliação de risco, por isso, o seu valor mínimo é 4 e o máximo será 20. O peso do indicador RISK no Planeamento é, igualmente, de 0,3.

A dimensão Planeamento termina com o indicador FRAMEW, uma variável binária, que assume o valor 1 caso seja utilizado algum *framework* e 0 caso contrário. No total da dimensão Planeamento, este indicador representa 0,4.

A segunda dimensão, Desempenho, foi calculada através da seguinte fórmula:

$$Desempenho = \frac{\sum_{PROCED_{ij}}}{PROCED_{max}} 0,8 + \sum_{TOOLS_i} 0,2$$

Relativamente aos procedimentos de auditoria realizados em cada uma das doze áreas de risco de cibersegurança, foi atribuída uma pontuação consoante o valor/tipo de procedimentos utilizados pelo auditor. Assim sendo, a pontuação máxima de 1 é atribuída caso o inquirido tenha selecionado "Reexecução" ou realize 3 ou mais procedimentos. Caso contrário, a pontuação será atribuída proporcionalmente, ou seja, a utilização de apenas um procedimento traduz-se em um terço e dois procedimentos em dois terços. Posto isto, o valor mínimo é 0 (e, por isso, é oculto da fórmula) enquanto o valor máximo ($PROCED_{max}$) é 1. $\sum PROCED_{ij}$ indica a pontuação total de procedimentos realizados nas doze áreas de risco, sendo que i representa o número de áreas de risco e j o número de procedimentos. Este indicador representa 80% da dimensão Desempenho.

No que diz respeito às ferramentas utilizadas pela AI, $\sum TOOLS_i$ corresponde ao valor total de ferramentas utilizadas. Posteriormente, o número de ferramentas usadas foi multiplicado por 0,1. Desta forma, o valor mínimo é 0 e o máximo 1. O peso deste indicador na dimensão é de 20%.

Para a última dimensão foi utilizada a seguinte fórmula:

$$Relato = \frac{\sum_{FREQ_i - FREQ_{min}}}{FREQ_{max} - FREQ_{min}} 0,3 + OPINION 0,7$$

A frequência de comunicação entre a AI e o Conselho de Administração é representada pelo indicador FREQ, tendo sido atribuída uma pontuação de 1 a 5 em que: 1 corresponde a "Nunca", 2 a "Períodos inferiores a 2 anos", 3 a "Períodos de 2 anos", 4 a "Anualmente" e 5 a "Trimestralmente ou em todas as reuniões do Conselho de Auditoria". Posto isto, o valor mínimo ($FREQ_{min}$) é 1 e o máximo ($FREQ_{max}$) é 5. Este indicador representa 30% da dimensão Relato.

A independência da opinião relativamente à *governance* de cibersegurança, gestão de riscos e CI é representada através de uma variável binária que assume o valor 1 se o departamento de AI emite uma opinião independente relativamente à *governance* de cibersegurança e CI e 0 caso contrário. O peso deste indicador é de 70%.

Após quantificar o valor de todas as dimensões, o IEAC foi determinado através da seguinte fórmula:

$$IEAC = \left[(Planeamento \times 0,4) + (Desempenho \times 0,4) + (Relato \times 0,2) \right] \times 100$$

3.2 Caracterização da Amostra

Para este ponto, foi elaborada uma tabela presente nos Anexos que contém dados acerca da estatística descritiva sobre a caracterização da amostra deste estudo.

No que diz respeito à variável género, a amostra é composta por 54 inquiridos (65,1%) do género masculino e 29 (34,9%) do feminino.

Relativamente à idade dos inquiridos, o grupo etário com maior representatividade compreende as idades entre 26 e 30 anos, incluindo 27 inquiridos (28,1%), seguido do intervalo de 31 a 40 anos com 23 inquiridos (24%). O terceiro grupo compreende as idades entre 18 e 25 anos, sendo composto por 21 indivíduos (21,9%). Por fim, o grupo com menor representatividade abrange as idades superiores a 40 anos com 12 indivíduos (12,5%). Em termos médios, a amostra deste estudo pode ser considerada jovem uma vez que a média de idades é de 31,10 anos.

No que diz respeito às habilitações dos indivíduos, 45 (54,2%) obtêm o Mestrado/Pós-Graduação, seguida da Licenciatura que inclui 35 inquiridos (42,2%). Os graus com menor representatividade são doutoramento, que inclui 2 inquiridos (2,4%), e Ensino Secundário com 1 individuo (1,2%).

Do ponto de vista geográfico, 35 inquiridos (42,2%) residem na região Norte, 28 (33,7%) na região Sul e 12 (14,5%) na região Centro. As regiões do Alentejo e do Algarve são áreas de residência de 5 indivíduos (6%) e 3 inquiridos (3,6%) residem nas Regiões Autónomas da Madeira e dos Açores.

Os dados revelam que 23 inquiridos (27,7%) são profissionais de AI especializados em SI enquanto os restantes 60 (72,3%) não são especialistas nesta matéria.

Dos inquiridos, 46 (55,4%) não ocupam um cargo de chefia na organização em que trabalham e 37 (44,6%) indivíduos afirmam ocupar um cargo de chefia.

Para a análise das características organizacionais, foi elaborada uma tabela também presente nos Anexos.

Em relação ao tipo de empresa, 32 inquiridos (38,6%) revelam trabalhar numa empresa com mais de 250 colaboradores, 24 (28,9%) numa empresa entre 51 e 250 colaboradores, 20 (24,1%) indicaram o intervalo entre 11 e 50 colaboradores e, por fim, 7 inquiridos (8,4%) afirmam trabalhar numa empresa com menos de 10 colaboradores. O número aproximado de colaboradores trata-se de um indicador que permite compreender a dimensão da empresa, através da classificação das mesmas como micro, pequena, média e grande empresa, de acordo com o Decreto-Lei n.º 372/2007, de 6 de novembro, Esta classificação compreende também o volume de negócios ou o balanço total anual, no entanto, uma questão que aborde este tema poderia aumentar a taxa de desistência de resposta ao questionário.

Relativamente ao setor de atividade, entre os indivíduos que responderam ao questionário, 38 (45,8%) trabalham em "Outras atividades de serviços", 13 (15,7%) em Atividades Financeiras e de Seguros, 7 (8,4%) em Atividades de Consultoria, científicas, técnicas e similares e 4 (4,8%) inserem-se no setor dos Transportes e Armazenagem. Os restantes setores incluem 2 ou 1 inquirido e encontram-se apresentados na Tabela XXII.

Foi também solicitado ao inquirido qual o tipo de ativos que melhor representava a organização em que trabalha. Como tal, 28 inquiridos (33,7%) escolheram "Ativos Intangíveis: Programas de Computador", 19 (22,99%) selecionaram "Ativos Financeiros" e 12 (14,5%) referem "Ativos Tangíveis". Com menor representatividade, 5 inquiridos (6%) consideraram "Outros Ativos", 4 (4,8%) mencionaram "Ativos Intangíveis: Propriedade Industrial" e, finalmente, 3 indivíduos (3,6%) optaram por "Ativos Intangíveis: Outros Ativos Intangíveis". A tipologia de ativos foi baseada no Código de Contas da Comissão de Normalização Contabilística.

3.3 Instrumentos de Medida

O questionário (Anexo I) é constituído por 12 secções. A primeira secção é composta por uma breve introdução com o propósito de informar os inquiridos sobre a finalidade do questionário e segurança dos seus dados.

O grupo seguinte apresenta uma única questão que pretende filtrar os inquiridos, garantindo que os dados das questões seguintes dizem respeito apenas a profissionais de AI.

A terceira secção aborda os dados sociodemográficos e duas questões sobre a especialização do inquirido em SI e ocupação de cargos de chefia.

O quarto grupo é referente à recolha de dados específicos sobre a organização.

As secções seguintes destinam-se à recolha de dados das 3 dimensões da auditoria mencionadas por Slapničar et al. (2022): Planeamento, Desempenho e Relato.

Relativamente às escalas, foi utilizada uma escala de Likert de 5 pontos em que 1 representa "Nada" e 5 "Totalmente". Excecionalmente, numa questão em que foi pedida uma avaliação do plano de recuperação da organização, 1 representa "Negativa" e 5 "Excelente".

A primeira secção do questionário é constituída por uma breve introdução, cujo objetivo é informar o inquirido sobre a finalidade dos seus dados e questões de privacidade. É ainda enfatizado que o questionário é totalmente anônimo e confidencial.

A secção subsequente inclui apenas uma questão destinada a validar os profissionais de AI. Caso o inquirido não seja um profissional de AI, o questionário não permite prosseguir para as próximas questões.

A terceira secção tem como objetivo recolher dados sociodemográficos como género, idade, área de residência e habilitações. Contém também duas questões destinadas a compreender a especialização do auditor interno em SI ou cibersegurança e a verificar se o profissional ocupa um cargo de chefia na organização.

O quarto grupo está reservado para questões sobre da organização, permitindo analisar a sua dimensão e vulnerabilidade, através do número aproximado de colaboradores, setor de atividade e tipologia de ativos que melhor descreve a empresa.

A quinta secção inicia a recolha de dados relativa à dimensão de Planeamento, sendo composta por 9 questões destinadas a avaliar a proatividade da AI. As respostas são realizadas através de uma escala de Likert de 5 pontos em que 1 representa "Nada" e 5 "Totalmente".

Em sequência da recolha de dados sobre o Planeamento, a sexta secção é composta por 4 questões relacionadas com as atividades reais de avaliação de risco.

Adicionalmente, foram incluídas duas questões sobre as competências dos Recursos Humanos (RH) da organização em termos de cibersegurança, bem como atividades de formação e sensibilização de colaboradores acerca da área.

Finalizando a dimensão Planeamento, foi criada a sétima secção que permite ao inquirido selecionar o(s) *framework*(s) que utiliza no seu processo de auditoria.

A secção seguinte é relativa à duração do ciclo de auditoria (em meses).

O nono conjunto de questões diz respeito à dimensão seguinte (Desempenho), cujo objetivo é conhecer os procedimentos de auditoria utilizados para cada uma das 12 áreas de risco de cibersegurança. Para tal, o inquirido deveria selecionar os procedimentos que realiza. Esta secção inclui ainda uma questão relativa às ferramentas de cibersegurança, possibilitando identificar quais aquelas que são utilizadas.

A décima secção é composta por 3 questões criadas para este estudo. A primeira permite compreender a avaliação do plano de recuperação (*Disaster Recovery*) para situações adversas da organização, sendo respondida numa escala de Linkert de 5 pontos em que 1 representa "Negativa" e 5 "Excelente". As duas questões seguintes recolhem dados aproximados sobre o número de incidentes de cibersegurança ocorridos na

organização durante os últimos 5 anos e também o valor aproximado do investimento realizado em cibersegurança, em percentagem do ativo, ao longo dos últimos 5 anos.

A décima-primeira secção é composta por uma única pergunta sobre cobertura de riscos, permitindo entender se a organização tem um seguro específico para cobrir riscos de cibersegurança ou não.

O questionário finaliza com a recolha de dados para a dimensão de Relato, sendo constituída por duas questões. A primeira aborda a periodicidade de comunicação dos resultados da eficácia de gestão de riscos de cibersegurança ao Conselho de Administração e a segunda refere-se à emissão de uma opinião independente sobre a *governance* de cibersegurança, gestão de riscos e controlos internos.

4 RESULTADOS

4.1 Média e Desvio Padrão na Amostra Total

4.1.1 Dimensão Planeamento

O ponto médio de uma escala de Linkert de 5 pontos corresponde ao valor 3.

Na Tabela VI verifica-se que as médias dos resultados das questões dos indicadores de proatividade da AI no planeamento e nas atividades reais de avaliação de riscos de cibersegurança são superiores a 3, estando acima da média da escala de Linkert. É de salientar que, as áreas com uma média superior a 4 pontos (familiarização com a exposição e cenário de cibersegurança da organização, cooperação entre a AI e a função de Segurança de Informação e identificação da localização e forma de armazenamento dos ativos digitais mais valiosos) indicam um bom posicionamento das organizações.

O desvio padrão destes indicadores sugere uma proximidade dos dados à média, indicando uma maior concordância entre as respostas dos inquiridos.

A Tabela VI apresenta dos dados relativos aos *frameworks* de gestão de riscos de cibersegurança utilizados. O *framework* mais utilizado é o da ISO, sendo utilizado por 35 inquiridos (42,8%). De seguida, 32 inquiridos (38,6%) utilizam a estrutura da NIST, 19 (22,9%) afirmam utilizar o COBIT, 6 (7,2%) a estrutura do CNCS e 4 (4,8%) afirmam a AICPA. Por fim,12 inquiridos (14,5%) não se baseiam em nenhum *framework*.

Tabela VI – Estatísticas da dimensão Planeamento

Proatividade da AI no Planeamento	N	Média	Desvio Padrão
A Auditoria Interna está proativamente familiarizada com a exposição e cenário de cibersegurança da organização?	83	4,16	0,819
A Auditoria Interna está proativamente familiarizada com os benchmarks do setor e tendências de gestão de riscos de cibersegurança?	83	3,78	0,842
Existe cooperação entre a Auditoria Interna e as funções de Segurança de Informação?	83	4,2	0,745
A Auditoria Interna realiza uma avaliação à maturidade da gestão de risco de cibersegurança da organização?	83	3,87	0,997
A Auditoria Interna discute a maturidade da gestão de riscos de cibersegurança com a gestão e com o conselho de auditoria da organização?	83	3,89	0,797
A Auditoria Interna identifica os processos de gestão de risco que o conselho ou a gestão exigem garantia?	83	3,9	0,821
A Auditoria Interna apoia a gestão na melhoria da gestão de riscos de cibersegurança através da realização de consultorias?	83	3,77	0,967
A Auditoria Interna utiliza uma abordagem de auditoria interna baseada em risco relativamente à cibersegurança?	83	3,9	0,864
A Auditoria Interna avalia o alinhamento entre a estratégia geral da organização e a estratégia de cibersegurança?	83	3,96	0,803
Atividades reais da AI relativamente à avaliação de risco			
A Auditoria Interna procura identificar a localização e forma de armazenamento de ativos digitais valiosos da organização como, por exemplo, bases de dados?	83	4,29	0,918
A Auditoria Interna realiza uma avaliação de risco que permita compreender a vulnerabilidade associada ao armazenamento dos ativos digitais mais valiosos?	83	3,8	0,894
A Auditoria Interna avalia o impacto e probabilidade do roubo ou comprometimento desses ativos digitais?	83	3,86	0,871
A Auditoria Interna procura identificar outros ativos digitais, bem como os seus níveis de proteção, valor e vulnerabilidade?	83	3,87	0,88
Framework de Gestão de Riscos de Cibersegurança utilizada	**N**	**Freq**	**%**
COBIT		19	22,9
NIST		32	38,6
AICPA		4	4,8
ISO		35	42,8
CNCS		6	7,2
Não é utilizado nenhum framework		12	14,5

Fonte:SPSS

4.1.2 Dimensão Desempenho

A Tabela VII apresenta estatísticas relativas à dimensão Desempenho. Assim, é de salientar que 4 inquiridos (4,8%) afirmam não utilizar ferramentas de cibersegurança. Contrariamente, os restantes 79 inquiridos utilizam, pelo menos, uma ferramenta de cibersegurança.

Das ferramentas referidas, as ferramentas de monitorização de segurança da rede são utilizadas por 58 indivíduos (60,4%), as ferramentas de encriptação por 45 (46,9%) e as de análise de vulnerabilidades da web por 42 (43,8%). Por outro lado, *packet sniffers*

constituem a ferramenta menos utilizada, tendo sido selecionada por 11 indivíduos (11,5%).

Tabela VII - Estatísticas da dimensão Desempenho

N.º de Ferramentas de Cibersegurança Utilizadas		Freq	%
Não são utilizadas ferramentas de cibersegurança		4	4,8
N.º de Ferramentas utilizadas			
	1	4	4,8
	2	3	3,6
	3	8	9,6
	4	8	9,6
	5	20	24,1
	6	13	15,7
	7	12	14,5
	8	6	7,2
	9	3	3,6
	10	2	2,4
Ferramentas de Cibersegurança utilizadas			
Ferramentas de Monitorização da Segurança da Rede		58	60,4
Ferramentas de Encriptação		45	46,9
Ferramentas de Análise de Vulnerabilidades da Web		42	43,8
Ferramentas de Defesa de Rede sem Fios		43	44,8
Packet Sniffers		11	11,5
Software Antivírus		48	50
Firewall		45	46,9
Managed Detection Services		22	22,9
Testes de Penetração		34	35,4
Sistema de Deteção de Intrusões		46	47,9
Outra(s)		0	0

Fonte:SPSS

4.1.3 Dimensão Relato

A Tabela VIII contém dados sobre a dimensão Relato. Observando a tabela, verifica-se que a comunicação entre a AI e o Conselho de Administração é anual em 34 inquiridos (41%) e trimestral ou em todas as reuniões do Conselho para 30 indivíduos (36,1%), sendo esta regularidade bastante positiva. Pelo contrário, existem 3 indivíduos (3,6%) que assumem nunca comunicar os resultados ao Conselho.

No que diz respeito à independência da opinião, 72 inquiridos (86,7%) afirmam a emissão de uma opinião independente, enquanto os restantes 11 (13,3%) referem o contrário.

Tabela VIII - Estatísticas da dimensão Relato

Frequência de comunicação com o Conselho	N	Freq	%
Nunca	83	3	3,6
Períodos inferiores a 2 anos	83	12	14,5
Períodos de 2 anos	83	4	4,8
Anualmente	83	34	41
Trimestralmente ou em todas as reuniões do Conselho		30	36,1
Independência da opinião emitida			
Sim	83	72	86,7
Não	83	11	13,3

Fonte:SPSS

4.1.4 Índice de Eficácia de Auditoria de Cibersegurança

A Tabela IX apresenta dados relativos ao IEAC calculado neste estudo, juntamente com o índice obtido no estudo de Slapničar et al. (2022).

A análise do IEAC é crucial para compreender a eficácia da auditoria de cibersegurança. Neste estudo, o valor médio do IEAC em Portugal é de 71,67, cujo valor máximo é de 96,31 e o mínimo de 13,36. Quando analisamos a composição deste índice, verifica-se que a dimensão Desempenho apresenta a menor média (62,58) enquanto a de Relato regista a maior (83,22).

Em contraste, o estudo de Slapničar et al. (2022), apresenta uma média de 57,89, com um valor máximo de 99,25 e um mínimo de 2. Ao analisar as dimensões, observa-se que Desempenho apresenta a menor média (53,39) e Planeamento a maior (63,68).

Ao realizar uma comparação dos resultados dos estudos mencionados, verifica-se que a média do IEAC em Portugal é superior à média do índice calculado por Slapničar et al. (2022), sugerindo uma maior eficácia da auditoria de cibersegurança em Portugal, relativamente aos vários países europeus, Israel, Austrália e Nova Zelândia. No entanto, esta amostra internacional é mais abrangente, incluindo realidades de diferentes Estados, o que pode refletir diferenças regulatórias, económicas e culturais que influenciam as regiões.

Globalmente, a média da dimensão Planeamento em Portugal (75,09) obtém valores médios superiores aos de Slapničar et al. (2022) (63,68), demonstrando que as práticas de auditoria de cibersegurança em Portugal são mais estruturadas ao nível do planeamento.

Os resultados da dimensão Desempenho em Portugal (62,48) também se revelam superiores aos do estudo de referência (53,39), o que indica uma maior eficácia nas funções associadas a esta dimensão.

A dimensão Relato apresenta uma diferença notável, sendo que o valor médio em Portugal e no estudo de Slapničar et al. (2022) é de 83,22 e 55,30, respetivamente. Esta assimetria sugere uma maior eficácia na comunicação com o Conselho de Administração, bem como ao nível da independência da opinião emitida pela auditoria.

Em suma, estes resultados assinalam melhores práticas de auditoria de cibersegurança e uma maior consciencialização sobre o tema em Portugal em comparação com os países europeus, Israel, Austrália e Nova Zelândia.

Tabela IX - Comparação de Índices

	Média	Desvio-Padrão	Mínimo	Máximo
IEAC Portugal	71,67	19,41	13,36	96,31
Planeamento	75,09	19,72	22,50	95,83
Desempenho	62,48	24,34	8,89	100,00
Relato	83,22	27,77	0,00	100,00
Índice do estudo de Slapničar et al. (2022	57,89	22,92	2,00	99,25
Planeamento	63,68	25,90	0,00	100,00
Desempenho	53,39	29,05	0,00	100,00
Relato	55,30	38,94	0,00	100,00

Fonte:SPSS

Para uma análise detalhada, os valores do IEAC foram agrupados por níveis de eficácia (Tabela X). Ao analisar, verifica-se que 43,4% dos inquiridos portugueses apresentam o nível de eficácia "Muito Alto" e 28,9% inserem-se no nível "Alto". É de destacar que os níveis mais baixos de eficácia dizem respeito a 2,4% ("Muito Baixo") e 7,2% ("Baixo").

Já no estudo de Slapničar et al. (2022), o nível "Muito Alto" enquadra 17,5% dos inquiridos e o "Alto" 32,8%. Os níveis "Muito Baixo" e "Baixo" inserem 9,8% e 10,9% dos indivíduos, respetivamente.

Para concluir, esta análise indica novamente uma maior eficácia da auditoria de cibersegurança em Portugal, uma vez que a maioria dos inquiridos se insere nos níveis elevados de eficácia e os níveis mais baixos têm pouca representatividade.

Tabela X - IEAC por níveis de eficácia

Nível de Eficácia	Intervalo de Eficácia	Freq	%
IEAC Portugal			
Muito Baixo	De 0 a 20,99	2	2,4
Baixo	De 21 a 40,99	6	7,2
Médio	De 41 a 60,99	15	18,1
Alto	De 61 a 80,99	24	28,9
Muito alto	De 81 a 100	36	43,4
Índice do estudo de Slapničar et al. (2022)			
Muito Baixo	De 0 a 20	18	9,8
Baixo	De 21 a 40	20	10,9
Médio	De 41 a 60	53	29
Alto	De 61 a 80	60	32,8
Muito alto	De 81 a 100	32	17,5

Fonte:SPSS

4.2 Análise de Diferenças Significativas em Subgrupos da Amostra

A divisão da amostra em subgrupos proporciona uma análise pormenorizada de tendências em que é possível determinar diferenças significativas entre os grupos. Para tal, foram criados subgrupos com base no género, idade, região de residência, setor de atividade da organização e número de colaboradores empresa. Para esta análise foi utilizado um intervalo de confiança de 95% e um nível de significância de 5%.

Para este efeito, foi necessário o teste de variância ANOVA e o teste T-Student. O último é utilizado para a comparação de médias entre dois grupos e, por isso, foi utilizado apenas para a variável género. Para as restantes variáveis, foi utilizado o teste ANOVA, apropriado para a comparação entre dois ou mais grupos.

As diferenças entre os subgrupos são significativas quando um valor de significância (p) é tal que $p \leq 0,05$, sendo que existe 95% de certeza que existem diferenças significativas entre os subgrupos da amostra.

Para a análise do primeiro subgrupo, baseado no variável género, foi realizado um teste t onde foi obtido um valor-p de 0,727. Consequentemente, não são observadas diferenças estatisticamente significativas entre os géneros (Tabela XI).

Tabela XI - Diferenças entre géneros

Género	N	Média	Z	Sig
Masculino	54	70,519	0,123	0,727
Feminino	29	73,824		

Fonte:SPSS

No que diz respeito à variável "idade", o valor-p ascende a 0,199 não se evidenciando diferenças estatisticamente significativas entre os intervalos de idade (Tabela XII)

Tabela XII - Diferenças por idade

Intervalo de Idade	N	Média	Z	Sig
18 a 25 anos	21	63,9386243		
26 a 30 anos	27	75,5179012		
31 a 40 anos	23	73,3253623	1,586	0,199
Superior a 40 anos	12	73,3935185		
Total	83	71,673494		

Fonte:SPSS

Considerando a variável "setor de atividade", o valor-p é de 0,014 e, portanto, verificam-se diferenças estatisticamente significativas entre os setores, uma vez que o valor é inferior a 0,05. No entanto, este resultado não é confiável uma vez que existe uma elevada diversidade na quantificação dos setores existindo, por exemplo, setores que incluem apenas um inquirido e setores que inserem 38 (Tabela XIII).

Tabela XIII - Diferenças por setor

Setor	N	Média	Z	Sig
Transportes e Armazenagem	4	74,321		
Outras atividades de serviços	38	76,497		
Indústrias Transformadoras	3	73,719		
Indústrias Extrativas	1	55,644		
Eletricidade, Gás, Vapor, Água quente e fria e Ar frio	2	71,733		
Educação	3	58,970		
Comércio por grosso e a retalho; Reparação de veículos automóveis e motociclos	2	92,294		
Captação, Tratamento e Distribuição de água;Saneamento, Gestão de Resíduos e Despoluição	2	59,069		
Atividades Imobiliárias	1	59,111	2,215	0,014
Atividades financeiras e de seguros	13	74,702		
Atividades dos organismos internacionais e outras instituições extra-territoriais	1	93,539		
Atividades de informação e comunicação	1	39,800		
Atividades de consultoria, científicas, técnicas e similares	7	69,047		
Alojamento, restauração e similares	2	34,081		
Agricultura, produção animal, caça, floresta e pesca	2	35,817		
Administração Pública e Defesa; Segurança Social Obrigatória	1	58,111		
Total	83	71,673		

Fonte:SPSS

Quanto à variável "região de residência", obteve-se um valor-p de 0,013. À semelhança do caso anterior, os resultados deste teste evidenciam diferenças estatisticamente significativas entre os grupos (0,013<0,05) mas, este resultado deve ser igualmente comentado uma vez que existem assimetrias entre os elementos

correspondentes a cada região. Desta forma, este resultado aparenta estar distante da realidade (Tabela XIV).

Tabela XIV-Diferenças por região

Região de Residência	N	Média	Z	Sig
Norte	35	63,957	3,392	0,013
Centro	12	84,097		
Lisboa	28	73,827		
Alentejo e Algarve	5	81,174		
Região Autónoma da Madeira e Região Autónoma dos Açores	3	76,072		
Total	83	71,673		

Fonte: SPSS

A variável "número de colaboradores" é um indicador que permite analisar a dimensão da organização. Neste caso, o valor-p foi de 0,022, indicando a existência de diferenças estatisticamente significativas entre pelo menos dois grupos, ou seja, entre IEAC referentes à dimensão da empresa (Tabela XV)

Tabela XV - Diferenças por N.º de Colaboradores

N.º de Colaboradores	N	Média	Z	Sig
Menos de 10 colaboradores	7	52,363	3,376	0,022
Entre 11 a 50 colaboradores	20	69,440		
Entre 51 a 250 colaboradores	24	72,591		
Mais de 250 colaboradores	32	76,606		
Total	83	71,673		

Fonte: SPSS

4.3 Teste de Hipóteses

H1: A avaliação das competências dos Recursos Humanos da organização em matérias de Cibersegurança está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

Para testar esta primeira hipótese, foi realizado um teste de regressão linear onde foi obtido um valor-p de 0,001 (Tabela XVI). Em resultado, verifica-se uma relação estatisticamente significativa entre as variáveis que representam a avaliação das competências dos RH em matérias de cibersegurança e o IEAC. Além disso, a correlação registada entre as variáveis é de 0,343 o que se traduz numa correlação positiva. Posto isto, os resultados indicam que uma avaliação mais elevada das competências dos RH está associada a um aumento do IEAC.

Tabela XVI - Teste de Regressão Linear (H1)

R	R-square	R Quadrado Ajustado	Erro Padrão da Estimativa	Z	Sig
0,343	0,118	0,107	18,339	10,812	0,001

Fonte:SPSS

H1a.: A formação dos Recursos Humanos da organização em matérias de Cibersegurança está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

À semelhança de H1, foi realizado um teste de regressão linear (Tabela XVII), cujo valor-p apresentado foi menor que 0,001 sendo inferior ao nível de significância e, por isso, indica a existência de estatísticas significativas. Em adição, a correlação entre as variáveis em teste foi de 0,559, o que permite concluir que a formação dos RH em matérias de cibersegurança está positivamente relacionada com o IEAC.

Tabela XVII - Teste de Regressão Linear (H1a)

R	R-square	R Quadrado Ajustado	Erro Padrão da Estimativa	Z	Sig
0,559	0,312	0,304	16,195	36,742	<0,001

Fonte:SPSS

H2: A presença de um especialista em Sistemas de Informação na chefia da organização está positivamente relacionada com o Índice de Eficácia de Auditoria de Cibersegurança.

Para testar H2, foi também realizado um teste de regressão linear (Tabela XVIII) onde foi obtido um valor-p de 0,002, evidenciando a existência de estatísticas significativas. Em resultado do teste foi obtida uma correlação de 0,332, sendo possível concluir que existe uma relação positiva entre presença de um especialista em SI na chefia da organização e o IEAC.

Tabela XVIII - Teste de Regressão Linear (H2)

R	R-square	R Quadrado Ajustado	Erro Padrão da Estimativa	Z	Sig
0,332	0,11	0,099	18,416	10,047	0,002

Fonte: SPSS

5 CONCLUSÃO

De uma forma global, é possível concluir que a eficácia da auditoria de cibersegurança em Portugal é elevada uma vez que, através do cálculo do IEAC e da sua comparação com o índice de Slapničar et al. (2022), são verificados valores superiores em Portugal. No entanto, a amostra pode não ser suficientemente consistente para ter uma elevada representatividade.

Com este estudo, é também possível identificar quais as áreas responsáveis pelo bom posicionamento em cibersegurança das empresas, bem como outras que podem ser melhoradas, nomeadamente ao nível do Planeamento.

Além disso, este estudo analisa parcialmente o papel dos RH na cibersegurança das organizações, permitindo concluir que a avaliação das competências e a formação e sensibilização dos RH em cibersegurança estão positivamente relacionadas com o IEAC. Neste sentido, incentiva-se às organizações o investimento nesta matéria.

Por fim, foi ainda verificado que a presença de um especialista em SI no Conselho de Administração influencia positivamente o IEAC, o que reforça a importância do alinhamento entre a liderança e melhores práticas de cibersegurança com o propósito de proteger as organizações de potenciais riscos cibernéticos.

5.1 Contribuições do Estudo

Dada a carência da literatura em estudos de auditoria de cibersegurança, este estudo contribui para o enriquecimento da comunidade científica, numa área que não está muito desenvolvida, principalmente em Portugal.

Por outro lado, o crescente número de ataques cibernéticos e suas consequências enfatizam a importância deste tema e da sua atualidade, o que acrescenta valor à investigação.

Do ponto de vista prático, são fornecidos *benchmarks* à AI, promovendo a sua eficácia e melhoria do trabalho de auditoria. Além disso, para a realização deste estudo foram utilizados dados baseados nos sistemas de cibersegurança das organizações portuguesas, permitindo identificar potenciais áreas de melhoria.

Por fim, a utilização de uma metodologia já desenvolvida permite a comparação entre a auditoria de cibersegurança em Portugal e uma geografia internacional.

5.2 Limitações e Sugestões para Investigações Futuras

A carência de estudos sobre o tema na literatura consiste também numa limitação, pois resulta na redução da validação de determinados dados e aumenta a dificuldade em aprofundar e desenvolver conhecimentos.

Relativamente à amostra deste estudo, deve ser salientado o número reduzido de respostas ao questionário, e por isso, a sua baixa representatividade face à população.

Como sugestões de pesquisas futuras, propõe-se a realização de uma análise entre o IEAC e o setor de atividade, zona de residência ou ambos, uma vez que não foi possível relacionar os indicadores nesta amostra dada a assimetria de respostas entre estes subgrupos.

É ainda proposto analisar a relação entre o IEAC e o investimento realizado em cibersegurança pelas organizações ou o número de ataques cibernéticos ocorridos ao longo de um período.

Pode ainda ser realizada uma investigação que permita compreender as práticas dos órgãos de administração, de forma a prevenir os ataques cibernéticos ou a elaboração de um estudo do ponto de vista legal, nomeadamente denúncia ao Ministério Público, que aborde as normas de cibersegurança existentes.

Por fim, sugere-se a monitorização periódica do índice criado neste estudo, permitindo o acompanhamento contínuo da eficácia da auditoria de cibersegurança.

6 REFERÊNCIAS

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. *Information Security Journal*, *30*(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649

Alqudah, H., Amran, N. A., Hassan, H., Lutfi, A., Alessa, N., alrawad, M., & Almaiah, M. A. (2023). Examining the critical factors of internal audit effectiveness from internal auditors' perspective: Moderating role of extrinsic rewards. *Heliyon*, *9*(10). https://doi.org/10.1016/j.heliyon.2023.e20497

Amador, J., & Silva, C. (2023). Uma visão sobre as TIC e a digitalização nas empresas portuguesas. *Revista de Estudos Económicos*, *IX, n.º4*.

Antunes, J. (2021). *A Auditoria de Contas*. https://www.oroc.pt/publicacoes/revista/revista/2021/

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. In *IEEE Access* (Vol. 8, pp. 6249–6271). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2963724

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804

Brodny, J., & Tutak, M. (2022). Digitalization of Small and Medium-Sized Enterprises and Economic Growth: Evidence for the EU-27 Countries. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2). https://doi.org/10.3390/joitmc8020067

Brogi, M., Arcuri, M. C., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership and Control*, *15*(2), 70–83. https://doi.org/10.22495/cocv15i2art6

Carreiras, H., Barrinha, A., Gameiro Marques, A., Santos, L., Santos, D., Fialho de Jesus, H., Barbas, J., Confraria, J., Borges Gouveia, L., Fernando Viegas Nunes, P., José Santos, S., & Martins Geraldes, S. (2020). *CIBERSEGURANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA*.

Chen, J., Henry, E., & Jiang, X. (2023). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. In *Journal of Business Ethics* (Vol. 187, Issue 1, pp. 199–224). Springer Science and Business Media B.V. https://doi.org/10.1007/s10551-022-05107-z

Chimwanda, E. (2022). *Essentials for an Effective Cybersecurity*. https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit

CNCS. (2023). *CIBERSEGURANÇA*.

CNPD. (2022). *Relatório de Atividades 2022*.

Comissão de Normalização Contabilistica. (n.d.). *Código de Contas*.

Correia, F. (2019). Ataque informático expõe documentos da PLMJ sobre casos mediáticos. *Público*.

COSO. (2013). *Internal Control-Integrated Framework Executive Summary*.

Cowley, S. (2019). Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement. *The New York Times*.

Diário da República. (2007). *Pequena e média empresa (PME)*. https://diariodarepublica.pt/dr/lexionario/termo/pequena-media-empresa-pme

Eurostat. (2023). *22% of EU enterprises had ICT security incidents*. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1

Gunasegaran, M., Basiruddin, R., & Binsaddiq, R. (2021). A Review of Cybersecurity Element in Fraud Prevention and Detection Mechanisms Article history. In *Open International Journal of Informatics (OIJI)* (Vol. 9, Issue 3).

IFAC. (2018). *GUIA DE APLICAÇÃO DAS ISA - CONCEITOS FUNDAMENTAIS E ORIENTAÇÃO PRÁTICA*. www.ifac.org/smp.

IPAI. (2024). *Auditoria Interna, o que é?* https://www.ipai.pt/sobre-nos/auditoria-interna-o-que-e/

ISA 200. (2009).

ISACA. (2024). *Glossary*. https://www.isaca.org/resources/glossary#glossi

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management*, *28*(2), 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

Kähkönen, T. (2023). Remote work during the COVID-19 pandemic: identification of working life impacts, employees' data protection abilities and trust outcomes. *Journal of Organizational Change Management*, *36*(3), 472–492. https://doi.org/10.1108/JOCM-06-2022-0179

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Litt, B., Tanyi, P., & Watson, M. W. (2023). Cybersecurity Breach at a Big 4 Accounting Firm: Effects on Auditor Reputation. *Journal of Information Systems*, *37*(2), 77–100. https://doi.org/10.2308/ISYS-2022-006

Maroco, J., & Garcia-Marques, T. (2013). Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas? *Laboratório de Psicologia*, *4*(1). https://doi.org/10.14417/lp.763

Maurer, T., & Nelson, A. (2021). A Ameaça Cibernética Global aos Sistemas Financeiros – FMI F&D. *Fundo Monetário Internacional*. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

Medeiros, N. (2023). *Artigo: O Fator Humano na Cibersegurança | Porto Business School*.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). *Social Engineering Attack Framework*.

NIST. (2019). *Glossary of key information security terms*. https://doi.org/10.6028/NIST.IR.7298r3

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Prakashbhai Bosamia, M. (2013). *Positive and Negative Impacts of ICT in our Everyday Life 1 Positive and Negative Impacts of Information and Communication Technology in our Everyday Life*.

Rouse, M. (2016). What is a Payload (Computer Virus)? - Definition from Techopedia. *Techopedia*.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, *2017-November*, 253–259. https://doi.org/10.1109/INCISCOS.2017.20

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*. https://doi.org/10.1016/j.accinf.2021.100548

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. In *Computers and Security* (Vol. 58, pp. 216–229). Elsevier Ltd. https://doi.org/10.1016/j.cose.2015.12.006

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Toapanta, S. M. T., Peralta, N. A., & Gallegos, L. E. M. (2019). Definition of parameters to perform audit in cybersecurity for public one organization of ecuador. *ACM*

International Conference Proceeding Series, 91–96. https://doi.org/10.1145/3375900.3375913

Turetken, O., Jethefer, S., & Ozkan, B. (2020). Internal audit effectiveness: operationalization and influencing factors. In *Managerial Auditing Journal* (Vol. 35, Issue 2, pp. 238–271). Emerald Group Holdings Ltd. https://doi.org/10.1108/MAJ-08-2018-1980

Vuko, T., Slapnicar, S., Čular, M., Drašček, M., & Slapničar, S. (2021). *Key Drivers of Cybersecurity Audit Effectiveness: a neo-institutional perspective*. https://www.researchgate.net/publication/355201244

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*. *5*(4). http://www.cisjournal.org

7 ANEXOS

Instrumento

Secção 1e 2

Caro Participante,

O meu nome é Matilde Costa e sou estudante do Mestrado em Contabilidade, Fiscalidade e Finanças Empresariais na Lisbon School of Economics and Management - Universidade de Lisboa. Assim, no âmbito da realização do meu Trabalho Final de Mestrado, elaborei o presente questionário cujo objetivo é a recolha de dados para a avaliação da **Eficácia da Auditoria de Cibersegurança em Portugal**.
Escasseia a literatura relacionada com este tema, pelo que, apelo à V/ colaboração com resposta, para aumentar o conhecimento nesta área.
Não existem respostas corretas ou erradas, e o questionário é totalmente **anónimo**. Por isso, responda com a maior sinceridade.
Os dados recolhidos serão apenas para fins académicos, sendo **confidenciais**.

Ao responder a este questionário está a contribuir para a recolha de dados para uma tese de Mestrado que pretende estudar a eficácia da auditoria de cibersegurança em Portugal. Futuramente, pode pedir a sua eliminação ou correção, de acordo com o **Regulamento Geral sobre a Proteção de Dados**.
O prazo de resposta irá decorrer até ao dia 25 de junho.

Caso tenha alguma **dúvida**, não hesite em contactar-me por endereço eletrónico (matildejgc@aln.iseg.ulisboa.pt) ou por contacto telefónico (917 221 917)

A sua participação é muito importante!
Obrigada!

É profissional de Auditoria Interna? *

- ◯ Sim
- ◯ Não

Secção 3

Qual é o seu género? *

- ◯ Feminino
- ◯ Masculino
- ◯ Outro

Qual é a sua idade? *

Short answer text

É especialista em Sistemas de Informação ou de Cibersegurança? *

- ◯ Sim
- ◯ Não

Das regiões indicadas, qual é a que corresponde à área da sua residência? *

- ○ Norte
- ○ Centro
- ○ Lisboa
- ○ Alentejo
- ○ Algarve
- ○ Região Autónoma dos Açores
- ○ Região Autónoma da Madeira

Das seguintes opções, qual é o seu grau de habilitações? *

- ○ 1.º Ciclo do Ensino Básico (4.º Ano)
- ○ 2.º Ciclo do Ensino Básico (6.º Ano)
- ○ 3.º Ciclo do Ensino Básico (9.º Ano)
- ○ Ensino Secundário (12.º Ano)
- ○ Licenciatura/Bacharelato
- ○ Mestrado/Pós-Graduação
- ○ Doutoramento

Na sua organização, ocupa um cargo de chefia? *

- ○ Sim
- ○ Não

Secção 4

Das seguintes opções, qual se aproxima da dimensão da sua empresa? *

- ○ Menos de 10 colaboradores
- ○ Entre 11 a 50 colaboradores
- ○ Entre 51 a 250 colaboradores
- ○ Mais de 250 colaboradores

Qual dos seguintes setores de atividade opera a sua empresa? *

- ◯ Agricultura, Produção Animal, Caça, Floresta e Pesca
- ◯ Indústrias Extrativas
- ◯ Indústrias Transformadoras
- ◯ Eletricidade, Gás, Vapor, Água quente e fria e Ar frio
- ◯ Captação, Tratamento e Distribuição de água; Saneamento, Gestão de Resíduos e De...
- ◯ Construção
- ◯ Comércio por grosso e a retalho; Reparação de veículos automóveis e motociclos
- ◯ Transportes e Armazenagem
- ◯ Alojamento, restauração e similares
- ◯ Atividades de informação e de comunicação
- ◯ Atividades financeiras e de seguros
- ◯ Atividades imobiliárias
- ◯ Atividades de consultoria, cíentificas , técnicas e similares
- ◯ Atividades administrativas e dos serviços de apoio
- ◯ Administração Pública e Defesa; Segurança Social Obrigatória
- ◯ Educação
- ◯ Atividades de saúde humana e apoio social
- ◯ Atividades artísticas, de espetáculos, desportivas e recreativas
- ◯ Outras atividades de serviços
- ◯ Atividades das famílias empregadoras de pessoal doméstico e atividades de produç...
- ◯ Atividades dos organismos internacionais e outras instituições extra-territoriais

...

Qual das seguintes tipologias de ativos descreve melhor os ativos da sua empresa? *

- ◯ Ativos Financeiros
- ◯ Ativos Tangíveis
- ◯ Ativos Intangíveis: Projectos de desenvolvimento
- ◯ Ativos Intangíveis: Goodwill
- ◯ Ativos Intangíveis: Programas de Computador
- ◯ Ativos Intangíveis: Propriedade Industrial
- ◯ Ativos Intangíveis: Outros Ativos Intangíveis
- ◯ Outros Ativos

Secção 5

A Auditoria Interna está proativamente familiarizada com a exposição e cenário de cibersegurança da organização? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna está proativamente familiarizada com os benchmarks do setor e tendências de gestão de riscos de cibersegurança? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

Existe cooperação entre a Auditoria Interna e as funções de Segurança de Informação? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna realiza uma avaliação à maturidade da gestão de risco de cibersegurança da organização? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna discute a maturidade da gestão de riscos de cibersegurança com a gestão e com o conselho de auditoria da organização? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna identifica os processos de gestão de risco que o conselho ou a gestão exigem garantia? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna apoia a gestão na melhoria da gestão de riscos de cibersegurança através da realização de consultorias? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna utiliza uma abordagem de auditoria interna baseada em risco relativamente à cibersegurança? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna avalia o alinhamento entre a estratégia geral da organização e a estratégia de cibersegurança? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

Secção 6

A Auditoria Interna procura identificar a localização e forma de armazenamento de ativos digitais valiosos da organização como, por exemplo, bases de dados? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna realiza uma avaliação de risco que permita compreender a vulnerabilidade associada ao armazenamento dos ativos digitais mais valiosos? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna avalia o impacto e probabilidade do roubo ou comprometimento desses ativos digitais? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna procura identificar outros ativos digitais, bem como os seus níveis de proteção, valor e vulnerabilidade? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna avalia as capacidades dos Recursos Humanos em termos de cibersegurança? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

A Auditoria Interna preocupa-se com a formação e sensibilização dos colaboradores em matérias de cibersegurança? *

	1	2	3	4	5	
Nada	○	○	○	○	○	Totalmente

Secção 7

Das estruturas de gestão de riscos de cibersegurança indicadas abaixo, indique aquela que a sua organização utiliza *

- ☐ Não é utilizado nenhum framework
- ☐ COBIT
- ☐ NIST
- ☐ AICPA
- ☐ International Organization for Standardization (ISO)
- ☐ Other...

Secção 8

Qual é a duração do seu ciclo de auditoria? (insira apenas o número, em meses) *

Short answer text

Secção 9

	Esta área não é verificada	Inquéritos/Questionários	Observação	Inspeção	Procedimer Analítico
Gestão de Riscos de Cibersegurança	☐	☐	☐	☐	☐
Segurança de Software	☐	☐	☐	☐	☐
Proteção de Dados	☐	☐	☐	☐	☐
Segurança da Nuvem	☐	☐	☐	☐	☐

	Esta área não é verificada	Inquéritos/Questionários	Observação	Inspeção	Procedimento Analíticos
Gestão de Acessos e de Identidade	☐	☐	☐	☐	☐
Gestão de Terceiros	☐	☐	☐	☐	☐
Segurança de Infraestrutura	☐	☐	☐	☐	☐
Gestão da Força de Trabalho	☐	☐	☐	☐	☐

	ritos/Questionários	Observação	Inspeção	Procedimentos Analíticos	Reexecução
Gestão de Ameaças e Vulnerabilidade	☐	☐	☐	☐	☐
Monitorização	☐	☐	☐	☐	☐
Gestão de Crises	☐	☐	☐	☐	☐
Resiliência Empresarial	☐	☐	☐	☐	☐

A AI verifica a utilização e os resultados das ferramentas de cibersegurança como parte das actividades de garantia em cada ciclo de auditoria? (Assinalar todas as opções aplicáveis)

- ☐ Ferramentas de Monitorização da Segurança da Rede
- ☐ Ferramentas de Encriptação
- ☐ Ferramentas de Análise de Vulnerabilidades da Web
- ☐ Ferramentas de Defesa de Rede sem Fios
- ☐ Packet Sniffers
- ☐ Software Antivírus
- ☐ Firewall
- ☐ Managed Detection Services
- ☐ Testes de Penetração
- ☐ Sistema de Deteção de Intrusões
- ☐ Other: _____

Secção 10

Qual a sua avaliação acerca dos planos de recuperação (Disaster Recovery) para situações adversas da organização? *

	1	2	3	4	5	
Negativa	○	○	○	○	○	Excelente

Indique o número aproximado de incidentes de cibersegurança que vitimizaram a sua empresa nos últimos 5 anos (Insira apenas o número) *

Your answer

Qual é o valor aproximado, em percentagem do ativo, do investimento em cibersegurança na sua empresa nos últimos 5 anos? (Indique apenas o número) *

Your answer

Secção 11

Existe algum seguro específico para cobrir riscos de cibersegurança na sua organização? *

- ○ Sim
- ○ Não

Secção 12

Com que frequência comunica os resultados de eficácia de gestão de riscos de cibersegurança ao Conselho? *

- ○ Nunca
- ○ Períodos inferiores a 2 anos
- ○ Períodos de 2 anos
- ○ Anualmente
- ○ Trimestralmente ou em todas as reuniões do Conselho de Auditoria

A Auditoria Interna emite uma opinião independente ao Conselho sobre a governance de cibersegurança, gestão de riscos e controlos internos? *

- ○ Sim
- ○ Não

Tabelas de Análise Estatística Descritiva

Questão	Opções	N	Percentagem
Género	Feminino	29	34,9
	Masculino	54	65,1
Idade	18 a 25 anos	21	21,9
	26 a 30 anos	27	28,1
	31 a 40 anos	23	24
	Superior a 40 anos	12	12,5
Habilitações	Doutoramento	2	2,4
	Mestrado/Pós-Graduação	45	54,2
	Licenciatura	35	42,2
	Ensino Secundário (12.º ano)	1	1,2
Região	Alentejo e Algarve	5	6
	Centro	12	14,5
	Lisboa	28	33,7
	Norte	35	42,2
	Região Autónoma da Madeira e Região Autónoma dos Açores	3	3,6
Cargo de Chefia	Sim	37	44,6
	Não	46	55,4
Especialização em SI	Sim	60	72,3
	Não	23	27,7

Fonte: SPSS

Questão	Opções	N	Percentagem
Colaboradores da empresa	Menos de 10 colaboradores	7	7,3
	Entre 11 a 50 colaboradores	20	24,1
	Entre 51 a 250 colaboradores	24	28,9
	Mais de 250 colaborarores	32	38,6
Setor de Atividade	Transportes e Armazenagem	4	4,8
	Outras atividades de serviços	38	45,8
	Indústrias Transformadoras	3	3,6
	Indústrias Extrativas	1	1,2
	Eletricidade, Gás, Vapor, Água quente e fria e Ar frio	2	2,4
	Educação	3	3,6
	Comércio por grosso e a retalho; Reparação de veículos automóveis e motociclos	2	2,4
	Captação, Tratamento e Distribuição de água;Saneamento, Gestão de Resíduos e Despoluição	2	2,4
	Atividades Imobiliárias	1	1,2
	Atividades financeiras e de seguros	13	15,7
	Atividades dos organismos internacionais e outras instituições extra-territoriais	1	1,2
	Atividades de informação e comunicação	1	1,2
	Atividades de consultoria, cientificas, técnicas e similares	7	8,4
	Alojamento, restauração e similares	2	2,4
	Agricultura, produção animal, caça, floresta e pesca	2	2,4
	Administração Pública e Defesa; Segurança Social Obrigatória	1	1,2
Tipos de Ativos	Ativos Tangíveis	12	14,5
	Ativos Financeiros	19	22,9
	Ativos Intangíveis: Propriedade Industrial	4	4,8
	Ativos Intangíveis: Projetos de desenvolvimento	12	14,5
	Ativos Intangíveis: Programas de computador	28	33,7
	Ativos Intangíveis: Outros Ativos Intangíveis	3	3,6
	Outros Ativos	5	6

Fonte: SPSS