INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

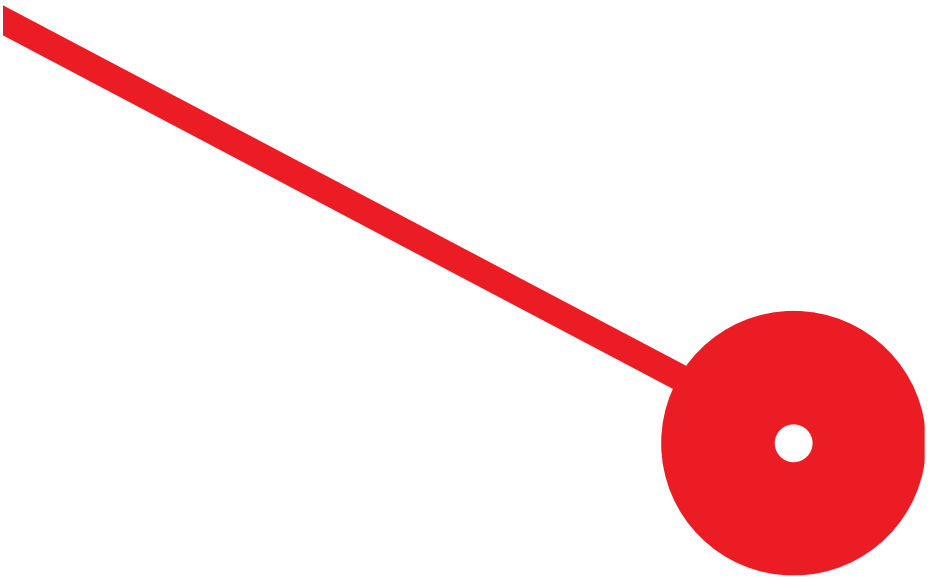
M MESTRADO
CONTABILIDADE E FINANÇAS

# Cibersegurança nas áreas de Contabilidade e Finanças das PME's

# Cybersecurity in the Areas of Accounting and Finance for SME's

Gonçalo Filipe Oliveira Santos

10/2024



Gonçalo Filipe Oliveira Santos. Cybersecurity in the areas of Accounting and Finance for SME's 10/2024

INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

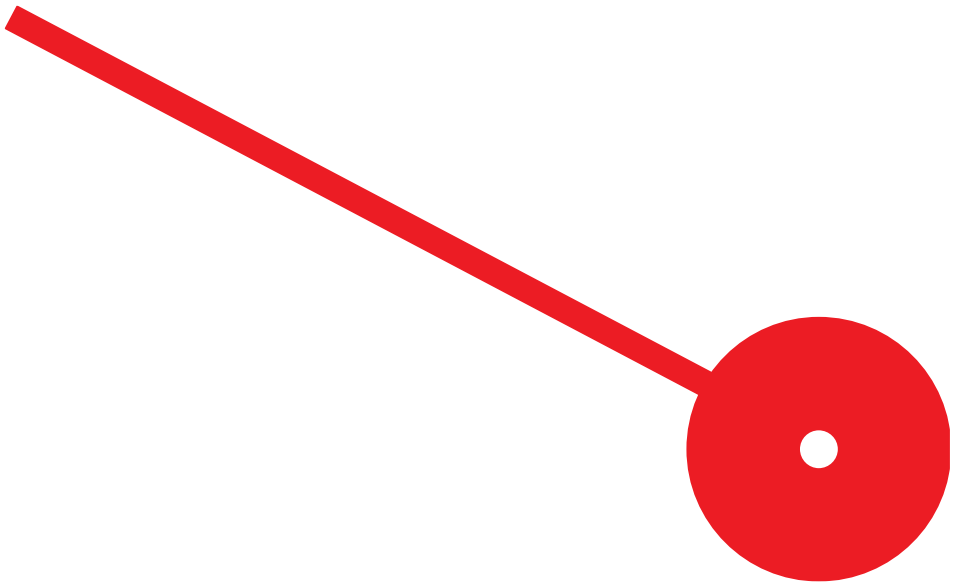
M MESTRADO
CONTABILIDADE E FINANÇAS

# Cibersegurança nas áreas de Contabilidade e Finanças das PME's

# Cybersecurity in the Areas of Accounting and Finance for SME's

Gonçalo Filipe Oliveira Santos

**Dissertação de Mestrado apresentada ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Contabilidade e Finanças, sob orientação da Professora Doutora Amélia Cristina Ferreira da Silva**



Gonçalo Filipe Oliveira Santos. Cybersecurity in the areas of Accounting and Finance for SME's
10/2024

## Agradecimentos

Durante todo o meu percurso académico contei, não só com o apoio da minha família, como também da Inês Miranda.

Sem dúvida que seu o amor, carinho, paciência e sobretudo insistência, não me teria sido possível finalizar este capítulo. Obrigado por estarem sempre lá.

Agradeço ainda, a todos os meus amigos e colegas que me apoiaram ao longo deste percurso.

Por fim, agradeço à Professora Doutora Amélia Cristina Ferreira da Silva pela disponibilidade, colaboração e dedicação neste estudo.

## Resumo

O presente estudo examina o papel da cibersegurança nas funções de contabilidade e finanças em pequenas e médias empresas (PME's), setores particularmente vulneráveis a ameaças cibernéticas devido à natureza sensível dos dados financeiros que gerem e às suas limitações em recursos de cibersegurança. Embora a literatura existente seja focada, sobretudo na cibersegurança em grandes organizações, esta pesquisa aborda uma lacuna importante ao centrar-se especificamente nas PME's.

Através de uma metodologia em duas fases — que combina entrevistas a especialistas com um inquérito quantitativo — este estudo explora como as práticas de cibersegurança, o envolvimento dos colaboradores e a qualidade dos sistemas de informação contabilística (QSIC), influenciam a qualidade da informação contabilística (QIC). Os resultados demonstram que o QSIC é fundamental para garantir a integridade dos dados, verificando-se fortes correlações entre QSIC e QIC. Adicionalmente, o estudo revela que o conhecimento, as atitudes e os comportamentos dos colaboradores em relação aos protocolos de cibersegurança têm um impacto significativo na segurança dos dados, sublinhando a necessidade de uma formação contínua e de uma rigorosa adesão às políticas. Embora esta investigação reforce teorias existentes sobre a importância da cibersegurança, acrescenta perspetivas específicas adaptadas ao contexto de restrição orçamental das empresas em estudo.

O estudo recomenda que estas entidades adotem uma abordagem equilibrada à cibersegurança, integrando controlos tecnológicos com medidas comportamentais para uma proteção de dados mais eficaz. Estudos futuros deverão expandir estes resultados, explorando tecnologias emergentes como a IA e o *blockchain* no contexto das PME's. Deve ainda, ser incorporado a formação em cibersegurança nos currículos dos profissionais das áreas em estudo, de modo a capacitar competências essenciais em segurança digital. Esta pesquisa destaca a necessidade urgente de estratégias proativas de cibersegurança nas pequenas e médias entidades, reforçando a importância de práticas rigorosas de proteção de dados para a manutenção da integridade financeira numa economia digital interconectada.



**Palavras-chave:** Cibersegurança, PME's, Qualidade dos Sistemas de Informação Contabilística, Qualidade da Informação Contabilística, Proteção de Dados, Gestão de Risco Cibernético, IA, *Blockchain*.

## Abstract

This study examines the role of cybersecurity in the accounting and finance functions of small and medium-sized enterprises, sectors increasingly vulnerable to cyber threats due to their sensitive financial data and limited cybersecurity resources. While substantial literature emphasizes cybersecurity in larger organizations, this research addresses a critical gap by focusing specifically on SME's.

Using a dual-phase methodology, combining expert interviews with a quantitative survey, this study explores how cybersecurity practices, employee engagement, and the quality of accounting information systems influence the quality of accounting information. The findings demonstrate that QAIS is central to ensuring data integrity, with strong correlations observed between QAIS and QAI. Additionally, the study reveals that employees' knowledge, attitudes, and behaviors toward cybersecurity protocols significantly impact data security, underscoring the need for continuous training and policy adherence. While the research supports existing theories on cybersecurity's importance, it contributes unique insights tailored to the resource-constrained environment of the companies being studied.

The study recommends that these companies should adopt a balanced approach to cybersecurity, integrating both technological controls and behavioral measures to enhance data protection. Future research should expand these findings by exploring emerging technologies such as AI and blockchain in SME contexts and incorporating cybersecurity training into accounting curricula to equip finance professionals with essential digital security skills. This research highlights the pressing need for proactive cybersecurity strategies in small and mid-entities, reinforcing the importance of vigilant data protection practices in maintaining financial integrity within an interconnected digital economy.

**Key words:** Cybersecurity, SME's, Accounting Information Systems, Quality of Accounting Information, Data Protection, Cyber Risk Management, AI, Blockchain.

# Contents

## List of Figures

## List of Tabels

## List of Abbreviations

AI – Artificial intelligence

CC – Cybersecurity Countermeasures

CSIRT – Computer Security Incident Response Team

DoS – Denial-of-service

EDI – Electronic Data Interchange

EIoIS – External Integration of Information Systems

EU – European Union

Fintech – Financial Technology

GDPR – General Data Protection Regulation

ICT – Information and Communication Technology

IEC – International Electrotechnical Commission

ISO – International Organization for Standardization

IoT – Internet of Things

IT – Information Technology

NIST – National Institute of Standards and Technology

P2P – Peer to Peer

QAI – Quality of Accounting Information

QAIS – Quality of Accounting Information Systems

Regtech – Regulatory Technology

RPA – Robotic process automation

SME's – Small and Medium-sized Enterprises

USB – Universal Serial Bus

# CHAPTER I – INTRODUCTION

Nowadays, most services, from personal finance to national infrastructure, are, to some extent, connected to a computer network, making them increasingly vulnerable to cyberattacks, which are becoming more frequent (Saravanan & Bama, 2019). Small and medium-sized enterprises, particularly those in accounting and finance, face unique and ongoing cybersecurity challenges due to the sensitive nature of financial data they manage. Handling valuable and often confidential information, these sectors are increasingly targeted by cybercriminals, facing threats that range from financial extortion to service disruptions through DoS attacks, both of which can compromise system performance and operational continuity (World Economic Forum, 2016; Centro Nacional de Cibersegurança Portugal, 2023). Muravskyi (2021) suggests that the effectiveness of cybersecurity practices within organizations is closely linked to the robustness of their accounting systems, further emphasizing the necessity of rigorous information protection practices, particularly in SME's.

The adoption of emerging technologies, such as blockchain, robotic process automation, Internet of Things, Big Data, Cloud Computing and Artificial intelligence, is transforming the financial sector, highlighting the importance of effective internal cybersecurity controls to prevent vulnerabilities (Smith, 2020; Hassani, Huang, & Silva, 2018). The rise of Cloud Computing and IoT, while bringing innovative efficiencies, has also revealed considerable weaknesses and highlighted potential interconnected consequences. Pendley (2018) emphasizes that basic security practices and critical data identification are essential for better protection against illegal cyber activities. Additionally, research by Matarneh et al. (2020) underlines that effective implementation of cybersecurity management can significantly reduce the risks associated with cloud-based accounting. Blockchain, for instance, is recognized for its decentralized and immutable structure, which provides transparency and integrity in financial transactions, yet it also presents implementation challenges due to cost and expertise requirements (Wang, Lin, & Luo, 2019; Algrari & Ahmed, 2019). This reinforces the need for solid security policies and efficient management of cybersecurity information. Such measures are crucial for ensuring the integrity and confidentiality of financial data, a vital aspect of trust and sustainability in business.

This context underscores the importance of proactive cybersecurity strategies in accounting and auditing, highlighting the need for Accounting Professionals to continuously adapt to new technological realities and emerging cyber threats. Furthermore, a proactive stance among finance and accounting professionals is essential

to developing secure technology environments. This proactive engagement demands an understanding of cybersecurity practices that extend beyond technical basics, urging finance professionals to actively participate in security practices (Pendley, 2018; Parsons et al., 2017). These practices include rigorous management of security policies and ongoing cybersecurity training, fostering a proactive and informed organizational culture in data protection (Callen-Naviglia & James, 2018; European Union Agency for Cybersecurity, 2020). The resilience of accounting systems and effective information management emerges as foundational to business cybersecurity, underscoring the importance of integrating emerging financial technologies while implementing strategies that effectively mitigate cyber risks (Fadziso et al., 2023).

This study investigates the impact of cybersecurity practices of SME on accounting information quality. To understand SME cybersecurity practices, the study seeks answers to several questions: How do organizations identify cybersecurity threats, incidents, and breaches? What are the organizational responses to cybersecurity risks and incidents? To what extent are certified accountants and financial managers involved in managing information security? What factors determine this level of involvement?

Employing a dual-phase methodological approach, this study combines expert interviews with questionnaires directed at certified accountants and financial managers, thereby offering an empirically grounded model of cybersecurity practices tailored for SME's. By examining the intersection of technological and behavioral factors in this focused context, this research not only reinforces existing theories but also aims to provide actionable insights for strengthening cybersecurity resilience in resource-limited environments (Cao, 2020; Saravanan & Bama, 2019) where accounting operates.

## 2.1. Technologies for Cybersecurity

Cybersecurity, defined as protection against digital attacks on systems, networks, and data connected to the Internet, has undergone significant changes over time. With the increase in connected devices and sensitive programs and the growth in the methods and skills of so-called “cyber attackers,” cybersecurity has become a crucial element in data and system protection strategies (Fadziso et al., 2023).

Initially focused on defending governmental infrastructures and data, this field has expanded to cover all entities, including small and medium-sized enterprises. Thus, cyber threats have evolved from the first computer viruses, which attacked isolated computers, to large-scale, sophisticated attacks using multiple vectors, more commonly known as Generation V attacks. These developments highlight the importance of initiative-taking approaches and ongoing risk management, especially for SME’s in the financial and accounting sectors (Fadziso et al., 2023).

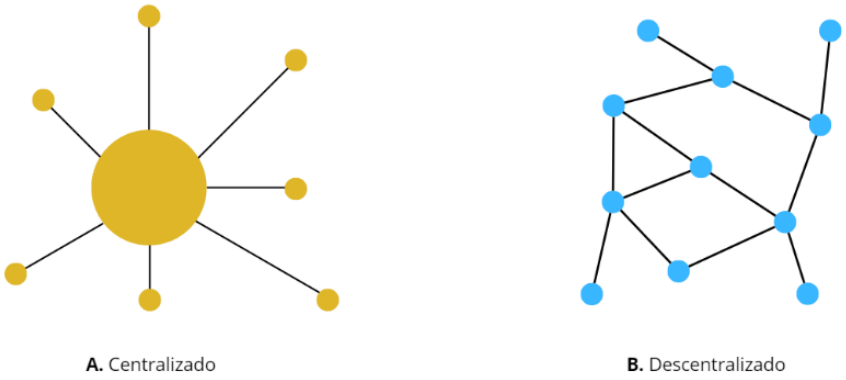
The evolution of cybersecurity has extended beyond traditional data protection to encompass the security of “cyber-physical” systems. These systems do not also connect physical and digital components, but are crucial for critical infrastructures, such as power grids. This expansion of cybersecurity reflects a shift from a data-centered defense, toward ensuring operational security in complex technological environments, emphasizing the importance of a multifaceted approach (Fadziso et al., 2023).

Blockchain technology, for instance, is valued for its decentralized and immutable nature, enhancing data protection, transparency, and the integrity of financial transactions. It is considered a milestone in technological innovation, having revolutionized various sectors, particularly the ones under study. This technology not only strengthens data security but also introduces new paradigms for financial and accounting management due to its capacity to ensure integrity and transparency in transactions.

Going back to its beginning, blockchain emerged in 2008 as an innovative response to recording transactions within a peer-to-peer system, aiming to eliminate intermediaries and enable direct transactions between the parties involved (Merugula et al., 2021). The historical development of blockchain can be categorized into three distinct phases: Blockchain 1.0, focused on cryptocurrency use and simple value transfers; Blockchain 2.0, which introduced smart contracts and more complex applications, including property and investments; and Blockchain 3.0, which further expanded its

applications beyond financial services (Merugula et al., 2021). In terms of cybersecurity, blockchain's decentralized structure promotes a solid defense mechanism against conventional cyberattacks, which often exploit vulnerabilities in centralized systems. The contrast between the centralized model (Figure 1A) and blockchain's decentralized model (Figure 1B) underscores how blockchain ensures that each transaction is simultaneously recorded in multiple locations, not only hindering fraud but also allowing for its rapid detection (Merugula et al., 2021).

*Figure 1 - Blockchain Structure.*




*Source: Own elaboration based on the article Study of Blockchain technology in Empowering the SME (Merugula et al., 2021)*

The primary function of the blockchain network is to operate as an autonomous entity that manages its own online services or digital currencies, which are conducted and exchanged under predefined requirements. The main feature is the registration and verification of software code on the blockchain, ensuring immutability and security against interference, as represented in figure2. Security mechanisms, implemented as software algorithms, enable secure data exchange between unknown and untrusted entities without the need for intervention by a centralized authority (Merugula et al., 2021).


*Figure 2 - How does blockchain work?*
*Source: Own elaboration based on the article Study of Blockchain technology in Empowering the SME (Merugula et al., 2021)*

The applications of this technology go beyond simple value transfers. This decentralization mechanism offers a solid defense against conventional cyberattacks, paving the way for innovations in the banking sector, where the technology transforms how information is managed and stored, providing an additional layer of security and efficiency. This is crucial for SME's, which, due to budget constraints, may not have previously had access to advanced cybersecurity solutions (Al Kemyani et al., 2022).

However, implementing this technology also presents challenges, particularly regarding technological adaptation and understanding by managers and employees. It is essential that SME's not only adopt blockchain but also invest in training their employees to maximize the benefits of this technology (Al Kemyani et al., 2022). However, companies face hurdles in implementing blockchain, including high costs and the necessity of technical expertise (Wang, Lin, & Luo, 2019). With its advancement and growing understanding of its benefits and challenges, it is expected that its adoption will become increasingly mainstream among these enterprises, shaping the future of cybersecurity in an increasingly digitized and interconnected business environment.

In the meantime, AI has demonstrated significant potential in advancing cybersecurity by enabling proactive threat detection and response capabilities. Mishra (2023) highlights AI's ability to analyze vast datasets, detecting complex patterns to preemptively identify malware and other security threats. However, effective deployment

of artificial intelligence also requires a careful balance with data privacy and regulatory compliance (Mishra, 2023). Additionally, Cao (2020) describes AI's role in optimizing risk management, where machine learning enhances the adaptability of cybersecurity measures in the dynamic financial sector (Cao, 2020). AI-driven behavioral analysis tools can further enhance cybersecurity by examining user patterns to detect suspicious activities, enabling real-time intervention before an attack occurs. By integrating these advanced technologies, SME's can navigate the complexities of today's cyber landscape with improved resilience.

## 2.2. Cyber Resilience and Mitigation Strategies

In today's digital landscape, small and medium-sized enterprises face substantial challenges due to the growing complexity of cyber threats. Emerging technologies like artificial intelligence and blockchain promise to transform cybersecurity practices and financial management, introducing new paradigms of security and operational efficiency (Smith, 2020). However, adopting these technologies in SME's often involves specific barriers, such as infrastructure costs and the need for skilled management.

SME's operate within a constantly evolving regulatory environment, which adds complexity to implementing emerging technologies. For instance, European legislation, such as the GDPR, imposes strict requirements that can be challenging for these companies without extensive resources or specialized knowledge (European Union Agency for Cybersecurity, 2020).

The evolution of FinTech and RegTech technologies also plays a role in adapting these companies to a more secure digital environment. These technologies not only facilitate regulatory compliance but also introduce innovative cybersecurity methods to proactively address rapidly evolving digital threats (Callen-Naviglia & James, 2018). Among these methods, multi-factor authentication is widely adopted by RegTechs and other entities, enhancing online security by requiring multiple authentication layers. Additionally, FinTechs leverage advanced encryption techniques to protect data during transmission and storage, safeguarding sensitive information from unauthorized access.

Building cyber resilience in SME's involves a proactive, layered defense approach, integrating advanced detection technologies, regulatory frameworks, and strategic planning. AlBenJasim et al. (2023) emphasize that for these enterprises, in finance, cyber resilience should encompass a comprehensive cybersecurity framework

that covers threat detection, risk management, and response capabilities throughout the business's lifecycle. For SME's, this layered security model helps to address challenges posed by limited resources and growing attack surfaces, particularly in industries handling sensitive financial data.

According to the European Union Agency for Cybersecurity (2020) aligning with standards such as ISO/IEC 27001 reinforces SME's' ability to manage cybersecurity systematically, guiding them in identifying vulnerabilities and implementing targeted, effective protections. This structured approach ensures resilience by incorporating risk assessment, continuous monitoring, and incident response protocols, which safeguard data integrity and availability. The Centro Nacional de Cibersegurança Portugal (2023) underscores the value of localized strategies, noting the need for cybersecurity practices adapted to regional threats and legal requirements, which is particularly relevant for SME's aiming to comply with both European and Portuguese standards.

The incorporation of advanced technologies such as artificial intelligence offers these companies significant advantages in detecting and mitigating threats in real-time. Agarwal et al. (2023) advocate for the use of AI-driven solutions in SME's, which not only enhance detection of anomalous activity but also automate responses to lower-level threats, thereby allowing businesses to focus resources on critical security functions. This can improve operational efficiency while reducing potential financial impacts of cyber incidents.

Furthermore, Çiftçi and Balcıoğlu (2023) highlight regulatory compliance as a cornerstone of cyber resilience for small and mid-caps. Regulatory adherence ensures that these companies operate within defined security parameters, maintaining standards that support both organizational security and trust. The authors suggest that regulatory compliance frameworks should not be perceived as burdens but rather as integral parts of the resilience strategy, guiding SME's in achieving a secure operational environment with structured, consistent practices.

Together, these strategies emphasize the importance of adopting a multi-faceted, compliance-oriented approach to cyber resilience in finance-focused SME's. By integrating regulatory standards, leveraging emerging technologies, and aligning with best practices in cybersecurity, they can strengthen their ability to withstand and respond to cyber threats effectively.

Cybersecurity regulations are foundational to operational security within the financial sector, especially for small and medium-sized enterprises that often operate with

limited resources to handle complex regulatory demands. In the European context, the European Union Cybersecurity Agency (2020) mandates measures such as intrusion detection systems and incident management protocols, designed to adapt to evolving threats in cybersecurity. These measures help protect critical infrastructures and preserve the integrity of financial operations, ensuring that SME's remain compliant with industry standards and secure against potential cyber threats.

As described before, blockchain technology is increasingly recognized as a transformative tool in financial accounting for its capacity to enhance data integrity and transparency, particularly through its immutable and decentralized ledger structure. Rula Almadadha (2024) emphasizes blockchain's potential in providing secure, transparent systems for transaction verification, which is invaluable for SME's striving to maintain regulatory compliance with limited resources. Furthermore, blockchain's role in safeguarding data through cryptographic methods and consensus protocols allows these companies to streamline compliance with data protection mandates like GDPR, enhancing both operational security and regulatory alignment.

In the context of FinTech, AlBenJasim et al. (2023) highlights the broad "attack surface" associated with digital financial platforms, which necessitates comprehensive cybersecurity frameworks. For small and medium-sized enterprises, implementing recognized standards, such as the NIST or ISO/IEC 27001, can help align with regulatory requirements while strengthening cybersecurity measures. These frameworks provide structured guidelines to protect data integrity, prevent unauthorized access, and ensure compliance with financial regulations. Additionally, the adoption of regulatory technologies offers a pathway for SME's to automate compliance processes, thus reducing the operational burden of regulatory adherence. Rula Almadadha (2024) notes that RegTech solutions, by simplifying regulatory complexity and enhancing cybersecurity defenses, empower SME's to focus on growth while ensuring they meet legal mandates effectively.

## 2.3. Cybersecurity in the Financial and Accounting Sector

The evolution of artificial intelligence and data science technologies has driven significant transformations in the fields of accounting and finance, especially within the context of FinTech. These technologies not only facilitate the implementation of complex accounting standards but also enhance the accuracy and efficiency of financial processes (Le Guyader, 2020). In recent years, the development and application of new AI techniques in FinTech have shown the potential to fundamentally transform the economy and finance. The synergy between AI, data science, and the need of the modern financial sector has, in a way, made FinTech smarter, safer, more personalized, and efficient. This includes the integration of advanced machine learning techniques and data analysis to improve financial products, services, and economic-financial systems (Cao, 2020).

Thus, artificial intelligence has shown a significant impact across multiple areas of the financial sector, including financial market analysis and forecasting, intelligent investment management, credit, and risk management. These technologies help simulate and model complex economic-financial relationships, improving decision-making and business strategy. Furthermore, AI and FinTech technologies, such as the previously discussed blockchain, are optimizing security, compliance, and risk management in the financial sector, facilitating new financial business models and revolutionizing existing practices, such as P2P lending, crowdfunding, and robot-advising (Cao, 2020).

Despite these notable advances, the adoption of AI in accounting and finance poses significant challenges, especially concerning data accuracy, ethics, and privacy. The reliance on AI solutions can create a skills gap, where professionals in these fields may become overly dependent on technology for tasks they previously fully understood (Le Guyader, 2019; Agarwal et al. (2023).

As technology advances, it will be crucial for these professionals to deeply understand both the technology and the accounting and financial principles it aims to serve. The future of AI in accounting and finance promises not only task automation but also the creation of new opportunities for strategic analysis and decision-making, thus shaping the future of the financial sector (Cao, 2020). In the current economic and technological landscape, the accounting and finance sectors are experiencing a notable increase in digital threats, driven by rapid digitalization. Emerging technologies, such as blockchain, RPA, and AI, are reshaping business operations, introducing new challenges in managing and protecting sensitive information (Smith, 2020).

However, this transformation heightens the risks of cyber-attacks and underscores the necessity of reinforcing cybersecurity procedures. The research points out the significance of cybersecurity risk management within accounting, emphasizing that robust security practices can greatly reduce vulnerabilities. This includes establishing comprehensive cybersecurity policies, implementing internal control systems, and continuous professional training as critical measures to maintain the integrity and confidentiality of financial data.

Smith (2020) highlights that despite the potential of these technologies to enhance automation and incorporate encryption, there is an essential focus on rigorous cybersecurity protocols, especially for SME's that may struggle to adapt to these more advanced technologies. Furthermore, Çiftçi and Balcıoğlu (2023) highlight the importance of a proactive approach in managing cyber risks, stressing the need for regulations and specific audits in the financial sector, suggesting that companies, in the absence of regulatory guidelines, should invest in security.

Cyberattacks in the financial and accounting sectors impose costs that extend beyond immediate damage, involving indirect costs like productivity losses, reputational harm, and increased borrowing expenses, which underline the need for a proactive response to the escalating complexity of cyber risks (Çiftçi & Balcıoğlu, 2023). The COVID-19 pandemic amplified these issues, accelerating digital transformation and increasing dependency on technologies susceptible to cyber threats. The shift to remote work and reliance on digital tools created new vulnerability points, prompting institutions to reinforce cybersecurity strategies and adapt swiftly to an evolving threat landscape (Deloitte, 2020). Financial professionals play a key role in combating these threats by developing secure IT environments and implementing effective cybersecurity practices. This proactive approach is essential to safeguarding critical organizational information (Pendley, 2018).

Accountants and financial professionals must remain vigilant regarding the regulatory implications of cybersecurity and data privacy. Familiarity with legislation and recommended practices is undoubtedly fundamental to maintaining the integrity and confidentiality of data (Pendley, 2018). In the European context, cybersecurity in the financial sector is closely connected to economic and political stability. Over recent years, the EU has advanced a "digital sovereignty" agenda, a framework emerging to address dependency on foreign digital infrastructures and services, particularly from major actors outside the EU like the United States and China. This approach, coined "Regulatory

Mercantilism," not only seeks to minimize reliance on foreign entities but also aims to strengthen cybersecurity resilience by fostering domestic digital capabilities. By positioning EU-based companies as trusted partners in security, the European Union aims to secure the financial sector from external threats and foster a more resilient digital landscape (Farrand & Carrapico, 2022).

The integration of blockchain in the financial sector, supported by regulatory sandboxes, allows companies to innovate within a controlled framework while adhering to regulatory requirements. Hassani et al. (2018) argue that regulatory sandboxes are particularly advantageous for SME's aiming to adopt blockchain-based solutions for secure, transparent, and efficient data management. These frameworks enable these companies to navigate complex regulatory landscapes with greater flexibility, fostering innovation while ensuring that security standards are upheld.

For the companies in finance and accounting, the convergence of blockchain, RegTech, and structured cybersecurity frameworks represents a robust approach to regulatory compliance. This integration not only addresses existing cybersecurity and data protection requirements but also positions SME's to manage future regulatory challenges in an increasingly digital financial landscape. The integration of cybersecurity in accounting goes far beyond the technical protection of data and is also an essential pillar to ensure trust in financial operations and regulatory compliance. Several recent studies have emphasized the importance of this integration, exploring its multiple impacts and approaches within the field of accounting.

Boss et al. (2022) stress the pressing need to include cybersecurity at all levels of accounting curricula. According to the authors, despite the high focus on this area and increased regulation, its curriculum coverage is often limited to information systems accounting courses. The study suggests introducing practical cybersecurity concepts in various accounting courses, such as the disclosure of cyberattacks in financial reports, the impact of security breaches on audits, and the risks inherent to storing personal information.

In a complementary way, Cram et al. (2023) conducted a comprehensive review of the literature on cybersecurity in accounting information systems, categorizing studies into four main areas: cybersecurity risks and threats, related controls and assurances, cybersecurity breaches, and mitigation strategies. This work highlights the need for additional research exploring the interaction between accounting information systems and cybersecurity, emphasizing the potential impact of this area on the future of accounting.

Eaton et al. (2019) propose a cybersecurity risk management model, highlighting how accountants' skills can be crucial for risk mitigation at various stages of the process. The study discusses the role accountants can play in both consulting and auditing, helping companies develop more robust risk management. High-profile security incident examples are used to reinforce their arguments.

Conversely, Haapamäki and Sihvonen (2019) focus on internal auditing and controls, arguing that a well-structured internal audit and effective controls are essential to mitigate cybersecurity risks in accounting. For the authors, investment in cybersecurity should be seen as a strategic priority, fundamental to ensuring the financial sustainability of companies.

Janvrin and Wang (2022) present a conceptual framework for responding to cybersecurity events, analyzing the impact these events can have on accounting, both financially and non-financially. They also propose response strategies based on empirical research to guide organizations in preparing for and mitigating incidents. The relevance of protecting accounting data in the digital environment is also underscored by Laichuk et al. (2023), who highlight the need for advanced computer systems to ensure the confidentiality, integrity, and authenticity of transmitted data. The study points to the increasing sophistication of cyber threats as a driving factor for the importance of information security, particularly concerning financial transactions.

Moreover, Li et al. (2023) explores the impact of professional skepticism on accounting students' performance in cybersecurity-related tasks. They identify that operational stress and certain personality traits can negatively influence cybersecurity performance, reinforcing the need to include specific cybersecurity training in accounting curricula.

Litt et al. (2023) examine the impact of a security breach on the reputation of one of the Big Four auditing firms, Deloitte. The study reveals that the breach resulted in significant damage to the company's reputation, affecting client approval and fees charged, and suggests that such incidents have far-reaching implications for auditors' reputations.

In turn, Mendoza et al. (2023) conducted a comparative study on cybersecurity habits among accounting and management university students in Mexican universities. The study identified the urgent need for curricular and extracurricular training in cybersecurity, emphasizing the correlation between cybersecurity knowledge and the security practices adopted by students.

Pendley (2018) argues that accounting and finance professionals must take a proactive approach to creating more secure IT environments. The author presents essential behaviors, organizational policies, and tools that accountants can use to prevent common cyber threats, reinforcing the need for these professionals' direct involvement in cybersecurity.

Rodger and George (2017) apply the triple bottom line approach to the global natural gas supply chain, proposing a sustainable economic model that balances accounting principles with environmental concerns. The study presents an innovative view by integrating sustainability and cybersecurity, proposing solutions aimed at reducing cyber vulnerability in global supply chains.

Finally, Zadorozhnyi et al. (2020) and Zadorozhnyi et al. (2021) emphasize the importance of using accounting as a foundation for ensuring corporate cybersecurity. They argue that accounting policy and internal regulations should serve as a platform for developing cybersecurity standards. The authors also explore the application of biometric technologies in accounting, suggesting that these technologies can improve data security, time tracking, and payroll management.

Thus, we can conclude that the intersection between cybersecurity and accounting is becoming increasingly significant. Protecting accounting data is a strategic necessity, directly impacting organizations' reputation, compliance, and operation. Research in this area highlights the importance of an integrated cybersecurity curriculum, the strengthening of internal controls, and the adoption of advanced technologies such as biometrics. Accounting professionals thus have a crucial role to play in safeguarding the integrity and confidentiality of financial data, contributing to the resilience of companies against growing cyber threats.

## 2.4. Cybersecurity practices and accounting information quality

With companies increasing reliance on digital systems for financial data management, understanding factors contributing to robust and reliable accounting information systems is essential for effective decision-making and compliance. Since cybersecurity is an important dimension of digital accounting, it is crucial to understand the relationship between professional and organizational practices regarding cybersecurity and how it influences the quality of accounting information.

***H1: The External Integration of Information System positively impacts the Quality of Accounting Information Systems***

The external integration of information systems, which represents the connectivity between an organization's internal systems and those of external partners, suppliers, and clients, has been recognized as a critical factor in the effectiveness of accounting information systems. Studies indicate that external system integration through technologies like Electronic Data Interchange (EDI) and extranets significantly contributes to data accuracy and efficiency in accounting (Zhao, Huo, Sun, & Zhao, 2013). These systems enable real-time information exchange and improve supply chain efficiency by reducing errors, thus enhancing data quality.

According to Rai, Patnayakuni, and Seth (2006), information systems integration facilitates information sharing and coordination of interorganizational activities, which is essential for the quality of internal systems. Additionally, research by Wang, Tai, and Wei (2006) highlights that information integration among companies creates a more collaborative environment, positively impacting system quality and the reliability of processed information. Thus, it is expected that greater external integration of information systems will positively impact the quality of accounting information systems, justifying hypothesis H1.

***H2: Cybersecurity countermeasures have a positive impact on the quality of accounting information systems***

In an increasingly digitalized business environment, cybersecurity measures are essential to ensure the integrity and reliability of information systems. Cybersecurity countermeasures, such as firewalls, anti-malware, and intrusion detection systems, are widely recommended to protect data from unauthorized access and ensure operational continuity (Baskerville et al., 2018). Chen, Ramamurthy, and Wen (2015) argue that organizational resilience, when supported by cybersecurity practices, enhances the security and quality of information systems.

Additionally, Straub and Welke (1998) found that implementing effective security measures fosters users' trust in information systems, increasing their adherence and proper use. These measures are crucial for ensuring that the accounting information system is secure, protected against external threats, and reliable, supporting the hypothesis that cybersecurity positively impacts the quality of accounting information systems.

***H3: The Knowledge of Policy and Procedures positively impacts the Quality of Accounting Information Systems***

Employees' knowledge of organizational security policies and procedures is vital for data protection and the effectiveness of accounting information systems. According to Parsons, McCormac, Butavicius, and Pattinson (2014), employees with a strong understanding of security policies are more likely to act preventively, identifying and responding to threats before they compromise system integrity. Similarly, Bulgurcu, Cavusoglu, and Benbasat (2010) emphasize that knowledge of security standards is directly linked to error reduction and risk mitigation.

In a broader analysis, D'Arcy, Hovav, and Galletta (2009) suggest that adequate training in security policies and incident response procedures significantly improves information systems effectiveness. This knowledge enables employees to act in an informed manner, which increases the quality of accounting information systems, justifying hypothesis H3.

***H4: The Attitude towards Policy and Procedures positively impacts the Quality of Accounting Information Systems***

Employee attitudes towards security policies and procedures are a critical determinant of compliance with security standards. Studies show that positive attitudes toward security policies are associated with greater adherence to established protocols, minimizing system vulnerabilities (Herath & Rao, 2009). When employees recognize the importance of following security policies, they tend to comply more rigorously, contributing to the effectiveness and security of information systems.

In examining employee behavior, Hu, Dinev, Hart, and Cooke (2012) found that positive attitudes toward information security increase the likelihood that employees will adopt secure practices in the workplace. This suggests that a favorable attitude toward security policies positively impacts the quality of accounting information systems, supporting hypothesis H4.

***H5: The Self-reported Behavior toward Policy and Procedures positively impacts the Quality of Accounting Information Systems***

Self-reported behavior regarding security policies and procedures reflects employees' daily practices in complying with security standards. This behavior includes actions such as regularly updating passwords, appropriately handling sensitive data, and

adhering to security protocols. Puhakainen and Siponen (2010) found that employee training and fostering a positive security environment encourage security behaviors essential for protecting information systems.

Additionally, Anderson and Agarwal (2010) demonstrate that proactive employee behaviors, such as compliance with security standards, reduce system vulnerabilities. Thus, self-reported behavior regarding security procedures is a direct indicator of accounting information systems quality, justifying hypothesis H5.

***H6: The Quality of Accounting Information Systems positively impacts the Quality of Accounting Information***

The quality of accounting information systems is a fundamental factor that directly impacts the quality of accounting information. Studies show that high-quality systems ensure that accounting information is accurate, reliable, and relevant, which is essential for organizational decision-making processes. Algrari and Ahmed (2019) argue that information system quality impacts the quality of the information generated, as robust, well-protected systems allow for the secure and efficient processing of data. According to Xu, Hu, and Xiao (2017), the quality of accounting information systems is essential for ensuring that the information generated meets reliability and accuracy requirements, strengthening decision-making and stakeholder confidence. Based on this, it is presumed that accounting information systems' quality positively impacts accounting information quality, justifying hypothesis H6.

The conceptual model represented in Figure 3 is designed to analyze the impact of cybersecurity and organizational practices on the quality of accounting information systems (QAIS) and, subsequently, the overall quality of accounting information (QAI) within small and medium-sized enterprises.

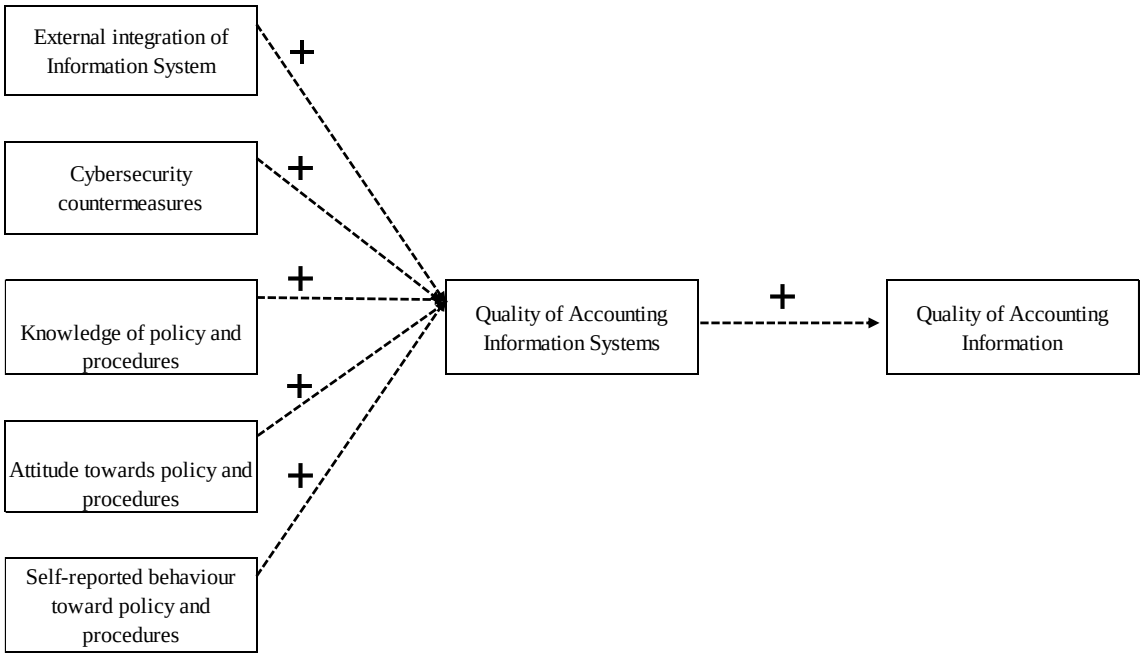



*Figure 3 - Conceptual model.*

## 3.1. Research objectives

The primary objective of this study is to understand and assess the impact of cybersecurity practices on accounting information. This overarching aim translates into specific goals, including exploring and evaluating the cybersecurity threats affecting SME's in accounting and finance, analyzing organizational response strategies, understanding the role and preparedness level of finance professionals (both accountants and managers) in information security, and identifying and analyzing the factors influencing these professionals involvement in cybersecurity management.

The research approach for this study is structured in two distinct phases, each contributing to the development and validation of the conceptual model. In Phase 1, a comprehensive document review was conducted, namely official reports of public entities regarding cybersecurity practices. It was important to contextualize the problem. After that, two cybersecurity specialists were interviewed. These interviews were conducted in July 2024, and it provided the foundational insights necessary to construct the initial conceptual model, offering a structured framework of key cybersecurity factors influencing accounting.

Phase 2 focused on the empirical validation of this model, wherein the model and its associated scales were rigorously tested. This testing phase ensured the reliability and accuracy of the scales, allowing for a robust assessment of the conceptual model's applicability. This two-phase methodology combines exploratory and confirmatory approaches, providing a comprehensive basis for understanding the influence of cybersecurity practices in accounting information.

## 3.2. Empirical contextual settings

Small and Medium Enterprises in Portugal face an increasingly challenging cybersecurity environment. Within the Portuguese context, the 2023 Cybersecurity Report highlights the growing importance of cybersecurity for organizations, emphasizing the need for continually adapting security strategies to a constantly evolving cyber landscape. This focus is essential because, despite increasing awareness of cyber risks, many of these companies still face significant challenges in developing and implementing effective protection strategies (Centro Nacional de Cibersegurança Portugal, 2023). Additionally, Catota, Morgan, and Sicker (2018) emphasize the critical role of cybersecurity incident response in Ecuador's financial sector, particularly in mitigating the impacts of cyberattacks on SME's. Their research highlights that these

organizations often lack resources and specialized personnel necessary for implementing dedicated incident response teams. The authors advocate for establishing a national CSIRT and enhancing information-sharing practices among financial institutions as essential measures to bolster cybersecurity resilience. However, financial and technical constraints significantly hinder SME's ability to adopt robust cybersecurity frameworks, leaving them more vulnerable to threats (Catota, Morgan, & Sicker, 2018).

In Portugal, the Bank of Portugal has been a key player in promoting cybersecurity in the financial system, adopting comprehensive strategies, forming specialized teams, and collaborating with national and international entities to prevent cybercrime. These practices foster a culture of knowledge-sharing in cybersecurity, addressing both information and physical security (Bank of Portugal, 2017).

Portugal's 2023 cybersecurity report highlights how increased connectivity across sectors—from personal finance to critical infrastructure—has intensified vulnerabilities to cyber threats. This connectivity, combined with the widespread integration of email, messaging, and social media into personal and professional spheres, has elevated exposure to attacks such as phishing, ransomware, and malware. The report stresses the urgent need for proactive cybersecurity measures, particularly for SME's, to protect sensitive data and ensure system resilience. It advocates a two-pronged approach: raising cybersecurity awareness at both public and organizational levels and strengthening investments in robust defense mechanisms. These strategies are essential to adapt cybersecurity policies to the fast-evolving technological landscape, especially within Portugal's SME ecosystem (Centro Nacional de Cibersegurança Portugal, 2023).

In 2023, individuals and SME's were among the most frequent targets of cyberattacks, with the public administration sector enduring the highest impact, primarily from ransomware, account compromise incidents, and phishing. The education, science, technology, higher education, and health sectors also saw significant cybersecurity challenges. Additionally, the report highlights emerging cybersecurity risks tied to the ongoing conflict in Ukraine and predicts that AI advancements will introduce more complex threats. Anticipated trends for 2024 include a rise in USB-based malware, misinformation propagated by generative AI, and escalating cyber sabotage and hacktivism (Centro Nacional de Cibersegurança, 2024).

Portugal's 2022 data revealed that 43% of companies had an ICT Security Policy reviewed within the past 24 months, a rate above the EU average of 32%. However, only 28% of companies had implemented multi-factor authentication, a key measure for

preventing unauthorized access. Furthermore, 72% of ICT security-related tasks were handled by external providers (Centro Nacional de Cibersegurança, 2023).

In comparing the cybersecurity budgets allocated by SME's in Portugal between 2022 and 2023, several trends emerge that reflect both continuity and incremental shifts in investment. In 2023, a significant 36.8% of SME's allocated less than €3,000 annually to cybersecurity functions, mirroring the trend seen in 2022, where a substantial portion of SME's also fell into this low-budget category. This consistency underscores a continued tendency among Portuguese SME's to allocate minimal funds to cybersecurity, despite the increasing cyber risks associated with expanding digital infrastructures (Centro Nacional de Cibersegurança, 2023).

For moderate budgets, 2023 saw around 17% of SME's committing between €3,000 and €8,000, with approximately 7% investing between €8,000 and €15,000. This allocation aligns with the data from 2022, where moderate budget levels reflected a cautious yet growing recognition of cybersecurity's importance (Centro Nacional de Cibersegurança, 2022, 2023). Meanwhile, the percentage of SME's committing to higher budget ranges (€15,000 to €50,000) remained steady in both 2022 and 2023 at about 6.6%. Additionally, only 3.4% of SME's in 2023 invested over €50,000, including nearly 1% with annual budgets surpassing €300,000, indicating that only a small fraction of SME's are making substantial investments in cybersecurity (Centro Nacional de Cibersegurança, 2023).

A concerning aspect of the 2023 data is the continued lack of dedicated cybersecurity budgets in some SME's; 8.6% reported having no cybersecurity budget, slightly up from 2022. Furthermore, 20.7% of SME's were uncertain or did not disclose their cybersecurity expenditure, which mirrors the previous year's data and points to a persistent issue of budget transparency and prioritization in this area (Centro Nacional de Cibersegurança, 2022, 2023).

The Bank of Portugal (2017) also emphasizes that cyber risks can compromise regulatory compliance and destabilize financial balance if adequate measures are not implemented.

In Portugal, the growing adoption of blockchain is evidenced by the interest of both the private sector and the government in exploring its different applications. The 2023 report from Portugal's National Cybersecurity Center highlights blockchain's role in enhancing information security, pointing to a growth trend in its use by SME's (Centro Nacional de Cibersegurança Portugal, 2023).

SME's in Portugal, particularly those in the studied areas, face several complex challenges regarding cybersecurity. Initially, as pointed out by Alahmari and Duncan (2021), limited financial capacity is a significant barrier. This budget constraint prevents many of these companies from adequately investing in advanced cybersecurity solutions, which is increasingly necessary as the sophistication of cyberattacks and dependence on digital systems grows.

Additionally, a lack of awareness about cyber risks poses a significant obstacle. According to the Bank of Portugal (2017), many SME's underestimate these risks, leading to insufficient investment in protective measures and subsequently increasing their vulnerability to cyberattacks. On the other hand, the integration of emerging technologies, such as blockchain, offers opportunities but also presents challenges, particularly due to limited resources and specialized knowledge required for safe implementation. Demirkan et al. (2020) discuss these integration challenges, highlighting that while blockchain has the potential to transform cybersecurity and accounting practices, its adoption demands substantial expertise and infrastructure that many organizations find difficult to establish. Saeed et al. (2023) emphasizes the importance of robust cyber threat intelligence to build cybersecurity resilience, which is essential to protecting interconnected sectors and preventing broader systemic impacts from cyberattacks.

Finally, the 2023 Cybersecurity Report in Portugal highlights that the most used critical services by SME's are e-mail and online platforms. Consequently, a trend emerges of constant vigilance over a broader spectrum of cyber threats, reinforcing the need to prepare for both direct attacks and indirect impacts, such as business interruptions and loss of customer trust (Centro Nacional de Cibersegurança Portugal, 2023). In this constantly evolving scenario, fintech companies are emerging as pioneers of significant changes in the financial sector. Despite offering innovative services that promote efficiency and financial inclusion, fintech companies also introduce complexities in cybersecurity. These companies, by processing a substantial amount of sensitive data and operating in advanced digital environments, become prime targets for cyberattacks. This new reality demands robust responses in cybersecurity, with strategies that must be continuously adapted to face emerging threats, as emphasized by Callen-Naviglia and James (2018).

Regarding SME's specifically, interaction with fintech companies leads to a deepened awareness of cyber risks. These companies, upon integrating these solutions,

face unique challenges, including the secure management of financial data and protection against targeted attacks. For instance, the implementation of blockchain provides security and transparency in transactions, but it also demands heightened attention to specific security challenges to ensure data integrity and confidentiality, as mentioned by Ahmad et al. (2023). In the Portuguese context, the 2023 Cybersecurity Report also emphasizes the relevance of cybersecurity in SME's, especially those interacting with fintech solutions. Despite increased awareness of cyber risks, many of this companies still lack adaptive and robust cybersecurity strategies, a challenge intensified by the growing reliance on fintech solutions, as reported by the 2023 Cybersecurity Report in Portugal.

## 3.3. Interviews with key informant

For the purpose of this research, the elected key informant profile corresponded to experts with substantial backgrounds in both technical cybersecurity and strategic cybersecurity policy.

The first interviewee is an academic and researcher specializing in software engineering, with expertise in information systems, distributed systems, and blockchain. The second interviewee is a cybersecurity analyst with a background in international relations and national security, bringing a strategic perspective to cybersecurity, particularly within policy frameworks and international security contexts. These were in-depth interviews with the purpose of collecting information about specific points: the technical challenges and solutions in implementing cybersecurity within small and medium-sized enterprises, the strategic role of cybersecurity in protecting sensitive financial data, and the necessary competencies for professionals to manage emerging cyber threats effectively.

The interviews, each approximately 10 minutes, were recorded and transcribed for a detailed analysis. As outlined below, their responses highlighted several essential points for enhancing the quality of accounting information systems in SME's. Both experts identified phishing and ransomware as primary threats, emphasizing that training and awareness are essential first steps. They recommended cost-effective measures, such as establishing clear security policies, implementing access controls, and investing in regular training sessions.

The first expert underscored the importance of technical defenses like frequent software updates and the potential of blockchain to enhance data integrity. Meanwhile,

the second expert stressed that building a cybersecurity-conscious culture is equally vital, with strong leadership fostering regulatory compliance and security-focused practices. Both identified AI as a critical emerging technology in cybersecurity, acknowledging its potential both to improve defenses and to challenge SME's financially as attacks become more sophisticated. The strategic expert emphasized that small and mid-enterprises should take a top-down approach to cybersecurity, aligning leadership priorities with security practices to strengthen resilience.

In summary, the interviews underscored the importance of a balanced approach to cybersecurity, blending technical measures and user awareness within a supportive organizational culture. This dual approach is crucial for enhancing the resilience and security of accounting information systems within these companies, particularly given the financial and operational limitations common to this sector.

## 3.4. Structure of the questionnaire survey

The questionnaire is structured into 8 sections with a total of 71 questions. The first question confirms participants' understanding of the study's objectives and characteristics according to the GDPR and their consent for aggregated academic use of their responses. The second group of questions addresses demographic and company details. The remaining questionnaire comprises seven variables, described below:

- Quality of Accounting Information – five points Likert scale from "strongly disagree" to "strongly agree";
- Quality of Accounting Information Systems – five points Likert scale from "strongly disagree" to "strongly agree";
- External Integration of Information Systems, "yes" or "no" question;
- Cybersecurity Countermeasures, "yes" or "no" questions;
- Knowledge of policy and procedures – five points Likert scale from "strongly disagree" to "strongly agree";
- Attitude towards policy and procedures;
- Self-reported behavior toward policy and procedures.

The Quality of Accounting Information focuses on the output quality of the financial information produced by AIS. It evaluates the accuracy, reliability, and relevance of financial data that supports decision-making processes within SME's. QAI refers to the ability of Accounting Information to respond to stakeholders' information

needs, which is crucial for informed decision-making, regulatory compliance, and stakeholder trust (Algrari & Ahmed, 2019).

The Quality of Accounting Information Systems evaluates the effectiveness of the accounting information system in supporting organizational needs, ensuring security, and adhering to internal policies. It incorporates multiple dimensions to assess the robustness of the AIS. The scale was adapted from the study by Algarri and Ahmed (2019) and it covers aspects such as flexibility, accuracy, security of data processed through accounting information systems, effectiveness, quality, and usability in supporting organizational goals.

External Integration of Information Systems refers to the extent an organization's systems are linked with external partners, suppliers, or clients. This construct, inspired by Baskerville et al. (2018), emphasizes the importance of seamless communication and data exchange between different entities. Items focus on aspects like the use of extranets, Electronic Data Interchange, and order management systems, which are critical for efficient supply chain management and data accuracy. Each item uses a Yes/No scale to evaluate how well a firm's systems are linked with internal and external partners, supporting streamlined operations, supply chain efficiency, and enhanced collaboration.

Cybersecurity Countermeasures concern essential preventive practices that companies should adopt to mitigate cyber threats. Based on Baskerville et al. (2018), these items are grounded cybersecurity protocols, specifically in enhancing organizational resilience. They assess practices such as implementing firewalls, anti-malware software, and intrusion detection systems. The selected items reflect the industry's best practices for maintaining a secure and resilient information environment. (Baskerville et al., 2018) allowing for straightforward insights into the firm's approach to safeguarding sensitive information through essential cybersecurity practices.

Knowledge of Policy and Procedures (SrB tPP) examines the employees' understanding of organizational policies and cybersecurity procedures, highlighting the role of informed staff in safeguarding data. Drawing from the work of Parsons et al. (2017), it aims to measure employees' knowledge of the bests practices, and the specific protocols needed to respond to cybersecurity threats.

Attitude towards Policy and Procedures (ATPP) addresses compliance and adherence to cybersecurity policies. Parsons et al. (2017) have demonstrated that positive attitudes are correlated with adherence to protocols, which in turn minimizes security risks. The listed items capture different dimensions of employee attitudes, such as their

perceived importance of following procedures and the perceived relevance of policies in preventing security breaches.

Self-reported behavior towards policy and procedures captures the degree to which employees actively follow cybersecurity procedures. The construct, based on Parsons et al. (2017), focuses on behaviors such as regular updates of passwords, proper handling of sensitive data, and adherence to the organization's security protocols. These behaviors are critical for maintaining cybersecurity within an organization, as self-reported adherence to protocols reflects the practical application of knowledge and attitudes in day-to-day operations.

Table X shows the items that comprise each construct asses through a questionnaire.

*Tabel 1 - Items used on the questionnaire.*

| Code | Item | Authors |
|---|---|---|
| QAIS1 | Accounting Information systems are flexible in data processing. | Algrari and Ahmed (2019) |
| QAIS2 | Accounting information systems help to achieve goals accurately and quickly | Algrari and Ahmed (2019) |
| QAIS3 | Data are processed through accounting systems consistent with accounting polices | Algrari and Ahmed (2019) |
| QAIS4 | The cost of accounting information system in the company is consistent with the nature and size of the accounting information provided by the system | Algrari and Ahmed (2019) |
| QAIS5 | Accounting information system in the company is easily updated data | Algrari and Ahmed (2019) |
| QAIS6 | The AIS provides accounting information that comparable | Algrari and Ahmed (2019) |
| QAIS7 | The AIS provides integrated accounting information that will affect the effectiveness of the company | Algrari and Ahmed (2019) |
| QAIS8 | AIS are characterized by the case ease and high quality | Algrari and Ahmed (2019) |
| QAIS9 | The inputs of AIS are presented in an easy and clear manner | Algrari and Ahmed (2019) |
| QAIS10 | Input and output of AIS are maintained in a secure manner | Algrari and Ahmed (2019) |
| QAI1 | The company is distinguished by its accounting information quality | Algrari and Ahmed (2019) |
| QAI2 | Accurate accounting information helps company make financial decisions | Algrari and Ahmed (2019) |
| QAI3 | Accounting information prepared to ensure its quality, accuracy and correctness | Algrari and Ahmed (2019) |
| QAI4 | The provided accounting information are consistent with user's needs in different financial periods per year | Algrari and Ahmed (2019) |
| QAI5 | The company's Accounting information is flexible in its use in various aspects | Algrari and Ahmed (2019) |
| QAI6 | The company's accounting information Are clear and uncomplicated | Algrari and Ahmed (2019) |

| | | |
|---|---|---|
| QAI7 | The company's accounting information is easily understood among its various users | Algrari and Ahmed (2019) |
| QAI8 | The company's accounting information are inclusive for all the financial aspects that users need in the decision –making process | Algrari and Ahmed (2019) |
| QAI9 | The accounting information provided in appropriate time | Algrari and Ahmed (2019) |
| QAI10 | Accounting information are easily saved, are retrieved at any time | Algrari and Ahmed (2019) |
| CC1 | Does you firm use Self-protection or control software against viruses | Baskerville et al. (2018) |
| CC2 | Does you firm use Firewalls (hardware or software)? | Baskerville et al. (2018) |
| CC3 | Does you firm use Secured servers (using protocols such as https)? | Baskerville et al. (2018) |
| CC4 | Does you firm use Authentication mechanisms (PIN codes, data encryption, digital signature)? | Baskerville et al. (2018) |
| EIoIS1 | Does your firm use an extranet? | Baskerville et al. (2018) |
| EIoIS2 | Does your firm use EDI? | Baskerville et al. (2018) |
| EIoIS3 | Does your firm use tracking tools? | Baskerville et al. (2018) |
| EIoIS4 | Does your firm use a purchasing/sales delivery systems coupled with internal systems for supplies? | Baskerville et al. (2018) |
| EIoIS5 | Does your firm use a purchasing/sales delivery systems coupled with internal systems for billing and payments? | Baskerville et al. (2018) |
| EIoIS6 | Does your firm use a purchasing/sales delivery systems coupled with internal systems for operations? | Baskerville et al. (2018) |
| EIoIS7 | Does your firm receive orders through internet? | Baskerville et al. (2018) |
| EIoIS8 | Does your firm receive orders through EDI? | Baskerville et al. (2018) |
| EIoIS9 | Does your firm place orders through internet? | Baskerville et al. (2018) |
| EIoIS10 | Does your firm place orders through EDI? | Baskerville et al. (2018) |
| EIoIS11 | Does your largest client have its system coupled with that of the firm for orders and billing? | Baskerville et al. (2018) |
| EIoIS12 | Does your firm have its system coupled with its largest suppliers for orders and billing? | Baskerville et al. (2018) |
| KoPP1 | A mixture of letters, numbers and symbols is necessary for work passwords. | Parsons et al. (2017) |
| KoPP2 | It's acceptable to use my social media passwords on my work accounts. | Parsons et al. (2017) |
| KoPP3 | I am not permitted to click on any links in emails from an unknown sender. | Parsons et al. (2017) |
| KoPP4 | I am allowed to open email attachments from unknown senders. | Parsons et al. (2017) |
| KoPP5 | While I am at work, I shouldn't access certain websites. | Parsons et al. (2017) |
| KoPP6 | I am allowed to enter any information on any website if it helps me do my job. | Parsons et al. (2017) |
| KoPP7 | When working in a public place, I have to keep my laptop with me at all times. | Parsons et al. (2017) |
| KoPP8 | I am allowed to send sensitive work files via a public Wi-Fi network. | Parsons et al. (2017) |

| | | |
|---|---|---|
| KoPP9 | Sensitive printouts can be disposed of in the same way as non-sensitive ones | Parsons et al. (2017) |
| KoPP10 | If I see someone acting suspiciously in my workplace, I should report it. | Parsons et al. (2017) |
| ATPP1 | It's safe to use the same password for social media and work accounts. | Parsons et al. (2017) |
| ATPP2 | It's a bad idea to share my work passwords, even if a colleague asks for it. | Parsons et al. (2017) |
| ATPP3 | It's safe to have a work password with just letters. | Parsons et al. (2017) |
| ATPP4 | It's always safe to click on links in emails from people I know. | Parsons et al. (2017) |
| ATPP5 | Nothing bad can happen if I click on a link in an email from an unknown sender. | Parsons et al. (2017) |
| ATPP6 | It's risky to open an email attachment from an unknown sender. | Parsons et al. (2017) |
| ATPP7 | It can be risky to download files on my work computer. | Parsons et al. (2017) |
| ATPP8 | Just because I can access a website at work, it doesn’t mean that it's safe. | Parsons et al. (2017) |
| ATPP9 | It's risky to send sensitive work files using a public Wi-Fi network. | Parsons et al. (2017) |
| ATPP10 | It's risky to access sensitive work files on a laptop of strangers can see my screen. | Parsons et al. (2017) |
| SrBtPP1 | I use different password for my social media and work accounts. | Parsons et al. (2017) |
| SrBtPP2 | I use a combination of letters, numbers and symbols in my work passwords. | Parsons et al. (2017) |
| SrBtPP3 | I don't always click on links in emails just because they come from someone I know. | Parsons et al. (2017) |
| SrBtPP4 | I don't open email attachments if the sender is unknown to me. | Parsons et al. (2017) |
| SrBtPP5 | I download any files onto my work computer that will help me get the job done. | Parsons et al. (2017) |
| SrBtPP6 | I assess the safety of websites before entering information. | Parsons et al. (2017) |
| SrBtPP7 | When working in a public place, I leave my laptop unattended. | Parsons et al. (2017) |
| SrBtPP8 | I check that strangers can't see my laptop screen if I'm working on a sensitive document. | Parsons et al. (2017) |
| SrBtPP9 | I leave printouts that contain sensitive information on my desk when I'm not there. | Parsons et al. (2017) |
| SrBtPP10 | If I noticed a security incident, I would report it. | Parsons et al. (2017) |

The questionnaire specifically targets employees in the accounting and finance departments. It was created using Google Forms and distributed during October 2024.

## 4.1. Statistical analysis

This study applied Partial Least Squares Structural Equation Modeling (PLS-SEM), following the methodological guidelines of Hair, Hult, Ringle, and Sarstedt (2017). The selection of PLS-SEM over Covariance-Based SEM (CB-SEM) was influenced by the sample size, which is lower than the ideal threshold for CB-SEM, and the flexibility of PLS-SEM in handling non-normally distributed data (Silva et al., 2017). Statistical analyses were conducted using SmartPLS version 3.0.

The analysis was structured as a two-step process based on the recommendations of Hair, Sarstedt, Ringle, and Gudergan (2018), enabling a systematic evaluation of the measurement model's reliability and validity before assessing the structural model's predictive power.

The first step involved evaluating reliability, convergent validity, and discriminant validity. Reliability was measured using outer loadings, with items removed if they exhibited loadings between 0.4 and 0.7, per Hair et al. (2017). Items were only removed if their exclusion improved the inter-item reliability (Rho_a) below 0.7 or enhanced the Average Variance Extracted (AVE). Rho_a reflects internal consistency, while an AVE above 0.5 signifies adequate convergent validity, indicating that constructs account for at least 50% of the variance in their indicators.

Discriminant validity was examined using Fornell and Larcker's (1981) criterion alongside the heterotrait-monotrait ratio (HTMT). Fornell and Larcker's criterion stipulates that the square root of AVE for each construct should exceed its inter-construct correlations, ensuring distinct constructs. The HTMT criterion was also applied, with values below 0.90 confirming discriminant validity.

In the second step, the structural model's explanatory power was assessed by examining the R-squared ($R^2$) values for endogenous latent variables. Model fit was evaluated using the Standardized Root Mean Square Residual (SRMR), with values below 0.10 indicating an acceptable model specification. Additionally, RMStheta values near zero were considered indicative of low residual correlations, supporting model fit (Henseler et al., 2014).

Variance Inflation Factor (VIF) was used to diagnose multicollinearity, with acceptable VIF values below 5. We also assessed each construct's contribution to the model using f-squared ($f^2$) effect sizes, interpreted per Hair et al. (2017) as 0.02 (small), 0.15 (medium), and 0.35 (large).

Following Shmueli, Ray, Estrada, and Chatla's (2016) recommendations, predictive relevance was assessed using the root mean square error (RMSE) and mean absolute error (MAE) through the PLS Predict algorithm with 10-fold validation. The observed reduction in RMSE and MAE relative to linear models indicated robust predictive power.

A bootstrap resampling method with 1000 iterations was conducted to estimate p-values and confidence intervals for path coefficients, ensuring rigorous significance testing. Non-standardized coefficients (β) were used to interpret the strength of associations, with t-statistics computed by dividing β by the standard deviation.

## 4.2. Results

### 4.2.1. Presentation of Results

Table 8 summarizes participant characteristics. The largest age group was 46–55 years (28.3%), followed by those over 55 (26.7%) and 25–35 (25.0%). Participants aged 36–45 years comprised 18.3%, with the smallest group being those under 25 years (1.7%). Regarding positions, most participants were Managers/Founders (33.3%), followed by Accountants/Accounting Technicians (26.7%) and administrative staff (21.7%). Smaller proportions occupied roles such as Financial Directors (8.3%), IT Engineers (3.3%), and various specialized roles like Database Specialists, IT Directors, Information Security Managers, and Partner/Consultants, each representing 1.7%.

The distribution of company sectors indicates that most participants were from the Services sector (63.3%), with smaller representations from Commerce (16.7%), Industry (11.7%), and Agriculture (3.3%). Sectors such as Unemployed, Energy, and Public Enterprise Entities each comprise 1.7% of the sample. In terms of revenue, the majority reported annual turnover below 500 thousand euros (48.3%), while 25.0% exceeded 2 million euros. Companies with revenue between 500 thousand and 1 million euros accounted for 20.0%, and those between 1 and 2 million euros represented 6.7%.

*Tabel 2 - Participants characteristics.*

| | n | % |
|---|---|---|
| **Age** | | |
| < 25 years | 1 | 1.7 |
| 25 - 35 years | 15 | 25.0 |
| 36 - 45 years | 11 | 18.3 |
| 46 - 55 years | 17 | 28.3 |
| > 55 years | 16 | 26.7 |
| **Position** | | |
| Manager/Founder | 20 | 33.3 |
| Accountant/Accounting Technician | 16 | 26.7 |
| Administrative | 13 | 21.7 |
| Financial Director | 5 | 8.3 |
| IT Engineer | 2 | 3.3 |
| Database Specialist | 1 | 1.7 |
| IT Director | 1 | 1.7 |
| Information Security Manager | 1 | 1.7 |
| Partner/Consultant | 1 | 1.7 |
| **Company Sector** | | |
| Services | 38 | 63.3 |
| Commerce | 10 | 16.7 |
| Industry | 7 | 11.7 |
| Agriculture | 2 | 3.3 |
| Unemployed | 1 | 1.7 |
| Energy | 1 | 1.7 |
| Public Enterprise Entity | 1 | 1.7 |
| **Volume (€)** | | |
| Between 1 and 2 million euros | 4 | 6.7 |
| Between 500 thousand and 1 million euros | 12 | 20.0 |
| Less than 500 thousand euros | 29 | 48.3 |
| More than 2 million euros | 15 | 25.0 |

Initial inspection of the model identified several outer loadings between 0.4 and 0.7, leading to their exclusion to enhance measurement reliability. The resulting model structure, displayed in Figure 3, encompasses the constructs: External Integration of Information Systems (EIIS), Cybersecurity Countermeasures (CCCM), Knowledge of Policy and Procedures (KPP), Attitude towards Policy and Procedures, Self-Reported Behavior towards Policy and Procedures (SrBtPP), Quality of Accounting Information Systems, and Quality of Accounting Information, illustrating their relationships and overall contribution to the study.

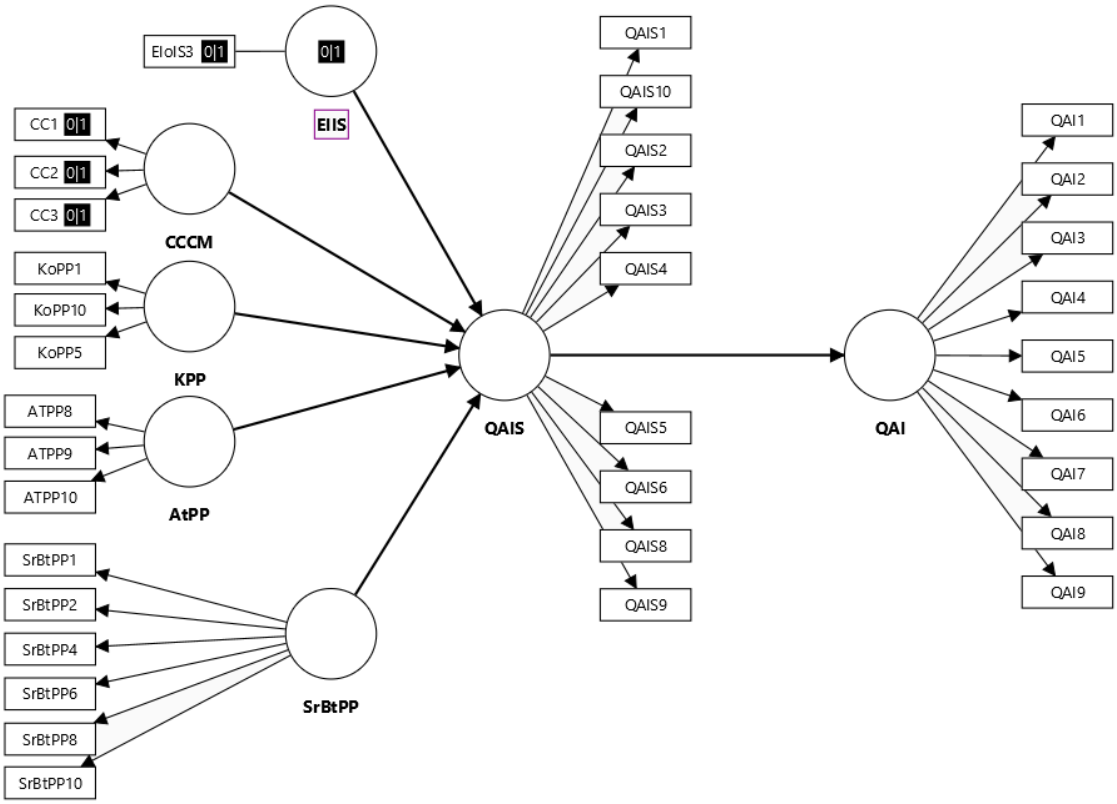



*Figure 4 – Final Model structure.*

The reliability and convergent validity findings, as shown in Table 9, indicate that nearly all constructs meet the necessary thresholds for Rho_a (≥0.70) and AVE (≥0.50), confirming their robustness within the model. The only exception is the KPP construct, which slightly falls below the Rho_a threshold. Overall, these outcomes support the reliability and validity of the model's constructs, as depicted in Figure 3.

*Tabel 3 - Reliability and convergent validity.*

| | Rho_a | AVE |
|---|---|---|
| AtPP | 0.874 | 0.777 |
| CCCM | 0.878 | 0.667 |
| KPP | 0.678 | 0.605 |
| QAI | 0.936 | 0.642 |
| QAIS | 0.946 | 0.685 |
| SrBtPP | 0.889 | 0.620 |

Discriminant validity results were confirmed, as each construct's square root of AVE was consistently higher than its correlations with other constructs, in line with Fornell and Larcker's (1981) criterion. This indicates that each construct shares more variance with its own indicators than with those of other constructs, reinforcing distinctiveness across constructs. Furthermore, HTMT values were all below the 0.90 threshold, with the KPP and SrBtPP correlation at 0.860. While still below the 0.90 cutoff, this relatively high value suggests a closer relationship between Knowledge of Policy and Procedures and Self-Reported Behavior toward Policy and Procedures.

This finding may reflect an alignment between respondents' knowledge and their self-reported behaviors regarding policies, an insight that may be pertinent to the study's context.

*Tabel 4 - HTMT matrix.*

| | AtPP | CCCM | EIIS | KPP | QAI | QAIS | SrBtPP |
|---|---|---|---|---|---|---|---|
| AtPP | | | | | | | |
| CCCM | 0.323 | | | | | | |
| EIIS | 0.150 | 0.298 | | | | | |
| KPP | 0.707 | 0.301 | 0.096 | | | | |
| QAI | 0.414 | 0.292 | 0.122 | 0.596 | | | |
| QAIS | 0.427 | 0.251 | 0.287 | 0.571 | 0.794 | | |
| SrBtPP | 0.696 | 0.336 | 0.167 | 0.860 | 0.619 | 0.628 | |

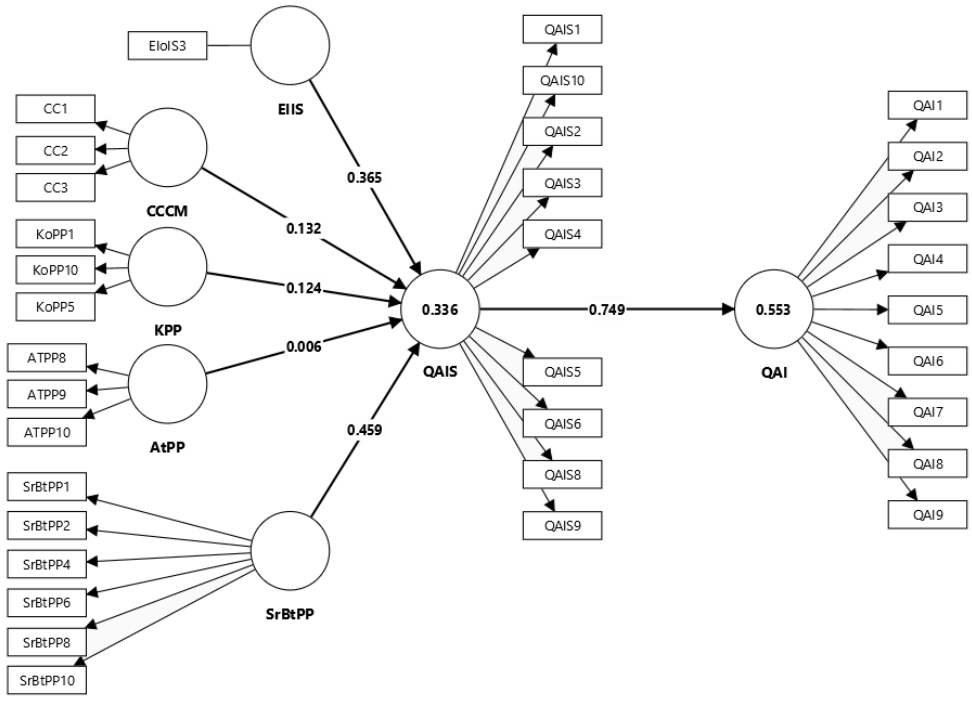



*Figure 5 - Model Results.*

The analysis of the model, as displayed in Figure 5, reveals moderate explanatory power for both Quality of Accounting Information Systems and Quality of Accounting Information, with adjusted R-squared values of 0.336 and 0.553, respectively. These R-squared values suggest that the model accounts for a moderate proportion of variance in these constructs.

The VIF values, all below 5, indicate no problematic multicollinearity among predictors. Additionally, f-squared analysis reveals that the association between QAIS and QAI has a high effect size ($f^2 = 1.28$), signifying a strong, positive influence of QAIS on QAI. This emphasizes the critical role of Quality of Accounting Information Systems in explaining the variance observed in Quality of Accounting Information within the model.

Overall, these findings indicate a well-fitting model with meaningful relationships, particularly highlighting the impact of QAIS on QAI, thus supporting the structural coherence and predictive relevance of the model. Further evaluation may continue to explore potential refinements or additional variables that could improve explanatory power.

*Tabel 5 - Assessment of f^2.*

| | f-square |
|---|---|
| AtPP → QAIS | 0.000 |
| CCCM → QAIS | 0.003 |
| EIIS → QAIS | 0.050 |
| KPP → QAIS | 0.013 |
| QAIS → QAI | 1.275 |
| SrBtPP → QAIS | 0.152 |

The $f^2$ analysis measures the impact of each construct on the model, indicating the strength of their effects. QAIS has a substantial influence on QAI with a high $f^2$ value of 1.275, underscoring its pivotal role in the model. Meanwhile, SrBtPP ($f^2 = 0.152$) and EIIS ($f^2 = 0.050$) contribute moderate effects to QAIS, supporting their relevance but at a smaller magnitude. AtPP, CCCM, and KPP show minimal effect sizes ($f^2 < 0.02$), indicating limited direct impact on QAIS within this model framework.

The model fit was evaluated with the Standardized Root Mean Square Residual (SRMR), resulting in a value of 0.118, which slightly exceeds the recommended threshold of 0.10. This indicates a less-than-ideal fit, suggesting that a larger sample size could potentially improve the model's fit.

| | SRMR |
|---|---|
| Model | 0.118 |

*Tabel 6 - Model fit.*

For predictive accuracy, indicators such as RMSE and MAE were lower than those from linear regression models, indicating the model's strong predictive power.

Table X provides an overview of total, indirect, and specific indirect effects. Notably, QAIS had a strong, significant impact on QAI ($\beta = 0.748$, $p < 0.001$), while SrBtPP significantly influenced both QAI ($\beta = 0.351$, $p = 0.012$) and QAIS ($\beta = 0.464$, $p = 0.005$) through direct effects. However, predictors like AtPP, CCCM, EIIS, and KPP did not demonstrate significant total effects on QAI or QAIS, with p-values above 0.05.

For indirect effects, SrBtPP continued to show a significant indirect influence on QAI ($\beta = 0.351$, $p = 0.012$), emphasizing its importance. Specific indirect effects revealed that SrBtPP impacts QAI through QAIS, underscoring QAIS's mediating role.

This analysis highlights SrBtPP and QAIS as critical factors for QAI, with QAIS exhibiting the strongest effect, indicating its central role in accounting information quality.

*Tabel 7 - Total and indirect effects.*

| | β | SE | t | p |
|---|---|---|---|---|
| **Total effects** | | | | |
| AtPP → QAI | 0.006 | 0.111 | 0.043 | 0.966 |
| AtPP → QAIS | 0.008 | 0.148 | 0.043 | 0.966 |
| CCCM → QAI | 0.100 | 0.342 | 0.289 | 0.772 |
| CCCM → QAIS | 0.135 | 0.481 | 0.275 | 0.783 |
| EIIS → QAI | 0.280 | 0.174 | 1.574 | 0.115 |
| EIIS → QAIS | 0.376 | 0.232 | 1.571 | 0.116 |
| KPP → QAI | 0.079 | 0.095 | 0.973 | 0.331 |
| KPP → QAIS | 0.105 | 0.124 | 0.995 | 0.320 |
| QAIS → QAI | 0.748 | 0.077 | 9.767 | **<0.001***** |
| SrBtPP → QAI | 0.351 | 0.137 | 2.499 | **0.012*** |
| SrBtPP → QAIS | 0.464 | 0.164 | 2.797 | **0.005**** |
| AtPP → QAI | 0.006 | 0.111 | 0.043 | 0.966 |
| AtPP → QAIS | 0.008 | 0.148 | 0.043 | 0.966 |

| | β | SE | t | p |
|---|---|---|---|---|
| CCCM → QAI | 0.100 | 0.342 | 0.289 | 0.772 |
| CCCM → QAIS | 0.135 | 0.481 | 0.275 | 0.783 |
| EIIS → QAI | 0.280 | 0.174 | 1.574 | 0.115 |
| EIIS → QAIS | 0.376 | 0.232 | 1.571 | 0.116 |
| KPP → QAI | 0.079 | 0.095 | 0.973 | 0.331 |
| **Total indirect effects** | | | | |
| AtPP → QAI | 0.006 | 0.111 | 0.043 | 0.966 |
| CCCM → QAI | 0.100 | 0.342 | 0.289 | 0.772 |
| EIIS → QAI | 0.280 | 0.174 | 1.574 | 0.115 |
| KPP → QAI | 0.079 | 0.095 | 0.973 | 0.331 |
| SrBtPP → QAI | 0.351 | 0.137 | 2.499 | **0.012*** |
| **Specific Indirect effects** | | | | |
| EIIS → QAIS → QAI | 0.280 | 0.174 | 1.574 | 0.115 |
| KPP → QAIS → QAI | 0.079 | 0.095 | 0.973 | 0.331 |
| SrBtPP → QAIS → QAI | 0.351 | 0.137 | 2.499 | **0.012*** |
| AtPP → QAIS → QAI | 0.006 | 0.111 | 0.043 | 0.966 |
| CCCM → QAIS → QAI | 0.100 | 0.342 | 0.289 | 0.772 |

### 4.2.2. Discussion of results

The hypothesis that External Integration of Information Systems positively impacts the QAIS is partially supported by the findings, though the impact was not statistically significant. According to prior studies, the integration of information systems with external partners, suppliers, and clients facilitates seamless data exchange, which in turn can enhance the overall quality and reliability of accounting information systems (Baskerville et al., 2018; Rai et al., 2006). Such integration allows for real-time information sharing and improves the accuracy of data in systems, which is especially beneficial for supply chain efficiency and error reduction. The lack of statistical significance could be attributed to specific challenges that these companies face in establishing sophisticated integration with external partners. They often lack the necessary resources and technological infrastructure to fully leverage external integration, which may limit the practical impact of EIIS on QAIS in this context. This result suggests

that while EIIS is theoretically beneficial, practical constraints in the SME environment may limit its efficacy. Future research could explore this relationship in more technologically mature firms or examine ways SME's can overcome barriers to external integration, perhaps through shared platforms or partnerships that reduce the financial burden of integration technologies.

The results also show a positive but statistically insignificant effect on Cybersecurity Countermeasures on QAIS. This finding challenges the well-documented importance of cybersecurity practices in ensuring robust information systems (Straub & Welke, 1998; Chen et al., 2015). Cybersecurity countermeasures such as firewalls, anti-malware tools, and intrusion detection systems are essential for preventing unauthorized access and ensuring system integrity. Prior literature emphasizes that robust cybersecurity fosters user trust and supports system reliability, which should theoretically enhance QAIS. The lack of a significant effect in this study could stem from the limited cybersecurity budgets and resources available to SME's. As highlighted in the literature, SME's often face financial and technical constraints that prevent them from implementing comprehensive cybersecurity measures (Muravskyi, 2021). Without sufficient cybersecurity infrastructure, the potential benefits of CCCM may not be fully realized in SME's, as limited measures may not be enough to impact the quality of accounting information systems significantly. This finding suggests a need for more targeted cybersecurity support for SME's, possibly through government subsidies or collaborative security frameworks that provide SME's with affordable access to essential security tools.

The hypothesis that Knowledge of Policy and Procedures positively impacts QAIS was not supported by statistically significant findings in this study. Existing literature, including works by Parsons et al. (2014) and Bulgurcu et al. (2010), emphasizes that employee knowledge of cybersecurity policies is critical for preventing errors and responding effectively to threats. When employees understand the security protocols and procedures, they are better equipped to detect and mitigate risks that could otherwise compromise system quality. However, the lack of significance in this study suggests that, in the context of SME's, simply having knowledge of policies may not be sufficient to impact QAIS meaningfully. This could indicate that while knowledge is necessary, it may not translate directly into improved system quality without concurrent enforcement and practical application. SME's might benefit from combining policy knowledge with hands-on training and regular policy refreshers to ensure that employees can effectively

apply this knowledge in real-world situations. This could also reflect a gap between knowledge and behavior, where employees are aware of policies but do not consistently act on them, underscoring the need for organizational support and monitoring to bridge this gap.

The hypothesis that a positive Attitude Toward Policy and Procedures would impact QAIS was also not supported by statistically significant results. This is somewhat surprising, given previous research that links positive employee attitudes with greater adherence to security policies, which should, in theory, support system quality (Herath & Rao, 2009; Hu et al., 2012). Employees who value and see the relevance of following cybersecurity protocols are typically more likely to comply with these standards, thereby reducing vulnerabilities and enhancing the system's reliability. In the case of SME's, however, the results suggest that attitude alone may not be a strong enough factor to influence QAIS significantly. This may reflect organizational cultures in SME's where cybersecurity is not highly prioritized, and attitudes towards policies are not strongly enforced. Additionally, employees in smaller firms may view cybersecurity as less critical due to limited awareness or perceived irrelevance, given their smaller scale of operations. This result implies that SME's might benefit from fostering a more cybersecurity-focused culture that not only promotes positive attitudes but also emphasizes the importance of these attitudes for system quality and organizational success.

The hypothesis that Self-Reported Behavior Toward Policy and Procedures (SrBtPP) positively impacts QAIS was supported by significant findings, suggesting that employee adherence to security practices is indeed crucial for maintaining high-quality accounting information systems. This aligns with the findings of Puhakainen and Siponen (2010) and Anderson and Agarwal (2010), who highlight that proactive security behaviors, such as regular password updates and proper data handling, are essential for system resilience. The significant effect of SrBtPP in this study indicates that employees' actions in following cybersecurity protocols have a direct impact on system quality. For SME's, this result underscores the importance of fostering a culture of compliance and accountability. Encouraging employees to adhere to security practices, perhaps through regular training, reminders, or performance incentives, could further enhance QAIS. It also suggests that while knowledge and attitude are important, the practical application of these elements—actual behavior—plays the most critical role in ensuring system quality. This finding supports the need for practical, behavior-focused initiatives that make adherence to security policies an integral part of daily operations within SME's.

The relationship between QAIS and QAI was found to be both strong and statistically significant, confirming the hypothesis that high-quality accounting information systems contribute to high-quality accounting information. This finding is consistent with previous literature (Algrari & Ahmed, 2019; Xu et al., 2017), which suggests that robust information systems are essential for producing accurate, reliable, and relevant accounting information. QAIS serves as the foundation for QAI, ensuring that data integrity is maintained, and that information generated by these systems is suitable for decision-making and regulatory compliance. The significant impact of QAIS on QAI in this study highlights the critical role that well-functioning accounting information systems play in supporting organizational objectives. These companies need to ensure the quality of their information systems is paramount for maintaining financial data integrity and supporting informed decision-making. This result reinforces the value of investing in reliable and secure accounting systems, even in resource-constrained environments, as a means of enhancing overall data quality and organizational resilience.

The findings of this study provide important insights into the relationships between cybersecurity practices, employee behaviors, and the quality of accounting information in SME's. While certain constructs (e.g., CCCM, EIIS, KPP, and AtPP) did not achieve statistical significance, the results emphasize the importance of self-reported behavior (SrBtPP) and the foundational role of QAIS in determining QAI.

The nonsignificant impact of some constructs, such as CCCM and EIIS, may reflect the practical challenges that small and mid-entities face in implementing comprehensive cybersecurity measures and integrating systems with external partners. Given these constraints, policymakers and industry bodies could consider providing support tailored to SME's, such as subsidies or shared cybersecurity resources, to help them overcome these barriers.

The strong relationship between SrBtPP and QAIS, as well as between QAIS and QAI, highlights the value of practical, behavior-focused initiatives in strengthening system quality and information integrity. These companies could benefit from focusing on behavior reinforcement strategies, such as regular training, reminders, and perhaps incentives that encourage adherence to cybersecurity practices. Additionally, the results suggest that small and mid-enterprises should prioritize building a robust accounting information system as a key element of their cybersecurity strategy, given its substantial impact on the quality of accounting information.

This study underscores the need for the small and mid-caps to adopt a multifaceted approach to cybersecurity, one that integrates both technological and behavioral dimensions to enhance the quality of their accounting information systems and, ultimately, the quality of their financial data. While resource constraints may limit certain cybersecurity practices, SME's can leverage employee behavior and a focus on QAIS to significantly improve data integrity and system resilience. These perceptions provide a foundation for SME's to make targeted improvements in their cybersecurity posture, supporting more reliable and secure accounting processes in a rapidly evolving digital landscape.

This study provides a focused investigation into cybersecurity's role in safeguarding accounting and finance functions within small and medium-sized enterprises, addressing a sector often overshadowed in cybersecurity research that predominantly targets larger organizations (World Economic Forum, 2016; European Union Agency for Cybersecurity, 2020). Although the impact of cybersecurity on financial data quality is widely acknowledged, this study contributes novel insights by applying these concepts to SME's, a group with distinct operational and resource constraints. By linking the quality of accounting information systems with the reliability of accounting information, this research reveals the foundational importance of well-integrated information systems and employee engagement in maintaining data security and integrity (Algrari & Ahmed, 2019).

This research confirms that cybersecurity's effectiveness in SME's depends not only on technological controls but also on proactive employee behaviors, highlighting that even with limited resources, organizations can significantly enhance data protection through strategic cybersecurity practices (Pendley, 2018; Parsons et al., 2017). The methodology employed a dual-phase approach combining expert interviews and quantitative analysis offers a structured framework that future research could leverage in similar contexts. While this study reinforces existing literature, it distinguishes itself by tailoring established cybersecurity concepts to the unique challenges and capacities of SME's, a critical yet often overlooked business segment.

Despite the study's contributions, it does not seek to introduce groundbreaking innovations but rather aims to enhance the practical application of cybersecurity within SME's. This approach is valuable, as it addresses how smaller enterprises, often less equipped with specialized resources, can implement effective cybersecurity measures without exhaustive investments. Nevertheless, it is crucial to recognize that this research extends rather than revolutionizes current understanding, acting as a focused supplement to broader cybersecurity literature by improving it, on SME's' specific needs and constraints.

Several limitations should be noted. The sample size and the regional focus may limit the broader applicability of results, while the reliance on self-reported behaviors, though insightful, may introduce response bias. To enhance the generalizability of these findings, future research could adopt a larger, more diverse sample and investigate additional regional contexts to better understand how varied regulatory frameworks affect SME's globally.

The findings point to several avenues for further exploration. As emerging technologies, such as AI-driven threat detection and blockchain-based security, gain traction, future studies could examine how these advancements specifically benefit SME's, offering new avenues for securing accounting information systems in resource-constrained environments (Smith, 2020; Wang et al. 2018). Research on embedding cybersecurity training within accounting curricula would also be instrumental, as it could equip future finance professionals with the skills necessary to adapt to a rapidly evolving threat landscape (Le Guyader, 2019). While these suggestions build upon existing knowledge, they underscore the continued need for precise, context-specific studies that consider SME's' limitations and capacities.

In conclusion, this study underscores cybersecurity's critical role in preserving the integrity of accounting information within SME's. As digitalization reshapes business operations, these companies must integrate cybersecurity into their strategic framework rather than treat it as a peripheral concern. This research enriches the academic discourse on cybersecurity by addressing a neglected segment, demonstrating that even incremental adjustments in cybersecurity practices can yield significant benefits for the companies studied. Such insights reinforce the importance of a proactive, well-informed approach to cybersecurity, necessary for maintaining financial integrity within an increasingly interconnected digital economy.

Agarwal, S., Alok, S., Ghosh, P., & Gupta, S. (2023). Fintech and credit scoring for the millennials: Evidence using mobile and social footprints. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3507827

Al Kemyani, M. K., Al Raisi, J., Tariq Al Kindi, A. R., Al Mughairi, I. Y., & Tiwari, C. K. (2022). Blockchain applications in accounting and finance: Qualitative evidence from the banking sector [Review of *Blockchain applications in accounting and finance: Qualitative evidence from the banking sector*]. *Journal of Research in Business and Management*, *10*(4), 28–39.

Alahmari, A. A., & Duncan, R. A. (2021, July 1). *Investigating potential barriers to cybersecurity risk management investment in SME's*. IEEE Xplore. https://doi.org/10.1109/ECAI52376.2021.9515166

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 1–17. https://doi.org/10.1080/08874417.2023.2251455

Algrari, A. Y., & Ahmed, R. M. (2019, November 7). The impact of accounting information systems' quality on accounting information quality. *Reform of Accounting and Auditing Systems- Reality & Requirements*.

Banco de Portugal. (2017). Cibersegurança no sistema financeiro: Riscos, cooperação e governação. *Banco de Portugal*.

Baskerville, R., Rowe, F., & Wolff, F.-C. (2018). Integration of information systems and cybersecurity countermeasures. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(1), 33–52. https://doi.org/10.1145/3184444.3184448

Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants cybersecurity isn't just for techies: Incorporating cybersecurity into the accounting curriculum. *Issues in Accounting Education*, *37*(3).

Callen-Naviglia, J., & James, J. (2018). Fintech, regtech and the importance of cybersecurity. *Issues in Information Systems*, *19*(3), 220–225. https://doi.org/10.48009/3_iis_2018_220-225

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal*, *21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67

Cao, L. (2020). *AI in finance: A review* [Review of *AI in finance: A review*]. 36.

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy002

Centro Nacional de Cibersegurança. (2024). *Relatório cibersegurança em portugal* (p. 109). Centro Nacional De Cibersegurança.

Centro Nacional de Cibersegurança Portugal. (2022). *Relatório cibersegurança em portugal*. Centro Nacional De Cibersegurança.

Centro Nacional de Cibersegurança Portugal. (2023). *Relatório cibersegurança em portugal* (p. 78). Centro Nacional De Cibersegurança.

Çiftçi, B., & Balcıoğlu, Y. S. (2023). Cybersecurity and financial risks: Challenges and solutions encountered in the finance sector and accounting field. *5th International Artemis Congress on Humanities and Social Sciences Proceedings Book*, 5.

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting*, *20*(1).

Deloitte. (2020). Reshaping the cybersecurity landscape. In *Delloite.com*. https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/risk/Cybersecurity.pdf

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain Technology in the Future of Business Cyber Security and Accounting. *Journal of Management Analytics*, *7*(2), 1–20. https://doi.org/10.1080/23270012.2020.1731721

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2).

European Union Agency for Cybersecurity. (2020). *The year in review* (p. 24).

Fadziso, T., Rao Thaduri, U., Dekkati, S., Rao Ballamudi, V. K., & Desamsetti, H. (2023). Evolution of the cyber security threat: An overview of the scale of cyber threat. *Digitalization & Sustainability Review*, *3*(1). https://doi.org/10.6084/m9.figshare.24189921.v1

Farrand, B., & Carrapico, H. (2024). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *13*(2).

Hair , J., Ringle, G., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM). *2nd Ed. Sage, Thousand Oaks*.

Hair Jr., J. F., M. Hult, G. T., M. Ringle, C., Sarstedt, M., Castillo Apraiz, J., Cepeda Carrión, G. A., & Roldán, J. L. (2019). *Manual de partial least squares structural*

*equation modeling (PLS-SEM) (segunda edición)*. OmniaScience. https://doi.org/10.3926/oss.37

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.

Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), 256–275.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common beliefs and reality about PLS. *Organizational Research Methods*, *17*(2), 182–209. https://doi.org/10.1177/1094428114526928

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: An event impact response framework. *Accounting Horizons*, *36*(4).

Laichuk, S., Maksym, Y., Koval, L., Dovzhyk, O., & Harkusha, S. (2023). Ensuring cybersecurity in accounting in the digital economy era. *Financial and Credit Activity-Problems of Theory and Practice*, *6*(53).

Le Guyader, L. P. (2019). Artificial intelligence in accounting: GAAP's "FAS133." *Journal of Corporate Accounting & Finance*. https://doi.org/10.1002/jcaf.22407

Li, Y. Q., Goel, S., & Williams, K. J. (2023). Exploring antecedents of professional skepticism on accounting students' performance in cybersecurity. *Journal of Emerging Technologies in Accounting*, *20*(1).

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).

Mendoza, A. L., Hernandez, R. S., Quezada, M. T. P., & Hernandez, R. V. (2023). Cybersecurity among university students from generation Z: A comparative study of the undergraduate programs in administration and public accounting in two

mexican universities. *TEM Journal-Technology Education Management Informatics*, *12*(1).

Merugula, S., Dinesh, G., Kathiravan, M., Das, G., Nandankar, P., & Karanam, S. R. (2021). Study of blockchain technology in empowering the SME. *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. https://doi.org/10.1109/icais50930.2021.9395831

Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875. MDPI. https://doi.org/10.3390/app13105875

Moniem Ali, O. A., Matarneh, A. J., Almalkawi, A., & Alhawamdeh, H. M. (2020). The impact of cyber governance in reducing the risk of cloud accounting in jordanian commercial banks - from the perspective of jordanian auditing firms. *Modern Applied Science*, *14*(3), 75. https://doi.org/10.5539/mas.v14n3p75

Muravskyi, V. (2021). *Accounting and cybersecurity - monograph*. Z.-M. Zadorozhnyi.

Nunnally, J. C. (1978). Psychometric theory. *2nd Ed. New York: McGraw-Hill.*

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance*, *29*(1), 53–58. https://doi.org/10.1002/jcaf.22291

Rodger, J. A., & George, J. A. (2017). Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global

cybersecurity vulnerability through information and communications technology. *Journal of Cleaner Production*, 142.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Saravanan, A., & Bama, S. S. (2019). A review on cyber security and the fifth generation cyberattacks. *Oriental Journal of Computer Science and Technology*, *12*(2), 50–56. https://doi.org/10.13005/ojcst12.02.04

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research*, *69*(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049

Silva, G. M., Styles, C., & Lages, L. F. (2017). Breakthrough innovation in international business: The impact of tech-innovation and market-innovation on performance. *International Business Review*, *26*(2), 391–404. https://doi.org/10.1016/j.ibusrev.2016.10.001

Smith, S. S. (2020). Emerging technologies and implications for financial cybersecurity. *International Journal of Economics and Financial Issues*, *10*(1), 27–32. https://doi.org/10.32479/ijefi.8844

Wang, R., Lin, Z., & Luo, H. (2018). Blockchain, bank credit and SME financing. *Quality & Quantity*, *53*(3), 1127–1140. https://doi.org/10.1007/s11135-018-0806-6

World Economic Forum. (2016). *The Global Risks Report 2016 11th Edition Insight Report* (p. 103). https://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

Zadorozhnyi, Z. M., Muravskyi, V., Yatsyshyn, S., & Bryk, M. (2021). The accounting system as the basis for organising enterprise cybersecurity. *Financial and Credit Activity-Problems of Theory and Practice*, *3*, 38.

Zadorozhnyi, Z. M., Muravskyi, V., Yatsyshyn, S., & Shevchuk, O. (2020). The accounting system as the basis for organising enterprise cybersecurity. *Financial and Credit Activity-Problems of Theory and Practice*, *3*, 34.

Apêndice 1 – Questão relacionada com a autorização da publicação dos dados do questionário.

Tomei conhecimento dos objetivos e características do estudo (de acordo com o Regulamento Geral de Proteção de Dados - RGPD), pretendo responder a este questionário e autorizo a publicação de dados, de forma agregada, para fins académicos. *

*Marcar apenas uma oval.*

- ◯ Sim.
- ◯ Não.

Apêndice 2 - Grupo de questões relativas à caracterização do respondente e empresa.

Idade *

*Marcar apenas uma oval.*

- ◯ <25 anos
- ◯ 25 - 35 anos
- ◯ 36 - 45 anos
- ◯ 46 - 55 anos
- ◯ >55 anos

Qual é a sua profissão? *

*Marcar apenas uma oval.*

- ◯ Contabilista/Técnico de contabilidade
- ◯ Gerente/Sócio Fundador
- ◯ Administrativo
- ◯ Diretor Financeiro
- ◯ Diretor de TI
- ◯ Engenheiro Informático
- ◯ Outro: _____

Qual é o setor da sua empresa? *

*Marcar apenas uma oval.*

- ◯ Comércio
- ◯ Serviços
- ◯ Indústria
- ◯ Outro: _____

Qual o volume de negócios? *

*Marcar apenas uma oval.*

- ◯ Inferior a 500 mil euros
- ◯ Entre 500 mil e 1 milhão de euros
- ◯ Entre 1 e 2 milhões de euros
- ◯ Superior a 2 milhões de euros

Apêndice 3 - Grupo de questões relativas à Qualidade do Sistema de Informação Contabilística.

**Qualidade do Sistema de Informação Contabilística (SIC)**

O Sistema de Informação Contabilística (SIC) é flexível em termos de processamento de dados. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O Sistema de Informação Contabilística (SIC) ajuda a alcançar objetivos da organização de forma rápida e precisa. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Os dados processados através do Sistema de Informação Contabilística (SIC) são consistentes com as políticas contabilísticas. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O custo do Sistema de Informação Contabilística (SIC) da empresa é consistente com a natureza e a dimensão da informação contabilística fornecida pelo sistema. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O Sistema de Informação Contabilística (SIC) na empresa permite a atualização fácil dos dados. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O Sistema de Informação Contabilística (SIC) fornece informação contabilística comparável. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O Sistema de Informação Contabilística (SIC) fornece informação contabilística integrada que afetará a eficácia da empresa.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

O Sistema de Informação Contabilística (SIC) é caracterizado pela facilidade de uso e alta qualidade. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

As entradas do Sistema de Informação Contabilística (SIC) são apresentadas de forma clara e evidente. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A entrada e saída de dados do Sistema de Informação Contabilística (SIC) são mantidas de forma segura. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Apêndice 4 - Grupo de questões relativas à Qualidade da Informação Contabilística.

A empresa distingue-se pela qualidade da sua informação contabilística.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Informação contabilística correta ajuda a empresa a tomar melhores decisões financeiras.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística é preparada para garantir a sua qualidade, precisão e exatidão.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística fornecida é consistente com as necessidades dos utilizadores em diferentes períodos financeiros.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística da empresa é flexível na sua utilização em vários aspetos.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informaçao contabilistica da empresa e clara e descomplicada. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística da empresa é facilmente compreendida pelos utilizadores.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística da empresa inclui todos os aspetos financeiros que os utilizadores necessitam para o processo de tomada de decisão.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística é fornecida atempadamente. *

*Marcar apenas uma oval.*

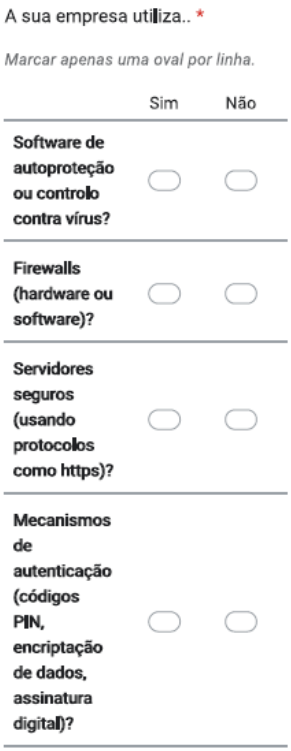
| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

A informação contabilística é facilmente armazenada e pode ser recuperada a qualquer momento.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Apêndice 5 - Grupo de questões relativas às Medidas de Segurança.



A sua empresa utiliza.. *

*Marcar apenas uma oval por linha.*

| | Sim | Não |
|---|---|---|
| Software de autoproteção ou controlo contra vírus? | | |
| Firewalls (hardware ou software)? | | |
| Servidores seguros (usando protocolos como https)? | | |
| Mecanismos de autenticação (códigos PIN, encriptação de dados, assinatura digital)? | | |

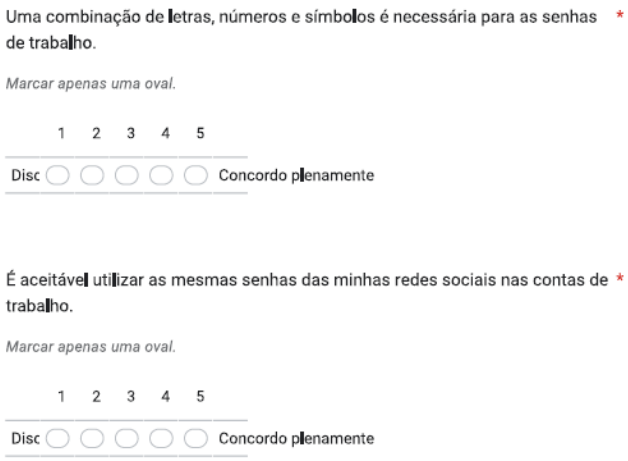
Apêndice 6 - Grupo de questões relativas à Integração de Sistemas de Informação Externos.

A sua empresa…

1- utiliza uma extranet?
2- utiliza EDI (Electronic Data Interchange -Transferência eletrónica de dados)?
3- utiliza ferramentas de rastreamento?
4- utiliza um sistema de compras/vendas associado a sistemas internos de gestão de stocks?
5- utiliza sistemas de compras/vendas integrados com os sistemas internos para faturação e pagamentos?
6- utiliza sistemas de compras/vendas integrados com os sistemas internos para gestão de operações?
7- recebe encomendas através da internet?
8- recebe encomendas através de EDI (Electronic Data Interchange - Transferência eletrónica de dados)?
9- faz encomendas através da internet?

10- faz encomendas através de EDI (Electronic Data Interchange - Transferência eletrónica de dados)?
11- tem o sistema integrado com o do seu maior cliente para encomendas e faturação?
12- tem o seu sistema integrado com o dos seus maiores fornecedores para a gestão de encomendas e faturação?

Apêndice 7 - Grupo de questões relativas ao Conhecimento sobre políticas e procedimentos.


Uma combinação de letras, números e símbolos é necessária para as senhas de trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É aceitável utilizar as mesmas senhas das minhas redes sociais nas contas de trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Não me é permitido clicar em *links* em *e-mails* de remetentes desconhecidos. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Tenho permissão para abrir anexos de *e-mails* de remetentes desconhecidos. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Enquanto estiver no trabalho, não devo aceder a *sites* de confiança duvidosa. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Tenho permissão para inserir qualquer informação num *site*, desde que me ajude a fazer o meu trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Quando estou num local público, tenho de manter o meu portátil comigo em todos os momentos. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Tenho permissão para enviar ficheiros de trabalho sensíveis via *Wi-Fi* público. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Documentos impressos sensíveis podem ser eliminados da mesma forma que os documentos não sensíveis. *

*Marcar apenas uma oval.*

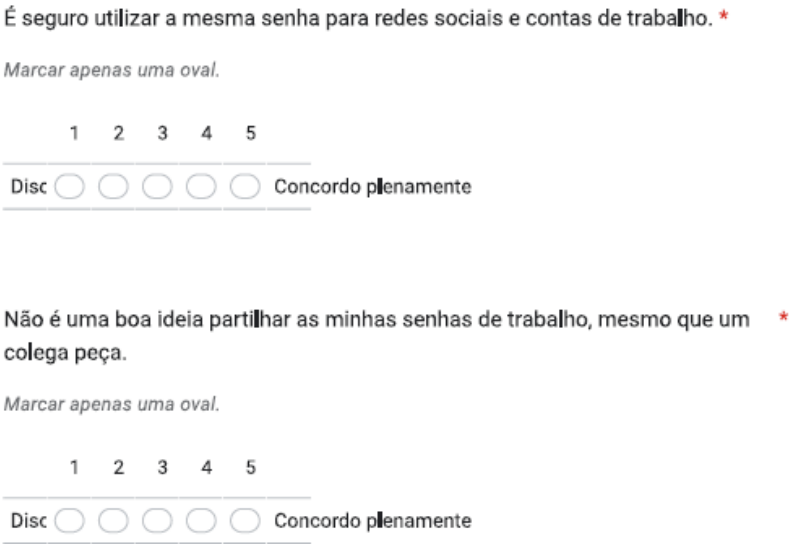
| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É importante reportar todos os incidentes de segurança. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Apêndice 8 - Grupo de questões relativas à Atitude em relação às políticas e procedimentos.



É seguro ter uma senha de trabalho apenas com letras. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É sempre seguro clicar em *links* em *e-mails* de pessoas que conheço. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Nada de mal pode acontecer se clicar num *link* num *e-mail* de um remetente desconhecido.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É arriscado abrir um anexo de um *e-mail* de um remetente desconhecido. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Pode ser arriscado descarregar ficheiros da *internet* para o meu computador de trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Só porque consigo aceder a um *site* no trabalho, não significa que seja seguro. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É arriscado enviar ficheiros de trabalho sensíveis via *Wi-Fi* público. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

É arriscado aceder a ficheiros sensíveis num portátil se estranhos puderem ver o meu ecrã. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Apêndice 9 - Grupo de questões relativas ao comportamento em relação às políticas e procedimentos.

Utilizo uma senha diferente para as minhas redes sociais e contas de trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Utilizo uma combinação de letras, números e símbolos nas minhas senhas de trabalho. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Não clico sempre em *links* de *e-mails* só porque vêm de alguém que conheço. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Não abro anexos de *e-mails* se o remetente for desconhecido. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Descarrego quaisquer ficheiros para o meu computador de trabalho que me ajudem a concluir o trabalho.

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Avalio a segurança dos *sites* antes de inserir informações. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Quando estou num local público, deixo o meu portátil sem supervisão. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Verifico se estranhos conseguem ver o meu ecrã, se estiver a trabalhar num documento sensível. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Deixo documentos impressos com informações sensíveis na minha secretária quando não estou lá. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

Se ocorrer um incidente de segurança, reporto-o imediatamente. *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Disc | ◯ | ◯ | ◯ | ◯ | ◯ | Concordo plenamente |

## Apêndice 10 - Primeiro email enviado às empresas

Questionário sobre Cibersegurança nas áreas da Contabilidade e Finanças das PME's

Exmo(a). Senhor(a),

O meu nome é Gonçalo Santos e sou estudante do Mestrado em Contabilidade e Finanças no Instituto Superior de Contabilidade e Administração do Porto (ISCAP).

No âmbito da minha dissertação, estou a realizar um estudo sobre cibersegurança nas Pequenas e Médias Empresas (PME's) em Portugal, com especial foco nas áreas da contabilidade e das finanças.

Gostaria de convidá-lo(a) a participar neste estudo, preenchendo um breve questionário. A sua participação é extremamente importante para compreender as práticas de cibersegurança adotadas pelas PME's e como estas influenciam a proteção de dados financeiros e contabilísticos.

Pode aceder ao questionário através do seguinte link.

Caso exista alguma dúvida, deixo o meu contacto na assinatura do e-mail.

Agradeço desde já o tempo dispensado e a sua valiosa contribuição para este estudo.

**Com os melhores cumprimentos,**

**Gonçalo Santos**

**Tlm: +351 9141[redacted]**

Apêndice 11 – Artigo publicado, intitulado "Integração dos desafios da cibersegurança na agenda dos Contabilistas e Investigadores"

**Título:** "Integração dos desafios da cibersegurança na agenda dos Contabilistas e Investigadores"

**Autores:**
Amélia Silva, CEOS.PP, Politécnico do Porto, acfs@iscap.ipp.pt
Albertina Paula Monteiro, CEOS.PP, Politécnico do Porto, amonteiro@iscap.ipp.pt
Gonçalo Santos, ISCAP, Politécnico do Porto, 2220310@iscap.ipp.pt

## 1. Introdução

A problemática da cibersegurança no campo da contabilidade está ainda pouco refletida entre os profissionais de contabilidade. Sendo um tema emergente, que cruza várias áreas de conhecimento, a investigação é ainda muito incipiente. Neste contexto, os profissionais e os académicos são desafiados a sair da sua zona de conforto e analisar, em conjunto, como podem dar resposta aos desafios da cibersegurança. Este artigo explora os riscos, desafios e melhores práticas associadas à segurança dos dados financeiros e identifica oportunidades de investigação.

## 2. Integração dos desafios da cibersegurança na agenda dos Contabilistas

A cibersegurança, crucial para proteger sistemas, redes e dados ligados à Internet, tem evoluído consideravelmente devido ao aumento de dispositivos interligados e à sofisticação dos ataques cibernéticos. Inicialmente focada na defesa de infraestruturas governamentais, agora abrange todos os tipos de entidades, incluindo pequenas e médias empresas (PMEs). A frequência e a sofisticação dos ciberataques têm vindo a aumentar de forma constante. Os ataques evoluíram de vírus simples para ataques tecnicamente complexos, exigindo assim abordagens proativas e uma gestão contínua do risco, especialmente no setor financeiro e contabilístico (Thaduri et al., 2023).

De acordo com um relatório da PwC (2020), 62% das empresas sofreram incidentes cibernéticos em 2019, uma tendência que continua a crescer anualmente. Segundo o Nacional de Cibersegurança (2023), em 2022, 43% das empresas portuguesas tinham uma política de segurança das Tecnologias da Informação e Comunicações (TIC) definida, mas apenas 28% aplicaram a autenticação multifatorial. A gravidade da situação é sublinhada pelo Banco de Portugal (2017), ao afirmar que os riscos cibernéticos podem

comprometer a conformidade legal e a estabilidade financeira. Neste contexto, as práticas básicas de segurança e identificação de dados críticos são essenciais para a proteção contra as atividades ilegais (Pendley, 2018), particularmente em empresas que adotam tecnologias na nuvem (Matarneh et al., 2020).

As empresas de contabilidade e de auditoria, que armazenam e processam grandes volumes de dados sensíveis, como históricos de transações e informações fiscais e financeiras de clientes, fornecedores e trabalhadores, são alvos privilegiados dos cibercriminosos. Exemplos disso incluem o phishing, que tem por objetivo roubar credenciais ou instalar malware, e o ransomware, situação em que o software malicioso encripta os dados, exigindo de seguida pagamentos avultados para a sua reposição. O acesso não autorizado a informações pode levar ao roubo de identidade, fraude financeira e perdas económicas significativas (AICPA, 2019), com consequentes danos na reputação e incumprimento de obrigações legais. A este propósito, Litt et al. (2023), analisaram o impacto da uma falha de cibersegurança na reputação de uma das "Big 4", e os autores Reidenbach e Wang (2021), estudaram as consequências, em termos financeiros e de auditoria, das falhas do sistema de segurança da Heartland Payment Systems, e as consequências foram altamente negativas em ambos os casos.

Na verdade, a confiança é uma pedra angular da profissão de auditoria. Clientes, investidores e reguladores confiam na avaliação dos auditores que, por sua vez, dependem da exatidão e da integridade dos dados financeiros para realizar as suas avaliações. A importância da confiança na área da auditoria, levaram Slapnicar et al. (2022) a desenvolver um "Índice de Auditoria de Cibersegurança", tendo os autores concluído que a maturidade da gestão de riscos cibernéticos está positivamente associada à eficácia da auditoria. Neste mesmo sentido, Li et al. (2024) comprovaram que os auditores que já tiveram experiência com incidentes de cibersegurança nos seus clientes, alteraram a sua atitude em termos de gestão de risco de auditoria e passaram a cobrar honorários mais altos a esses clientes. Além disso, estes auditores começaram a promover a implementação de políticas de cibersegurança junto dos clientes que ainda não tinham sido vítimas de ciberataques.

Além de tudo isto, as empresas de contabilidade têm de cumprir vários regulamentos e normas, como o Regulamento Geral sobre a Proteção de Dados (RGPD) na Europa e a Lei Sarbanes-Oxley nos Estados Unidos. Estes regulamentos impõem controlos rigorosos sobre a proteção de dados e exigem que as empresas implementem medidas robustas de cibersegurança. O incumprimento pode resultar em pesadas coimas, entre outras

consequências legais. Para mitigar os riscos, a legislação europeia e as diretrizes do Banco de Portugal impõem medidas proativas, como sistemas de deteção de intrusões e gestão de incidentes.

Com efeito, a implementação de estratégias bem estruturadas pode mitigar riscos e aumentar a resistência contra ameaças futuras (Johnson & Thompson, 2021). Entre as medidas recomendadas destacam-se as seguintes: (i) realizar avaliações de risco regulares (NIST, 2018); (ii) conhecer a legislações e práticas recomendadas para garantir a integridade dos dados (Pendley, 2018), (iii) utilizar software de segurança de código aberto e promover a formação e sensibilização contínua de funcionários (ENISA, 2020; Johnson & Thompson, 2021), (iv) utilizar tecnologias de segurança avançadas, como a tecnologia blockchain (Smith & Zhang, 2020), a autenticação multifactor e os sistemas de deteção de intrusão (CISA, 2020), (v) desenvolver e atualizar regularmente os planos de resposta a incidentes e as medidas de segurança (SANS Institute, 2019). Não obstantes estas medidas ajudarem salvaguardar a integridade dos dados, a verdade é que uma estratégia eficaz de cibersegurança exige recursos financeiros e humanos significativos, muitas vezes inacessíveis às PMEs, deixando estas empresas mais vulneráveis a ataques cibernéticos (ISACA, 2019).

## 3. Integração dos desafios da cibersegurança na agenda de investigação

A investigação em cibersegurança na contabilidade apresenta várias oportunidades que podem contribuir significativamente para a melhoria das práticas e políticas no setor.

Entre as principais áreas identificadas, suportadas por literatura científica, está o desenvolvimento de modelos preditivos de ameaças cibernéticas, que envolve a exploração de métodos avançados de análise de dados e de machine learning para prever ameaças específicas que podem afetar os sistemas de contabilidade e auditoria (Chou et al., 2019), além de investigar a eficácia de diferentes técnicas de machine learning na deteção precoce de anomalias e de comportamentos suspeitos em sistemas financeiros (Tam et al., 2021).

Outro foco de estudo é o impacto das falhas de segurança na reputação e valor das empresas, onde se analisa como as falhas de cibersegurança afetam a reputação das empresas de auditoria e de contabilidade, assim como as suas avaliações financeiras (Gordon et al., 2015), e se estuda como diferentes setores económicos são afetados por essas falhas, bem como quais são as estratégias mais eficazes para mitigar esses impactos (Eling & Schnell, 2016).

A integração de cibersegurança nos currículos de contabilidade também é uma área de interesse, com a avaliação da eficácia de diferentes abordagens pedagógicas para incorporar cibersegurança nos currículos de contabilidade e auditoria (Janvrin & Watson, 2017). Por exemplo, Boss et al., (2020) investigaram a percepção e preparação dos estudantes de contabilidade em relação aos desafios de cibersegurança no mercado de trabalho.

A relevância do assunto levou alguns autores a explorar a relação entre cibersegurança e desempenho financeiro das empresas. Goel e Shawky (2009) estudaram como o investimento em cibersegurança pode influenciar o desempenho financeiro. Outros autores, como Akam et al. (2018) e Janvrin e Wang (2022), investigaram como a implementação de sistemas robustos de cibersegurança pode afetar a eficiência operacional e o desempenho financeiro e não financeiro.

No campo da educação, a discussão sobre se a incorporação da cibersegurança no currículo dos cursos de contabilidade e auditora é uma área de investigação relevante (Li et al., 2023). Boss et al. (2022) argumentam que a cibersegurança deve ser incorporada em todos os níveis do currículo de contabilidade. Eles propõem casos práticos que exploram questões como a divulgação de cibersegurança em relatórios financeiros e os impactos de falhas de segurança em auditorias e riscos associados ao armazenamento de informações pessoais.

Numa abordagem mais técnica, há estudos que avaliam as ferramentas e tecnologias de cibersegurança em auditoria, e examinam a eficácia de diferentes ferramentas, como autenticação biométrica e sistemas automatizados de monitoramento (Janvrin et al., 2012). Numa abordagem similar, situam-se os trabalhos que propõem metodologias para avaliar a eficácia e eficiência das práticas de cibersegurança implementadas pelas empresas de auditoria (Pincus et al., 2017).

Por outro lado, o ceticismo profissional e as competências em cibersegurança são estudados para entender seu impacto na performance dos auditores (Hurley et al., 2013), além de investigar como a pressão profissional e os traços de personalidade dos contabilistas afetam sua capacidade de lidar com ameaças cibernéticas (Li et al., 2023).

Uma outra linha de investigação procura desenvolver e validar frameworks de resposta a incidentes de cibersegurança de modo a minimização dos impactos financeiros e operacionais (SANS Institute, 2019). Neste contexto, os casos práticos de empresas que enfrentaram falhas de cibersegurança são estudados para identificar melhores práticas e áreas de melhoria (Reidenbach & Wang, 2021).

A busca de padrões e a identificação de efeitos do contágio de falhas de cibersegurança, particularmente entre empresas do mesmo setor, são um tema de investigação com interesse prático, pois permite identificar estratégias para mitigar esses efeitos (Kelton & Pennington, 2020).

O impacto das características dos conselhos de administração na cibersegurança também foi alvo de estudo. Por exemplo, Héroux e Fortin (2024) analisaram como a expertise em Técnologias de Informação, a independência e a diversidade de género influenciam as políticas e práticas de cibersegurança das empresas, enquanto Jiang et al. (2022) avaliaram a eficácia dos comités de cibersegurança dentro dos conselhos de administração na promoção de práticas de cibersegurança robustas.

Finalmente, importa realçar que existe uma pressão crescente para que as empresas divulguem informações específicas sobre as suas estratégias de cibersegurança e os reguladores financeiros emitam requisitos cada vez mais rigorosos para melhorar a qualidade deste reporte (Héroux & Fortin, 2020; Kelton & Pennington, 2020, Kelton, 2021; Jiang et al. 2022; Masoud & Al-Utaibi (2022). Com efeito, a eficácia das políticas de divulgação de riscos de cibersegurança tem-se afirmado como um campo de investigação muito relevante. Héroux e Fortin (2020) analisaram a eficácia dessas políticas na melhoria da transparência e confiança dos investidores, enquanto Kelton & Pennington (2020) estudaram a resposta do mercado às divulgações voluntárias de cibersegurança na percepção do mercado e na mitigação dos efeitos de contágio. No entanto, Wang et al. (2022) alertam para o facto de poder haver lugar a reações negativas do mercado quando as empresas divulgam as suas falhas de cibersegurança, sugerindo assim que a transparência nas divulgações de cibersegurança pode ter implicações complexas. Tratando-se de um tema para o qual ainda não há práticas consolidadas e consenso quanto aos seus efeitos financeiros e de sustentabilidade, a questão da divulgação, voluntária e involuntária, de informação sobre as estratégias de cibersegurança constituem um campo de investigação altamente relevante.

## 4. Conclusão

Em conclusão, podemos afirmar que, a integração da cibersegurança na contabilidade é essencial, a qual requer progressos que vai desde a formação académica até à prática profissional, para garantir a proteção adequada dos dados e a confiança nas informações contabilísticas. A investigação contínua e a adaptação curricular são fundamentais para preparar futuros profissionais para enfrentar os desafios crescentes neste campo.