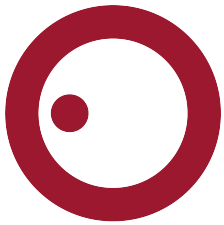


IPL

escola superior de tecnologia e gestão
instituto politécnico de leiria

Ciberconsciencialização em Contexto Académico: Estudo com Estudantes de Áreas não-CTEAM na ESTG-IPLeiria

Cristiana Isabel Santos Sousa

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

Leiria, Setembro 2025

Página intencionalmente deixada em branco.

escola superior de tecnologia e gestão
instituto politécnico de leiria

Ciberconsciencialização em Contexto Académico: Estudo com Estudantes de Áreas não-CTEAM na ESTG-IPLeiria

Cristiana Isabel Santos Sousa

Supervisor: Mário João Gonçalves Antunes
Professor Coordenador, Politécnico de Leiria

Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

Dissertação

Leiria, Setembro 2025

Página intencionalmente deixada em branco.

Ciberconsciencialização em Contexto Académico: Estudo com Estudantes de Áreas não-CTEAM na ESTG-IPLeiria

Página intencionalmente deixada em branco.

Agradecimentos

O desenvolvimento desta dissertação foi um percurso repleto de desafios e incertezas, mas também de apoio, inspiração e força. Por isso, expresso aqui o meu agradecimento a todos os que me acompanharam ao longo desta jornada.

Ao Professor Doutor Mário Antunes, agradeço pela sua orientação, apoio, disponibilidade, ensinamentos e esclarecimento de dúvidas, tornando possível a concretização deste trabalho.

Aos Investigadores Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac e Tara Zwaans, manifesto a minha sincera gratidão por autorizarem utilizar a escala que desenvolveram, essencial para a realização deste estudo.

Aos Professores Coordenadores de Curso, Doutor Luís Cabral de Oliveira, Doutora Magali Pedro Costa, Doutor Ricardo Marques, Doutora Liliana Vitorino e Dr. Jorge Barros Mendes, deixo um agradecimento pela ajuda na divulgação do questionário junto dos estudantes.

Às Professoras Célia Santos e Susana Cardal, agradeço por disponibilizarem tempo de aula para a realização de uma sessão de sensibilização sobre a cibersegurança, contribuindo diretamente para a relevância prática deste trabalho.

Por fim, agradeço aos meus colegas, amigos e familiares, cujo apoio, incentivo e compreensão foram fundamentais para a conclusão desta etapa.

Página intencionalmente deixada em branco.

Resumo

A evolução tecnológica e a crescente digitalização da sociedade têm provocado transformações significativas na forma como as pessoas comunicam, estudam, trabalham e interagem com o mundo. No entanto, esta dependência da tecnologia também aumenta a exposição a riscos como fraudes, roubo de identidade e outras ameaças associadas ao cibercrime. Neste contexto, a cibersegurança assume um papel fundamental, não apenas para os profissionais da área das tecnologias, mas para todos os cidadãos.

Com o aumento da cibercriminalidade é essencial adotar práticas seguras no utilização das tecnologias. Contudo, os estudantes que frequentam cursos fora das áreas da Ciência, Tecnologia, Engenharia, Artes e Matemática (CTEAM) têm, geralmente, menos contacto com conceitos e práticas de cibersegurança na sua formação académica.

Este trabalho tem como objetivo avaliar o nível de consciencialização para a cibersegurança dos estudantes da Escola Superior de Tecnologia e Gestão (ESTG) do Politécnico de Leiria, que não pertencem a cursos das áreas de CTEAM, com vista à implementação de estratégias de sensibilização. A avaliação utiliza a escala *Human Aspects of Information Security Questionnaire* (HAIS-Q) para medir os conhecimentos, as atitudes e os comportamentos dos estudantes em diferentes tópicos da cibersegurança. O questionário foi respondido por 104 estudantes e os resultados revelaram que, embora muitos participantes demonstrem alguma perceção dos riscos digitais, ainda persistem comportamentos vulneráveis em áreas específicas, evidenciando a importância da ciberconsciencialização. A estratégia de sensibilização consistiu em duas partes principais: aula aberta focada nos principais comportamentos de risco abordados pela escala HAIS-Q; e desenvolvimento de um vídeo explicativo disponibilizado *online*. Esta abordagem demonstrou ser eficaz na promoção de comportamentos mais seguros na utilização das tecnologias.

Esta dissertação contribui para a área da ciberconsciencialização ao centrar-se num público menos estudado e que combina uma avaliação e uma intervenção prática. A dissertação reforça ainda a importância de integrar conteúdos de cibersegurança nos planos de estudo, especialmente fora das áreas tecnológicas, promovendo a formação de cidadãos mais conscientes, responsáveis e preparados para enfrentar os desafios do mundo digital.

Palavras-Chave: Cibersegurança, Ciberconsciencialização, Competências Digitais, Educação Digital

Página intencionalmente deixada em branco.

Abstract

Technological evolution and the increasing digitalization of society have led to significant changes in the way people communicate, study, work and interact with the world. However, this dependence on technology also increases exposure to risks such as fraud, identity theft and other threats associated with cybercrime. In this context, cybersecurity plays a fundamental role, not just for technology professionals, but for all citizens.

With the rise in cybercrime, it is essential to adopt safe practices when using technology. However, students who attend courses outside the fields of Science, Technology, Engineering, Arts, and Mathematics (STEAM) generally have less contact with cybersecurity concepts and practices in their academic training.

This study aims to assess the level of cybersecurity awareness among students at the School of Technology and Management of the Polytechnic of Leiria, who are not enrolled in STEAM courses, with the goal of implementing awareness strategies. The assessment uses the Human Aspects of Information Security Questionnaire (HAIS-Q) scale to measure the students' knowledge, attitudes, and behaviors on different cybersecurity topics. The questionnaire was answered by 104 students, and the results revealed that, although many participants demonstrate some awareness of digital risks, vulnerable behaviors still persist in specific areas, highlighting the importance of cyber awareness. The awareness strategy consisted of two main parts: an open class focused on the main risky behaviors addressed by the HAIS-Q scale; and the development of an explanatory video published online. This approach proved to be effective in promoting safer behaviors in the use of technology.

This dissertation contributes to the field of cyber awareness by focusing on a less studied audience and combining an assessment with a practical intervention. The dissertation also reinforces the importance of integrating cybersecurity content into study plans, especially outside of technological areas, promoting the training of more aware, more responsible, and better prepared citizens to face the challenges of the digital world.

Keywords: Cybersecurity, Cyber-awareness, Digital Skills, Digital Education

Página intencionalmente deixada em branco.

Conteúdo

Página intencionalmente deixada em branco.

Lista de Figuras

Página intencionalmente deixada em branco.

Lista de Tabelas

Página intencionalmente deixada em branco.

Página intencionalmente deixada em branco.

Siglas

CAS Cybersecurity Attitudes Scale. (*p. 24*, *25*)
CET Cursos de Especialização Tecnológica. (*p. 41*)
CNAES Concurso Nacional de Acesso ao Ensino Superior. (*p. 28*, *41*, *74*, *82–84*)
CNCS Centro Nacional de Cibersegurança. (*p. 34–36*)
CSE Computer Self-Efficacy. (*p. 24*)
CTEAM Ciência, Tecnologia, Engenharia, Artes e Matemática. (*p. iv*, *3*, *4*, *17*, *18*, *20*, *24*, *27*, *28*, *31*, *37–39*, *85*, *89*, *90*, *92*)

DVD Digital Video Disc. (*p. 30*)

ESAD.CR Escola Superior de Artes e Design. (*p. 4*)
ESECS Escola Superior de Educação e Ciências Sociais. (*p. 4*)
ESSLei Escola Superior de Saúde. (*p. 4*)
ESTG Escola Superior de Tecnologia e Gestão. (*p. iv*, *4*, *24*, *27*, *31*, *37*, *39*, *90*, *92*)
ESTM Escola Superior de Turismo e Tecnologia do Mar. (*p. 4*)

GPIUS2 Generalized Problematic Internet Use Scale 2. (*p. 24*)

HAIS-Q Human Aspects of Information Security Questionnaire. (*p. iv*, *vii*, *4*, *5*, *19*, *24–32*, *43*, *90*, *92*)

IA Inteligência Artificial. (*p. 36*, *92*)
IEEE Institute of Electrical and Electronics Engineers. (*p. 7*)
IP Internet Protocol. (*p. 11*)

KAB Knowledge-Attitude-Behavior. (*p. 28*)

M23 Maiores de 23 anos. (*p. 41*)

PRISMA Preferred Reporting Items for Systematic reviews and Meta-Analyses. (*p. 6*)

STEAM Science, Technology, Engineering, Arts, and Mathematics. (*p. vii*)

TeSP Cursos Técnicos Superiores Profissionais. (*p. 4*, *41*)

TI Tecnologias de Informação. (*p. 29*)

USB Universal Serial Bus. (*p. 30*, *33*, *65–67*, *88*, *90*)

VPN Virtual Private Network. (*p. 13*, *33*)

WWW World Wide Web. (*p. 1*)

Página intencionalmente deixada em branco.

1 Introdução

A Internet teve origem no contexto militar durante a Guerra Fria, com o objetivo de desenvolver um sistema de comunicação que conseguisse resistir a um eventual ataque nuclear (Naughton, 2016). Entre 1983 e 1995, expandiu-se para universidades e centros de investigação, sendo o email a principal forma de utilização na época. Com o surgimento do World Wide Web (WWW), tornou-se acessível ao público em geral, popularizou-se e foi evoluindo para o que existe atualmente (Naughton, 2016).

A utilização da Internet cresceu de forma exponencial, com os indivíduos e as empresas a efetuarem, atualmente, múltiplas transações diárias *online* e não no mundo real. Esse crescimento também fez com que crimes tradicionais migrassem para o meio digital (Aslan et al., 2023). Apesar da Internet, dos computadores e dos *smartphones* terem transformado o mundo e de se terem tornado uma parte indispensável do nosso dia-a-dia, também facilitaram a prática de crimes (Holt et al., 2015).

Cibercrime é o termo utilizado para descrever qualquer ato criminoso que envolve tecnologia, seja como ferramenta, alvo ou local de atividade, que têm como objetivo obter ilegalmente informações sensíveis ou distribuir programas informáticos destrutivos, causando perturbações que podem prejudicar pessoas ou empresas (Das et al., 2013; Gupta et al., 2016; Goni et al., 2022). A rápida expansão e diversificação das estratégias da cibercriminalidade representam um grande desafio, tanto para compreender a dimensão dos riscos envolvidos quanto para desenvolver políticas eficazes de prevenção (Sabillon et al., 2016).

Nesse contexto, a cibersegurança surgiu como um conjunto de medidas e ações destinadas a proteger redes, sistemas de informação e as pessoas que interagem nesses ambientes (Conselho de Ministros n.º 92/2019, 2019). Contudo, o termo é frequentemente utilizado para descrever situações em que dispositivos pertencentes a indivíduos, empresas ou infraestruturas críticas estão sob ataque ou em risco de serem atacados (Bay, 2016). Além disso, o conceito tem sido muitas vezes associado à segurança da informação. Enquanto a segurança da informação incorpora o papel do ser humano no

processo de proteção, a cibersegurança trata-o como um potencial alvo (Thakur et al., 2016).

Atualmente, praticamente todos os sistemas enfrentam ameaças à sua segurança digital, sendo, por isso, essencial que incorporem funcionalidades de segurança como parte integrante da sua arquitetura (Borky et al., 2019). Embora seja crucial proteger os sistemas e as redes, é igualmente importante que as pessoas adotem medidas para se protegerem contra possíveis ameaças. Para isso ser possível, é importante mudar comportamentos, devido a grande parte dos incidentes de segurança estar relacionada ao fator humano (Mersinas et al., 2025).

De acordo com o relatório de cibercrime disponibilizado pelo Ministério Público, o Gabinete de Cibercrime recebeu 3973 denúncias em 2024. Em comparação com o ano anterior, que registou 2916 denúncias, verificou-se um aumento de 36,25%. Os cibercrimes mais recorrentes foram as burlas do tipo "*olá mãe, olá pai*", as fraudes relacionadas com falsos pagamentos de faturas de eletricidade, o *phishing*, as burlas *online* e as chamadas telefónicas fraudulentas (Cibercrime, 2025).

Tendo em conta o crescimento contínuo da cibercriminalidade ao longo dos anos e o tipo de ataques serem mais direcionados ao utilizador e não tanto ao sistema, tornou-se essencial capacitar os utilizadores para se protegerem das ameaças digitais. A adoção de boas práticas de cibersegurança por parte dos utilizadores contribui significativamente para a proteção dos seus dados pessoais e dispositivos, e pode reduzir de forma eficaz o número de violações de segurança (Mersinas et al., 2025).

1.1 Importância do Estudo

Apesar da Internet ter um impacto positivo na vida das pessoas, também apresenta desafios, como, por exemplo, as fraudes *online* (Rahman et al., 2020; Amankwa et al., 2021). Muitas vezes, os indivíduos são vítimas deste tipo de ameaças, devido à falta de consciencialização e da adoção de mecanismos de proteção (Rahman et al., 2020).

Promover a sensibilização e o conhecimento sobre a cibersegurança desde jovens é essencial para educar sobre como agir de forma segura e para prevenir os riscos da utilização da Internet (Rahman et al., 2020; Amankwa et al., 2021). No entanto, para as pessoas que não possuem formação na área das tecnologias, como as que ainda não concluíram os estudos ou que estão fora do sistema educativo, existe uma falta de programas que ofereçam informações sobre a cibersegurança (Mcnulty et al., 2020).

Um estudo, com o objetivo de evidenciar a importância da sensibilização para a cibersegurança, desenvolveu um programa de treino para a educação cibernética destinado a funcionários sem formação na área das tecnologias (Keshvadi, 2023). Após a implementação do programa de treino 83% dos participantes relatou compreender melhor as causas dos ciberataques, 93% dos participantes demonstraram um melhor conheci-

mento das políticas de cibersegurança das suas organizações e 100% dos participantes aprovaram a integração da educação sobre cibersegurança na formação de segurança da sua organização (Keshvadi, 2023).

Uma das formas mais eficazes de sensibilizar as pessoas para a importância da cibersegurança é incluir programas de sensibilização nas escolas. A escola deve desempenhar um papel ativo na transmissão de conhecimentos e na sensibilização para a importância da cibersegurança, preparando os estudantes para adotarem boas práticas, tanto a nível pessoal como no seu futuro profissional.

Atualmente, existem alguns programas que podem ser integrados desde o 1º ciclo até ao ensino secundário, com o objetivo de promover a consciencialização e a adoção de comportamentos seguros na Internet. Entre eles destacam-se iniciativas como o SeguraNet[1] e o Internet Segura[2] que visam promover uma utilização mais segura e responsável da Internet entre crianças e jovens.

No caso do ensino universitário, os estudantes que não estudam em cursos de áreas de CTEAM muitas vezes não têm contacto com temas relacionados com a cibersegurança, apesar de serem fundamentais tanto para a vida académica quanto para o futuro profissional (Mcnulty et al., 2020).

Neste contexto, esta dissertação tem como foco os estudantes do ensino superior que frequentam cursos fora das áreas CTEAM. Esses estudantes podem, ou não, ter recebido algum tipo de formação relacionada com a cibersegurança no seu percurso académico anterior, mas atualmente estão inseridos em cursos onde as tecnologias não constituem o principal foco.
Assim, a principal motivação para a realização deste trabalho é:

1. Avaliar de que forma estes estudantes encaram as questões da cibersegurança. Dado que cada estudante possui um percurso académico e/ou profissional distinto, é essencial avaliar o que já sabem sobre cibersegurança, o que consideram ser comportamentos seguros ou inseguros, e que medidas adotam no seu dia-a-dia. Avaliar o seu nível de consciencialização permitirá identificar os pontos que necessitam de estratégias de sensibilização mais eficazes.
2. Sensibilizar estes estudantes para os riscos a que estão expostos e promover as boas práticas da cibersegurança. Para além de avaliar o seu nível de consciencialização, é igualmente importante transmitir conhecimentos atualizados sobre o tema. Mesmo que já possuam alguma informação, as ameaças e os métodos utilizados pelos cibercriminosos estão em constante evolução. Por isso, os conhecimentos e as práticas de segurança que adotam também devem acompanhar essa evolução.

[1] SeguraNet: `www.seguranet.pt`
[2] Internet Segura: `www.internetsegura.pt`

1.2 Contexto do Estudo

O presente trabalho foi desenvolvido no Politécnico de Leiria, que é uma instituição pública de ensino superior que iniciou a sua atividade na década de 1980 e localiza-se na região de Leiria e Oeste. A instituição tem cinco escolas superiores distribuídas pelas cidades de Leiria, Caldas da Rainha e Peniche. Em Leiria, encontram-se a Escola Superior de Educação e Ciências Sociais (ESECS), a Escola Superior de Tecnologia e Gestão (ESTG) e a Escola Superior de Saúde (ESSLei). Nas Caldas da Rainha, situa-se a Escola Superior de Artes e Design (ESAD.CR) e, em Peniche, a Escola Superior de Turismo e Tecnologia do Mar (ESTM).

Este trabalho foi realizado exclusivamente na ESTG. A escola foi criada em 1985 pelo Decreto do Governo n.º 46/85, de 22 de novembro, tendo iniciado a sua atividade académica no ano letivo de 1989/1990. Atualmente, é o maior estabelecimento de ensino superior do distrito de Leiria, oferecendo vários cursos técnicos superiores profissionais (TeSP), de licenciatura, mestrado e doutoramento, em regimes diurno e pós-laboral, nas áreas de Engenharia e Tecnologia, Ciências Empresariais e Ciências Jurídicas.

As atividades deste estudo foram desenvolvidas nos cursos de Administração Pública (Regime Diurno), Contabilidade e Finanças (Regime Diurno), Gestão (Regime Diurno e Pós-laboral), Marketing (Regime Diurno) e Solicitadoria (Regime Diurno e Pós-laboral).

1.3 Objetivos

O desenvolvimento deste trabalho teve como principal motivação compreender de que forma os estudantes do ensino superior, não pertencentes as áreas CTEAM, abordam a cibersegurança. E, além disso, sensibilizar esses estudantes para as ameaças existentes e para as melhores práticas que devem adotar.
Tendo em conta o contexto apresentado, e com o objetivo de orientar a sua execução, este trabalho foi estruturado em torno de dois objetivos principais:

1. **Avaliar o nível de consciencialização**
   Este objetivo foi cumprido através da disponibilização de um questionário baseado na escala HAIS-Q. O questionário utilizado avalia os conhecimentos, as atitudes e os comportamentos dos estudantes em relação vários tópicos da cibersegurança. Com o questionário foram recolhidas 104 respostas, que foram analisadas com recurso a estatística descritiva, com o objetivo de comparar os resultados médios entre os diferentes grupos de participantes.
2. **Implementar estratégias de sensibilização**
   Este objetivo foi atingido através do planeamento e realização de uma aula aberta, baseada nos tópicos abordados pela escala HAIS-Q. A aula foi realizada nos cursos de Gestão e Marketing, onde foram apresentados os problemas relativos a cada tópico da escala, as ameaças que podem surgir desses problemas, as possí-

veis medidas que podem ser adotadas para prevenir as ameaças e exemplos práticos para cada tópico como notícias e vídeos. Além disso, como não foi possível realizar as aulas em todos os cursos-alvo do estudo, os materiais utilizados foram reunidos num vídeo explicativo, posteriormente disponibilizado no YouTube.

1.4 Estrutura do Documento

Este relatório de dissertação está organizado em cinco capítulos, estruturados de modo a garantir uma leitura clara e sequencial do trabalho realizado.

O Capítulo 1 - Introdução - apresenta o tema central da dissertação, a motivação do seu desenvolvimento, o contexto em que se insere e os seus objetivos. Inclui ainda uma descrição da estrutura geral do documento.

O Capítulo 2 - Revisão Sistemática da Literatura - apresenta os estudos relacionados com a cibersegurança no contexto universitário. Descreve a metodologia adotada na seleção dos estudos e apresenta um resumo desses estudos. Além disso, enquadra os estudos revistos face aos objetivos desta dissertação, destacando as contribuições que este trabalho pretende proporcionar em comparação com a literatura existente.

O Capítulo 3 - Desenvolvimento - está dividido em três secções. A Secção 3.1 descreve a metodologia geral adotada na implementação do trabalho, detalhando as etapas envolvidas e o seu processo de desenvolvimento. A Secção 3.2 apresenta o desenvolvimento e a aplicação do questionário baseado na escala HAIS-Q. Esta secção descreve os motivos da sua escolha da escala, o processo de construção do questionário, o período de recolha de respostas, o público-alvo e as questões de investigação a que se pretende responder. A Secção 3.3 apresenta o origem da escala e a sua evolução ao longo do tempo, contemplando igualmente o seu funcionamento e a sua estrutura. A Secção 3.4 detalha o planeamento e a aplicação de uma aula de sensibilização para a cibersegurança. Descreve os tópicos abordados, o Quiz utilizado para avaliar a retenção dos conhecimentos, as datas e os cursos em que a aula foi realizada, bem como uma breve reflexão sobre a sua implementação. Adicionalmente, apresenta o processo de criação do vídeo explicativo dos conteúdos da aula, desenvolvido com recurso a inteligência artificial.

O Capítulo 4 - Análise de Resultados - apresenta uma análise individual por cada item da escala e apresenta uma discussão sobre os resultados obtidos, que recorre a estatística descritiva para responder às questões de investigação.

Por fim, o Capítulo 5 - Conclusão - apresenta uma reflexão sobre o trabalho efetuado, destacando os principais contributos, as limitações encontradas e sugestões para trabalho futuro.

2

Revisão Sistemática da Literatura

O presente capítulo apresenta uma análise dos estudos que incidem sobre a avaliação do nível de sensibilização para a cibersegurança em estudantes do ensino superior, alinhando-se, deste modo, com a temática deste trabalho.
A seleção dos estudos foi conduzida com base nas diretrizes da metodologia *Preferred Reporting Items for Systematic reviews and Meta-Analyses* (PRISMA), que permitiu sistematizar o processo de revisão (Secção 2.1). Concluídas todas as fases metodológicas, procedeu-se à apresentação de um resumo dos artigos selecionados (Secção 2.2). No final, estabeleceu-se uma relação crítica entre os estudos analisados e os objetivos delineados para este trabalho, evidenciando os contributos que este trabalho propõe face à literatura existente (Secção 2.3).

2.1 Metodologia de Pesquisa

O processo de pesquisa e seleção dos estudos relacionados com este trabalho foi realizado com o auxilio da metodologia PRISMA.[1] Esta metodologia contém diretrizes que asseguram que o processo de seleção, análise e inclusão dos trabalhos seja elaborado de forma sistemática e transparente.
O processo de pesquisa e seleção de trabalhos proposto pela metodologia divide-se em três fases:

- **Fase 1 - Identificação**: Nesta fase escolhem-se as bases de dados de trabalhos e em cada uma efetuam-se pesquisas com palavras-chave relativas ao tema pretendido. Ainda nesta fase, excluem-se trabalhos repetidos e que não estejam no período temporal definido.
- **Fase 2 - Triagem**: Nesta fase avaliam-se os estudos identificados de forma a excluir aqueles que não se enquadram no contexto pretendido.

[1] PRISMA: `https://www.prisma-statement.org/`

- **Fase 3 - Incluído**: Esta fase representa o resultado final da triagem e a revisão dos trabalhos selecionados.

A Figura 2.1 ilustra o fluxograma da metodologia PRISMA, com os resultados obtidos na pesquisa e análise dos estudos relacionados com este trabalho.

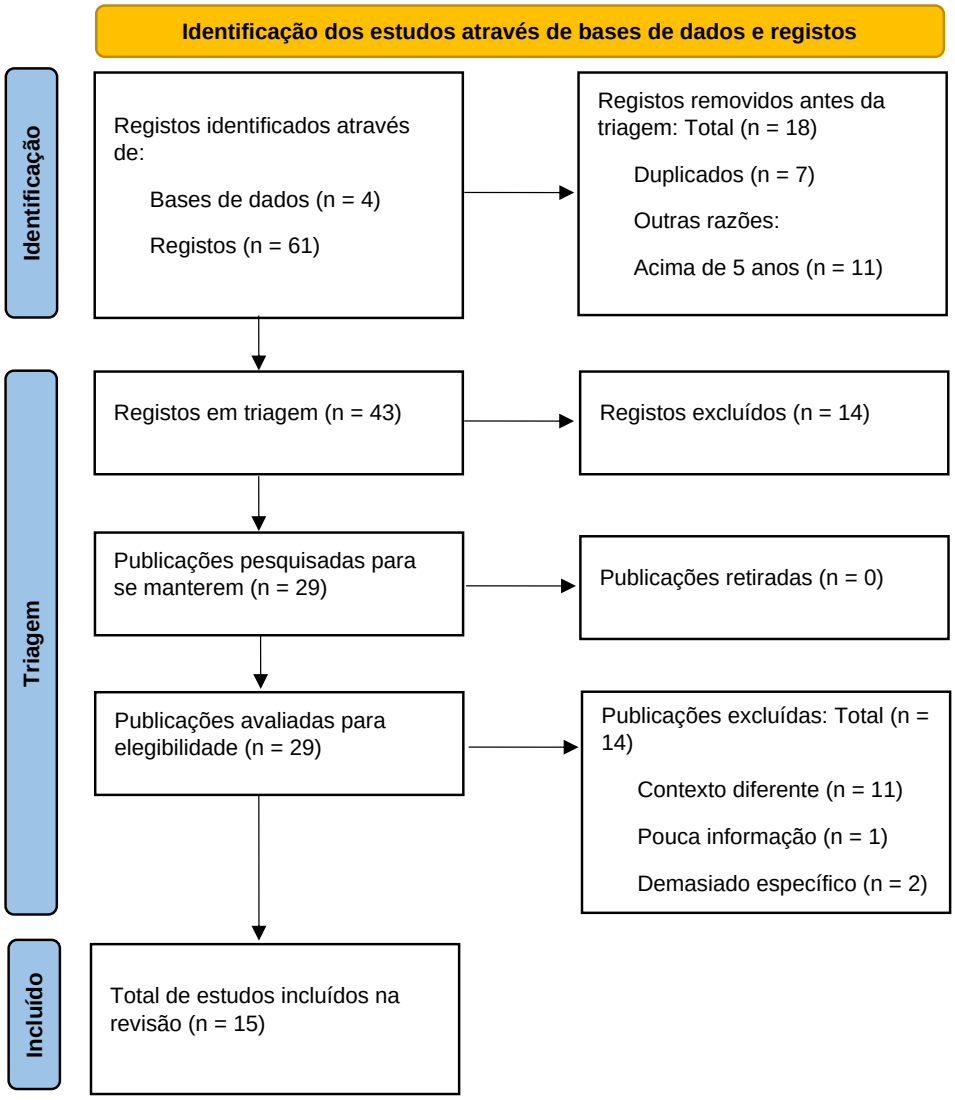


Figura 2.1: *Fluxograma da metodologia PRISMA.*

A **fase de identificação** teve como objetivo identificar todos os trabalhos que aparentavam estar relacionados como o tema pretendido. Para isso, foram escolhidas para realizar a pesquisa quatro bases de dados: Google Scholar[2], IEEE[3], Scopus[4] e ScienceDirect[5]. A escolha recaiu sobres estas bases de dados por serem bastante utilizadas para publicar artigos ou trabalhos de variados temas.

[2] Google Scholar: `https://scholar.google.com/`
[3] IEEE: `https://ieeexplore.ieee.org`
[4] Scopus: `https://www.scopus.com/`
[5] ScienceDirect: `https://www.sciencedirect.com/`

Para a pesquisa nas bases de dados escolhidas foram criadas algumas palavras-chave relacionadas com o tema deste trabalho. As palavras-chave utilizadas foram as seguintes:

- "*cyber awareness in higher education*"
- "cibersegurança no contexto escolar"
- "cibersegurança no ensino superior"
- "*cyber awareness*"

A pesquisa em cada uma das bases de dados utilizando as palavras-chave definidas, resultou na identificação de 61 trabalhos que, com base na leitura do seu título, aparentavam estar relacionados como o tema deste trabalho. Após a identificação dos trabalhos foram definidos e aplicados dois filtros de exclusão antes de se passar à fase de triagem. O primeiro filtro de exclusão foi a remoção de trabalhos duplicados, ou seja, os trabalhos que apareceram em mais do que uma base de dados. O segundo filtro de exclusão foi a definição de um período temporal como forma de garantir que os trabalho identificados são relevantes para a atualidade. O período temporal definido foi de cinco anos, ou seja, só foram incluídos trabalhos que foram publicados entre 2019 e 2024. A aplicação dos filtros resultou na remoção de 18 trabalhos, 7 que estavam duplicados e 11 que estavam fora do período temporal definido. Assim, dos 61 trabalhos previamente identificados, passaram para a fase de triagem 43 trabalhos.

A **fase de triagem** teve como objetivo analisar os trabalhos identificados de forma a remover os que não se enquadravam com o tema pretendido, isso foi feito recorrendo a três etapas de exclusão.
A primeira etapa de exclusão consistiu na leitura do resumo de todos os trabalhos identificados para remover os trabalhos que não possuíam uma relação direta com o tema pretendido. A execução desta etapa resultou na exclusão de 14 trabalhos.
A segunda etapa consistiu na verificação de acessibilidade às versões completas dos trabalhos identificados. Em todos os trabalhos foi possível aceder à versão completa pelo que não foi removido nenhum trabalho nesta fase.
A última etapa consistiu na leitura completa dos trabalhos identificados para remover os que não enquadravam com os objetivos deste trabalho. Nesta etapa foram removidos 14 trabalhos, 11 que apresentavam um contexto diferente do pretendido, 1 que carecia de profundidade o que tornou difícil de o enquadrar com este trabalho e 2 por serem excessivamente específicos para uma área.
A aplicação das etapas descritas anteriormente resultou na exclusão de um total de 28 trabalhos, 14 na primeira etapa, zero na segunda etapa e 14 na última etapa.

A **fase de inclusão**, que é a última fase desta metodologia, teve como objetivo aglomerar todos os trabalhos que foram aprovados nas fases anteriores para se proceder à sua revisão de forma a serem incluídos no tópico de trabalhos relacionados (Secção 2.2). Neste caso, após a execução de todos os procedimentos da metodologia, foram incluídos 15 trabalhos que se relacionam com o tema deste trabalho.

2.2 Trabalhos Relacionados

Nesta secção, descrevem-se os estudos selecionados após a aplicação da metodologia de pesquisa. Os estudos encontram-se organizados em quatro categorias que facilitam a compreensão do seu conteúdo.
A primeira categoria apresenta estudos que realizaram uma análise geral sobre os conhecimentos em cibersegurança, abordando aspetos como as práticas adotadas, os comportamentos online e os possíveis riscos a que os utilizadores podem estar expostos.
A segunda categoria reúne os estudos centrados no cibercrime, ou seja, estudos que procuraram compreender o nível de conhecimento dos utilizadores em relação aos diferentes tipos de ataques existentes.
A terceira categoria agrupa estudos que recorreram à simulação de ataques, com o objetivo de avaliar quão facilmente um utilizador pode tornar-se vítima de um ataque cibernético.
Por fim, a quarta categoria inclui os estudos cujo público-alvo não são instituições de ensino superior, mas o seu conteúdo foi considerado relevante para o contexto deste trabalho.

2.2.1 Avaliação do Nível de Consciencialização

Em (Raju et al., 2022) os autores avaliam, através de um questionário, o nível de consciencialização para a cibersegurança dos estudantes da *UiTM Terengganu Faculty of Computer and Mathematical Sciences* na Malásia, que contou com a participação de 110 estudantes. Os resultados indicaram que os participantes demonstram possuir conhecimentos sobre alguns aspetos da cibersegurança, como ciberataques, *ciberbullying* e proteção de informações pessoais. O estudo, no entanto, revelou, que apesar do conhecimento demonstrado, os participantes envolvem-se em atividades de risco, como a partilha de palavras-passe e o acesso a sítios *Web* desconhecidos. O estudo concluiu que ainda não existe um conhecimento aprofundado e adequado da cibersegurança entre os participantes.

Em (Zwilling et al., 2022) os autores analisam a relação entre a consciencialização, os conhecimentos e os comportamentos em matérias de cibersegurança, bem como a utilização de ferramentas de proteção. O estudo foi administrado através de um questionário aplicado a 459 estudantes universitários das áreas de gestão e administração, provenientes de instituições de ensino superior de Israel, Eslovénia, Polónia e Turquia. Os resultados indicaram que os participantes estão familiarizados com o conceito "cibersegurança" e que evitam a divulgação de informações sensíveis na *Web*. Os resultados, no entanto, revelam que os participantes, em geral, apenas tomam medidas básicas de proteção, como a utilização de palavras-passe fortes e a instalação de antivírus. Além disso, os participantes com maior conhecimento em informática demonstraram um nível mais elevado de consciencialização para a cibersegurança e implementam mais medidas preventivas contra ataques. O estudo concluiu que os participantes turcos

consideram as ameaças de cibersegurança mais alarmantes, enquanto os participantes israelitas e os polacos demonstram menos preocupação.

Em (Setiawan et al., 2024) os autores avaliam o nível de consciencialização para a segurança da informação de estudantes universitários após a pandemia da Covid-19. O estudo realizou um questionário a 52 estudantes de uma instituição de ensino superior em Surabaya, Indonésia. Os resultados indicaram que os participantes apresentavam um bom nível de consciencialização para a cibersegurança, embora tenham sido identificadas áreas que requerem melhorias. Destacando, dessas áreas, as atitudes em relação à gestão de palavras-passe, os conhecimentos e atitudes sobre a utilização do email e os conhecimentos e comportamentos associados à utilização da Internet e das redes sociais.

Em (Chen et al., 2021) os autores investigam os comportamentos problemáticos relacionados com a segurança da informação, a utilização compulsiva da Internet e o nível de consciencialização de estudantes universitários em Taiwan. O estudo contou com a participação de 514 estudantes provenientes de três universidades. Os resultados indicaram que os participantes com um nível de consciencialização mais elevado e os participantes das áreas das ciências, apresentavam comportamentos menos problemáticos em relação à segurança da informação. No entanto os resultados indicaram que os participantes que usam a Internet de forma mais compulsiva tendem a apresentar comportamentos mais problemáticos em relação à segurança da informação.

Em (Nurbojatmiko et al., 2020) os autores avaliam o nível de consciencialização para a segurança da informação de 73 utilizadores da plataforma *Academic Information System*, utilizada na *Universitas Islam Negeri Syarif Hidayatullah*. Os resultados indicaram que a maioria dos participantes adotam medidas para proteger a confidencialidade dos seus dados e que compreendem a importância de manter a integridade das suas informações, de forma a evitar alterações não autorizadas. O estudo concluiu que os participantes, em geral, demonstram possuir conhecimentos suficientes sobre a importância da segurança da informação e que adotam comportamentos adequados na gestão da segurança da informação quando utilizam a plataforma.

Em (Moletsane et al., 2020) os autores avaliam o nível de consciencialização para a segurança da informação em dispositivos móveis entre 397 estudantes de uma universidade da África do Sul. Os resultados revelaram atitudes positivas em relação à segurança móvel, como a adoção de práticas de utilizar palavras-passe fortes. Os resultados, no entanto, mostraram que essas atitudes são menos evidentes nos participantes que afirmaram possuir mais conhecimentos sobre ameaças à cibersegurança. O estudo concluiu que o conhecimento sobre as ameaças à cibersegurança não parece influenciar as crenças dos participantes sobre as suas vulnerabilidades *online*, nem alterar as suas intenções de adotarem comportamentos mais cautelosos.

Em (Neigel et al., 2020) os autores avaliam, através de um questionário, o impacto

dos fatores humanos na higiene da cibersegurança, que contou com a participação de 173 estudantes provenientes da *Towson University* e da *University of Central Florida*. Os resultados indicaram que os participantes estavam conscientes e ativamente empenhados em vários aspetos da higiene da cibersegurança, como a gestão de palavras-passe e a utilização do email, Internet, redes sociais e dispositivos móveis. Além disso, os participantes demonstraram auto-eficácia informática, ou seja capacidade de utilizar um computador de forma eficaz para realizar uma tarefa, no entanto indicaram pouca confiança na tecnologia. O estudo também revelou que os participantes mais velhos apresentavam atitudes mais fortes em relação à higiene da cibersegurança e que adotavam mais comportamentos de segurança. O estudo concluiu, ainda, que os participantes do sexo feminino aparentam possuir conhecimentos mais elevados, atitudes mais fortes e adotam mais comportamentos de higiene da cibersegurança em comparação com os participantes do sexo masculino.

Em (Oliveira et al., 2023) os autores avaliam, através de um questionário, o nível de consciencialização para a higiene da cibersegurança e ameaças cibernéticas entre 110 estudantes do primeiro ano de licenciaturas em informática da *Bialystok University of Technology*, na Polónia e do Instituto Politécnico de Viana do Castelo, em Portugal. Os resultados indicaram que maioria dos participantes não utiliza a opção de autenticação multi-fator, no entanto reconhecem que a utilização de redes públicas não é segura e que o modo de navegação anónima não oculta o seu endereço de IP. O estudo revela, também, que os participantes portugueses tendem a realizar mais cópias de segurança dos seus ficheiros e a utilizar palavras-passe diferentes em *Websites* distintos, ao contrário da maioria dos participantes polacos, que não adotam essas práticas. O estudo revelou, ainda, que uma proporção maior dos participantes polacos relatou ter sido vítima de um ataque cibernético em comparação com os participantes portugueses. O estudo concluiu que os participantes polacos e portugueses apresentam diferenças nas suas perceções e conhecimentos relativos à cibersegurança, com os polacos a demonstrar mais confiança nos seus conhecimentos.

2.2.2 Avaliação do Nível de Sensibilização para o Cibercrime

Em (Soylu et al., 2021) os autores avaliam, através de um questionário, o nível de consciencialização sobre o cibercrime entre 133 estudantes do *Department of Information Systems* da *Al-Farabi Kazakh National University* no Almaty, Cazaquistão. Os resultados indicaram que os participantes apresentam um nível moderado de consciencialização em relação à cibercriminalidade, demonstrando estarem, em geral, cientes da dimensão dos cibercrimes e das consequências dessas ameaças na integridade e no desenvolvimento social. Os resultados revelaram, ainda, que a maioria dos participante acredita que os funcionários públicos devem receber formação em cibersegurança. O estudo concluiu que existe a necessidade de capacitar os estudantes sobre o tema, recomendando que o ensino sobre a cibercriminalidade seja incluído nos programas curriculares de todos os níveis de ensino.

Em (Awodiran et al., 2023) os autores avaliam, através de um questionário, o nível de consciencialização sobre o cibercrime entre 171 estudantes da *Afe Babalola University*, na Nigéria. Os resultados indicaram que os participantes apresentam um nível baixo de consciencialização para o cibercrime, sendo relativamente mais baixo nos participantes do sexo masculino em comparação com os do sexo feminino.

2.2.3 Simulação de Ataques

Em (Ciupe et al., 2024) os autores realizam, através dos serviços educativos do Office 365, uma simulação de ataques de *phishing* na *Technical University of Cluj-Napoca's*, na Roménia. A simulação de ataques de *phishing* utilizou cinco tipos de ataques: *Credential Harvest*, que visava induzir os utilizadores a clicar num *link* para verificar uma conta ou para aceder a uma plataforma de ensino; *Drive-by-URL*, que consistia no envio de uma notificação de "palavra-passe expirada", incentivando os utilizadores a clicar num botão para renovar a palavra-passe; *Link in the Attachment*, que consistia no envio de um *link* num anexo para um inquérito; *Link to Malware*, que tinha como objetivo levar os utilizadores a clicar num botão para aceder a serviços promocionais ou a clicar num *link* para aceder a um painel de administração para visualizar uma fatura; e *OAuth Consent Grant*, que consistia no envio de um *link* para manter a conta ativa após uma atualização de serviços. Os resultados indicaram que os ataques *Drive-by-URL* e *Oauth consent* registaram o maior número de cliques nos *links* fornecidos, enquanto o ataque *Link to Malware* teve uma adesão menor. No que diz respeito ao reporte de *spam*, os ataques *Credential Harvest* e *Link in the Attachment* apresentaram as taxas mais baixas.

Em (Shukla et al., 2022) os autores avaliam o nível de consciencialização para a cibersegurança numa empresa do setor financeiro através da simulação de um ataque de *phishing* e analisam, através de um questionário, a utilização de redes sociais entre 43 estudantes de um curso universitário de segurança informática. A avaliação na empresa consistiu na simulação de um ataque de *phishing* composta por três fases. Na primeira fase, foi enviado um email com uma falsa promoção para obter mais espaço de armazenamento no Gmail. Na segunda fase, os funcionários receberam formação sobre as práticas de cibersegurança, e, na terceira fase, o ataque de *phishing* foi repetido. Os resultados mostraram uma redução significativa no número de funcionários que abriram o email, clicaram no link ou preencheram os dados no formulário durante a terceira fase, sugerindo que a formação foi eficaz. O questionário aplicado aos estudantes indicou que todos os participantes utilizam várias plataformas de redes sociais, sendo o Facebook e o YouTube as plataformas mais populares.

2.2.4 Outros Trabalhos

Em (Breitinger et al., 2020) os autores investigam as escolhas de segurança que os utilizadores aplicam nos dispositivos móveis. O estudo foi administrado através de um questionário distribuído em várias redes sociais, tendo como público-alvo as gerações

Y (1981-1996) e Z (1997-2012). Os resultados indicaram que os participantes adotam medidas adequadas de bloqueio de ecrã, mas não utilizam VPN ao conectarem-se a redes públicas. O estudo concluiu, ainda, que os participantes tendem a instalar menos produtos de segurança em dispositivos móveis, tornando esses dispositivos relativamente menos seguros em comparação com os computadores.

Em (Salem et al., 2021) os autores avaliam, através de um questionário, o nível de consciencialização para a cibersegurança de 200 estudantes de várias instituições de ensino palestinianas. Os resultados indicaram que os participantes possuem um bom nível de conhecimentos relacionados com a utilização do email e dispositivos móveis. Contudo, apresentaram um nível mais baixo de conhecimentos sobre a gestão de palavras-passe, a utilização de redes sociais e as práticas de proteção contra engenharia social. O estudo também revelou que os participantes mais velhos demonstram um nível maior de consciencialização em comparação com os mais jovens, e que os participantes do sexo masculino aparentam estar mais conscientes do que os do sexo feminino. O estudo revelou, ainda, que a maioria dos participantes afirmou nunca ter frequentado uma formação sobre a segurança da informação, mas expressou o desejo de aprender mais sobre essa área.

Em (Marques, 2021) os autores avaliam, através de um questionário, o nível de consciencialização para a cibersegurança de 164 estudantes do 6º e 9º anos do Colégio Conciliar de Maria Imaculada, em Leiria, Portugal. O questionário de avaliação foi aplicado durante as aulas de Tecnologias de Informação e Comunicação e os resultados indicaram que, em geral, os participantes adotam comportamentos que podem comprometer a sua segurança, bem como a segurança da instituição, familiares e amigos. O projeto implementou, ainda, um questionário de auto-diagnóstico, disponibilizado na plataforma Moodle da instituição, permitindo que os estudantes, de forma autónoma, avaliassem e melhorassem os seus conhecimentos sobre a cibersegurança. O processo de auto-diagnóstico incluiu a apresentação de *feedback* e sugestões de leitura associadas às respostas das perguntas do questionário.

2.3 Sumário

Esta secção apresenta o enquadramento dos estudos analisados em relação aos objetivos do presente trabalho. A maioria dos estudos avaliou o nível de consciencialização sobre cibersegurança e cibercrime entre estudantes do ensino superior. Com o intuito de identificar de que forma este trabalho pode evoluir e melhorar o que já foi desenvolvido, foram os pontos fortes e fracos de cada estudo, com base no tipo de instrumento de avaliação utilizado, se o método de avaliação utilizado recorre a escalas ou se é suficientemente abrangente quando não se baseia numa escala. Além disso, verificou-se, também, se os estudos propõem medidas para promover a cibersegurança e se implementam estratégias de sensibilização.

Trabalho	Pontos Fortes	Pontos Fracos
Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution (Raju et al., 2022)	-Utiliza um questionário como instrumento de avaliação, baseado em atividades na Internet e em conhecimentos gerais da cibersegurança. -Sugere que seja criado um programa para aumentar os conhecimentos sobre cibersegurança.	-Não aplica estratégias de sensibilização.
Cyber Security Awareness, Knowledge and Behavior: A Comparative Study (Zwilling et al., 2022)	-Utiliza um questionário como instrumento de avaliação, focado em conhecimentos, atitudes e comportamentos. -Sugere criar programas de treino para aumentar a sensibilização para a cibersegurança.	-Não aplica estratégias de sensibilização.
Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic (Setiawan et al., 2024)	-Utiliza um questionário como instrumento de avaliação, baseado numa escala que avalia conhecimentos, atitudes e comportamentos em vários tópicos da cibersegurança. -Sugere que os temas da cibersegurança sejam incluídos nas escolas.	-Não aplica estratégias de sensibilização.
Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan (Chen et al., 2021)	-Utilizou um questionário como instrumento de avaliação baseado em várias escalas. -Sugere programas de treino para pontos específicos.	-Não aplica estratégias de sensibilização.

Information Security Awareness of Students on Academic Information System Using Kruger Approach (Nurbojatmiko et al., 2020)	-Utilizou um questionário como instrumento de avaliação, baseado em conhecimentos, atitudes, comportamentos, confidencialidade, integridade e disponibilidade.	-Focou-se apenas num sistema específico. -Não sugere nem aplica programas de treino ou estratégias de sensibilização.
Mobile Information Security Awareness Among Students in Higher Education : An Exploratory Study (Moletsane et al., 2020)	-Baseou-se nos métodos conhecimento, atitude, comportamento para construir um instrumento de avaliação.	-Focou-se apenas em dispositivos móveis. -Não sugere nem aplica programas de treino ou estratégias de sensibilização.
Holistic cyber hygiene education: Accounting for the human factors (Neigel et al., 2020)	-Utilizou um questionário como instrumento de avaliação baseado em várias escalas distintas. -Sugere que os temas da cibersegurança sejam incluídos nas escolas.	-Não aplica estratégias de sensibilização.
Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland (Oliveira et al., 2023)	-Utilizou um questionário para avaliar as boas práticas da cibersegurança e os conhecimentos acerca de ameaças. -Sugere criar programas de treino ou usar a gamificação como uma forma de aprender sobre a cibersegurança.	-Não aplica estratégias de sensibilização.
Identifying the Cybercrime Awareness of Undergraduate and Postgraduate Students: Example of Kazakhstan (Soylu et al., 2021)	-Utilizou um questionário para avaliar os conhecimentos relacionados com o cibercrime. -Sugere várias medidas que educadores, governo e cidadãos em geral podem adotar.	-Não aplica estratégias de sensibilização. -Questionário focado apenas no cibercrime.

Cybercrime Consciousness Among Undergraduate Students (Awodiran et al., 2023)	-Utilizou um questionário para avaliar os conhecimentos relacionados com o cibercrime. -Sugere que sejam feitas mais campanhas para prevenir o cibercrime.	-Não aplica estratégias de sensibilização. -Questionário focado apenas no cibercrime e limitado apenas ao autodiagnóstico.
Reinforcing Cybersecurity Awareness through Simulated Phishing Attacks: Findings From an HEI Case Study (Ciupe et al., 2024)	-Simulação de um ataque de *phishing* como instrumento de avaliação. -Recorreu a vários tipos de mensagens de *phishing* para fazer a avaliação. -Sugere várias medidas que podem ser adotadas na utilização do email.	-Não aplica estratégias de sensibilização.
A Comparative Study of Cyber Security Awareness, Competence and Behavior (Shukla et al., 2022)	-Simulação de um ataque de *phishing* numa empresa e aplicação de um questionário sobre redes sociais em estudantes. -Fez uma simulação, de seguida realizou uma formação e mais tarde repetiu a simulação para comparar os dados.	-Questionário focou-se apenas na quantidade de redes sociais os estudantes utilizam.
A survey on smartphone user's security choices, awareness and education (Breitinger et al., 2020)	-Utilizou um questionário para avaliar as configurações de segurança adotadas nos smartphones. -Recomenda que as configurações padrão sejam mais seguras e que estas sejam mais fáceis de alterar.	-Não aplica estratégias de sensibilização.
Evaluation of Information Security Awareness among Palestinian Learners (Salem et al., 2021)	-Utiliza um questionário como instrumento de avaliação, focado em conhecimentos, atitudes e comportamentos. -Sugere criar campanhas de sensibilização e incluir estes temas nas escolas.	-Não aplica estratégias de sensibilização.

Estratégia Integrada de Avaliação e Consciencialização Cibernética em Contexto Escolar (Marques, 2021)	-Utilizou três questionários, dois para avaliar comportamentos, atitudes baseados em duas escalas e um de auto-diagnóstico. -Planeou e aplicou aulas de sensibilização.	-Estudo aplicado apenas a alunos do 2º ciclo.

Tabela 2.1: *Pontos fortes e fracos dos estudos.*

A maioria dos estudos, como pode verificar na Tabela 2.1, avaliou o nível de consciencialização para a cibersegurança através de questionários, embora alguns estudos tenham optado pela simulação de ataques para efetuar essa avaliação. Contudo, a maior parte dos trabalhos limitou-se a apresentar os resultados obtidos na avaliação e a sugerir medidas que podem ser adotadas, dedicando pouca atenção à implementação de estratégias de sensibilização para a cibersegurança.

Um exemplo que se destacou pela positiva foi o estudo «*A Comparative Study of Cyber Security Awareness, Competence and Behavior*» (Shukla et al., 2022), que utilizou uma abordagem mais abrangente, embora tenha sido focada em funcionários. Primeiro, realizou uma simulação de um ataque de *phishing*, depois realizou uma formação sobre as práticas de cibersegurança, e posteriormente repetiu a simulação. Os resultados mostraram uma redução significativa no número de potenciais vítimas entre a primeira e a segunda simulação, evidenciando a importância e a eficácia das ações de sensibilização para a cibersegurança. Este estudo também realizou uma avaliação numa universidade, no entanto foi apenas um questionário limitado à quantidade de redes sociais utilizadas pelos estudantes.

Outro exemplo que se destacou pela positiva foi o projeto «*Estratégia Integrada de Avaliação e Consciencialização Cibernética em Contexto Escolar*» (Marques, 2021), que avaliou o nível de consciencialização através de questionários baseados em escalas e realizou de aulas de sensibilização. No entanto, este projeto foi implementado em estudantes de 2º e 3º ciclo do ensino básico, e não em estudantes de ensino superior.

Neste sentido, esta dissertação propõe-se a seguir os princípios apresentados nos dois exemplos anteriores, designadamente avaliar o nível de consciencialização e implementar uma estratégia de sensibilização. Colmatando, assim, a lacuna identificada na maioria dos estudos analisados e contribuindo para uma abordagem mais completa e eficaz na promoção da cibersegurança.

O estudo apresentado nesta dissertação é direcionado a estudantes do ensino superior que não pertencem às áreas de CTEAM, que, em geral, nos seus planos curriculares não abordam amplamente as tecnologias da informação. A falta dessa abordagem torna-os mais vulneráveis a riscos e ameaças do mundo digital, uma vez que a cibersegurança

é uma competência cada vez mais essencial, independentemente da área de formação. Realizar um estudo focado exclusivamente em estudantes de áreas não CTEAM representa uma abordagem inovadora e necessária, contribuindo para os tornar mais conscientes e preparados para os desafios do mundo digital, e, acima de tudo, mais aptos para adotar comportamentos mais seguros na utilização das tecnologias, tanto em contextos académicos como profissionais.

3
Desenvolvimento

O presente capítulo descreve o desenvolvimento das atividades realizadas para cumprir os objetivos delineados para este trabalho. Ao longo do capítulo, apresenta-se a metodologia adotada e detalha-se o processo de desenvolvimento de duas das três etapas que a compõem.

A metodologia seguida neste trabalho foi estruturada em três etapas principais (Medir, Avaliar e Intervir) com o intuito de garantir o cumprimento dos objetivos definidos (Secção 3.1). A etapa Medir teve como finalidade desenvolver um questionário, baseado na escala HAIS-Q (Secção 3.3), para medir o nível de consciencialização para a cibersegurança (Secção 3.2). A etapa Intervir implementou uma estratégia de sensibilização para a cibersegurança, através da realização de uma aula aberta, concebida com base nos tópicos avaliados pela escala HAIS-Q, e a criação de um vídeo explicativo com os mesmos conteúdos, para divulgação *online* (Secção 3.4).

3.1 Metodologia de Trabalho

A metodologia adotada no desenvolvimento deste trabalho seguiu uma estrutura composta por três etapas principais: Medir, Avaliar e Intervir. Na primeira etapa foi desenvolvido um instrumento para medir o nível de consciencialização para a cibersegurança. Na segunda foram analisados os dados recolhidos com o instrumento de avaliação. E, na última foi elaborada e implementada uma estratégia de sensibilização para a cibersegurança.

Estas etapas tiveram como base uma escala que serviu de apoio, tanto na construção do instrumento de medição, como no planeamento da estratégia de sensibilização.

A Figura 3.1 apresenta a metodologia geral adotada no desenvolvimento deste trabalho, que consistiu, de forma resumida, em medir o nível de consciencialização para a cibersegurança através de uma escala, analisar os dados obtidos e, com base nas áreas abordadas pela escala, planear e aplicar uma estratégia de sensibilização.

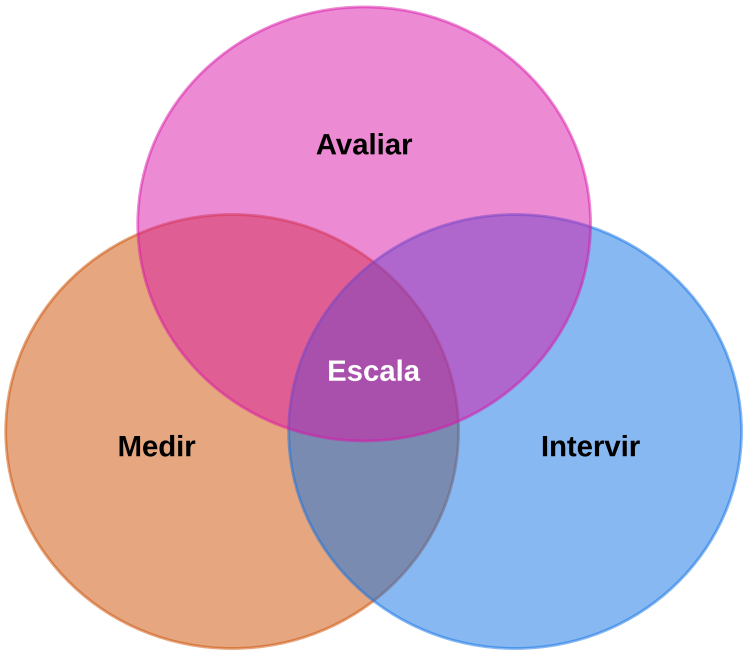


Figura 3.1: *Metodologia geral do trabalho.*

Esta abordagem permitiu não apenas avaliar o nível de consciencialização dos participantes, mas também promover a adoção das boas práticas da cibersegurança. Ao recorrer a uma escala validada, assegurou-se a fundamentação científica necessária para o desenvolvimento de estratégias consistentes e potencialmente eficazes para promover comportamentos mais seguros no meio digital.

3.1.1 Etapa 1 - Medir

Esta etapa teve como objetivo construir um questionário para servir de instrumento de medição do nível de consciencialização para a cibersegurança dos estudantes. Nesta etapa, foi selecionada uma escala para servir de base para o questionário.

A Figura 3.2 apresenta o processo metodológico seguido para construir e aplicar o questionário que serviu de instrumento de medição do nível de consciencialização para a cibersegurança dos estudantes de licenciaturas que não pertencem às áreas CTEAM.

Este processo metodológico teve sete fases que permitiram assegurar a precisão e a relevância do questionário, de forma a garantir que se adequava às características e necessidades específicas do público-alvo.

Na Fase 1 - ***Seleção da Escala*** - foram identificadas e analisadas escalas potencialmente adequadas ao contexto deste trabalho, com o intuito de selecionar a mais apropriada para a construção do questionário.

Na Fase 2 - ***Pedido de Autorização*** - procedeu-se ao envio de um email, aos autores da

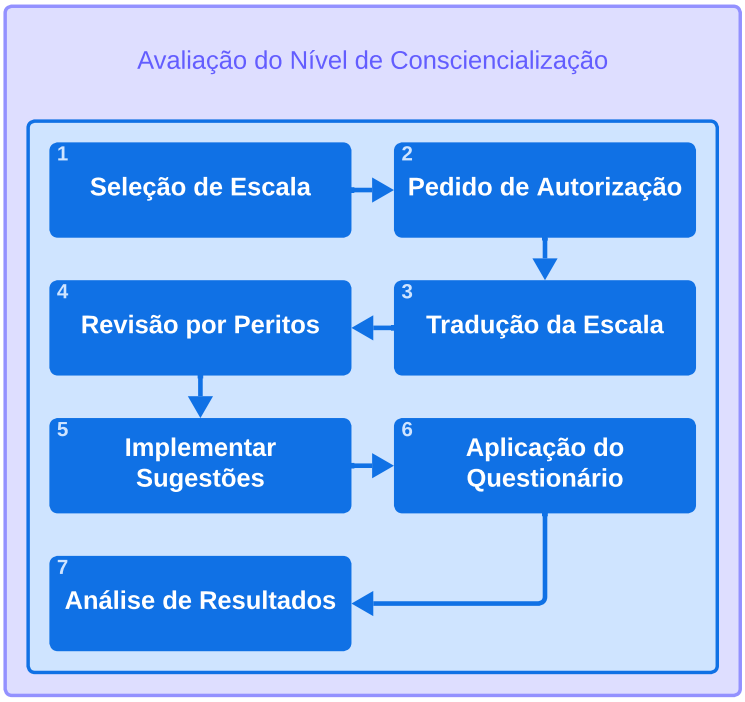


Figura 3.2: *Metodologia adotada para construir o questionário de avaliação.*

escala selecionada, a solicitar permissão para a sua utilização e adaptação ao contexto específico deste trabalho.

Na Fase 3 - ***Tradução da Escala*** - a escala foi traduzida do seu idioma original, em inglês, para português europeu.

Na Fase 4 - ***Revisão por Peritos*** - os itens da escala foram enviados a especialistas da área da cibersegurança, com o objetivo de recolher sugestões quanto à sua adequação em relação aos objetivos do estudo.

Na Fase 5 - ***Implementação de Sugestões*** - foram analisadas as sugestões fornecidas pelos especialistas e implementadas as que contribuíam para a melhoria do questionário.

Na Fase 6 - ***Aplicação do Questionário*** - o questionário foi divulgado junto do público-alvo pretendido.

Por fim, na Fase 7 - ***Análise de Resultados*** - foram definidas as questões de investigação a serem respondidas com os dados recolhidos.

Na Secção 3.2, cada uma destas fases encontra-se descrita em detalhe, incluindo as decisões tomadas durante o seu processo de desenvolvimento.

3.1.2 Etapa 2 - Avaliar

Esta etapa teve como objetivo analisar as respostas recolhidas com o questionário para avaliar o nível de consciencialização para a cibersegurança dos participantes, bem como identificar as áreas que necessitam de estratégias de sensibilização mais eficazes.

A Figura 3.3 apresenta o processo metodológico seguido para analisar as respostas recolhidas com o questionário e avaliar o nível de consciencialização para a cibersegurança dos estudantes.

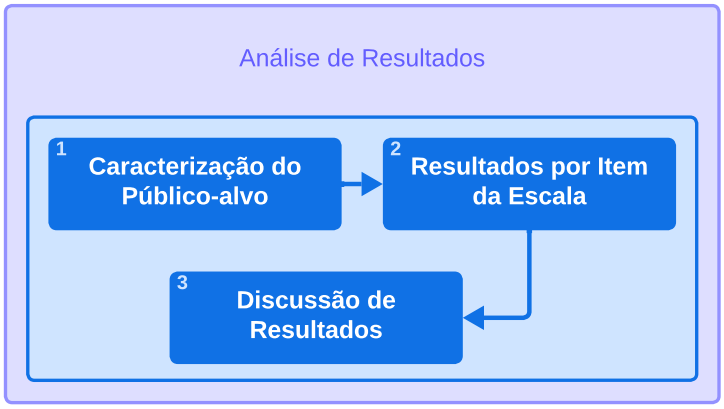


Figura 3.3: *Metodologia adotada para analisar os resultados do questionário de avaliação.*

Este processo metodológico teve três fases que permitiram assegurar precisão da análise dos resultados, de forma a permitir identificar os pontos fortes e fracos nas várias áreas avaliadas pela escala.

Na Fase 1 - ***Caracterização do Público-alvo*** - foram a analisadas as respostas às questões de carácter demográfico, com o objetivo de identificar a distribuição das respostas pelos diferentes grupos de participantes.

Na Fase 2 - ***Resultados por Item da Escala*** - foi descrita a distribuição das respostas para cada item da escala, com base nos dados estatísticos fornecidos pela plataforma de divulgação do questionário.

Por fim, na Fase 3 - ***Discussão de Resultados*** - foi utilizado um programa de análise estatística para estudar os dados recolhidos e responder às questões de investigação previamente definidas, com o objetivo de interpretar e discutir os principais achados do estudo e de identificar as áreas que requerem intervenções de sensibilização mais eficazes.

No Capítulo 4, apresentam-se os resultados da análise dos dados recolhidos com o questionário de avaliação.

3.1.3 Etapa 3 - Intervir

Esta etapa teve como objetivo criar e implementar uma estratégia de sensibilização para as boas práticas da cibersegurança, especificamente uma aula aberta.
A estratégia foi desenvolvida com base nas áreas abordadas pela escala, com o objetivo de alertar os participantes para os comportamentos de riscos existentes em cada uma das áreas e divulgar os comportamentos preventivos adequados que devem adotar.

A Figura 3.4 apresenta o processo metodológico adotado para criar e implementar a estratégia de sensibilização para a cibersegurança.

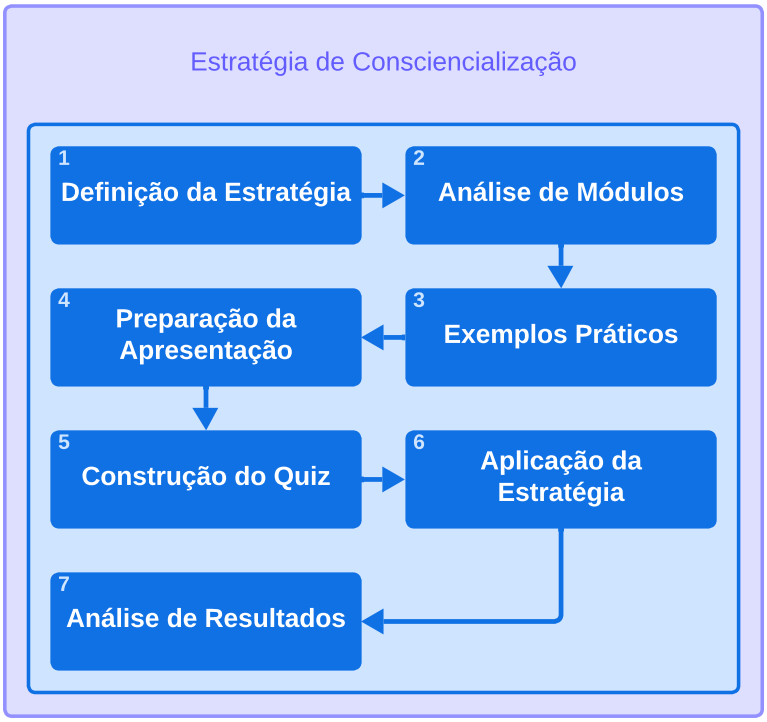


Figura 3.4: *Metodologia utilizada na estratégia de sensibilização.*

Este processo metodológico teve sete fases que garantiram que a estratégia fosse abrangente, integrasse abordagens teóricas e práticas, e que utilizasse um método para avaliar a retenção dos conhecimentos transmitidos aos participantes.

Na Fase 1 - ***Definição da Estratégia*** - foi definida a estrutura de implementação da estratégia, os seus objetivos e o seu público-alvo.

Na Fase 2 - ***Análise de Módulos*** - foram analisadas as áreas abordadas pela escala, com o objetivo de determinar os principais problemas existentes, identificar as potenciais ameaças que podem ocorrer desses problemas e sugerir possíveis medidas preventivas.

Na Fase 3 - ***Exemplos Práticos*** - foram selecionados para cada tópico exemplos práticos, como notícias e vídeos demonstrativos, com o objetivo de ilustrar os riscos existentes e reforçar a importância das boas práticas de cibersegurança.

Na Fase 4 - ***Preparação da Apresentação*** - foram desenvolvidos os materiais necessários para a implementação da estratégia.

Na Fase 5 - ***Construção do Quiz*** - foi desenvolvido um Quiz para avaliar a compreensão e a retenção dos conhecimentos transmitidos com a aplicação da estratégia.

Na Fase 6 - ***Aplicação da Estratégia*** - foi aplicada a estratégia de sensibilização junto do público-alvo pretendido.

Por fim, na Fase 7 - ***Análise de Resultados*** - foi apresentada uma reflexão sobre a aplicação da estratégia de sensibilização e foram analisados os resultados obtidos com a aplicação do Quiz.

No Secção 3.4, cada uma destas fases é apresentada e descrita em detalhe, incluindo as decisões tomadas ao longo do seu desenvolvimento.

3.2 Avaliação do Nível de Consciencialização

Nesta secção, descreve-se o desenvolvimento da etapa **Medir**, que teve como objetivo construir um questionário destinado a avaliar o nível de consciencialização para a cibersegurança dos estudantes das licenciaturas de áreas não CTEAM, lecionadas na ESTG. Para tal, esse processo foi dividido em sete fases, que serão detalhadas ao longo desta secção, juntamente com as respetivas decisões tomadas.

3.2.1 Fase 1 - Seleção de Escala

A primeira fase desta etapa consistiu na seleção de uma escala para servir de base para o questionário. Para isso, realizou-se uma análise das escalas que mais se destacaram durante a revisão da literatura apresentada no Capítulo 2. Dessa revisão destacaram-se as escalas *Computer self-efficacy* (CSE), *Generalized Problematic Internet Use Scale* 2 (GPIUS2) e HAIS-Q. Adicionalmente, foi realizada uma pesquisa complementar com o intuito de identificar outras escalas relevantes, o que resultou na inclusão da escala Cybersecurity Attitudes Scale (CAS).

Análise de Escalas

A escala **CSE** (Thatcher et al., 2008) avalia a capacidade de um indivíduo conseguir utilizar as tecnologias de forma independente e com sucesso no desempenho das suas funções. A escala é composta por dez itens avaliados numa escala de *Likert*, e o resultado obtido indica o nível de auto-eficácia informática dos indivíduos.

A escala **GPIUS2** (Caplan, 2010) mede a utilização problemática da Internet, abordando os aspetos emocionais, cognitivos e comportamentais, com o objetivo de identificar possíveis transtornos. A escala é composta por 15 itens subdivididos em cinco

áreas: Preferência por Interações Online; Regulação do Humor; Preocupação cognitiva; Resultados negativos; e Utilização Compulsiva da Internet. Cada área inclui cinco itens, avaliados numa escala de *Likert*.

A escala **HAIS-Q** (Parsons et al., 2017) avalia, numa escala de *Likert*, os níveis de conhecimentos, atitudes e comportamentos dos indivíduos em relação às práticas de cibersegurança. A escala é composta por 63 itens, distribuídos por sete áreas principais, cada uma subdividida em três subáreas específicas. Cada subárea inclui três itens que avaliam, respetivamente, os conhecimentos, as atitudes e os comportamentos dos inquiridos.

Por fim, a escala **CAS** (Howard, 2018) avalia as atitudes relacionadas à adesão de políticas de cibersegurança e a perceção da vulnerabilidade a ciberataques. A escala é composta por dez itens, respondidos numa escala de *Likert*.

As escalas analisadas anteriormente são eficientes e adequadas aos seus contextos. No entanto, por se tratar de um estudo focado em estudantes universitários, com o objetivo de avaliar as práticas de cibersegurança que adotam, a escala HAIS-Q foi considerada a mais abrangente e adequada.

A Secção 3.3 apresenta uma descrição detalhada do processo de desenvolvimento da escala, da sua estrutura e do seu funcionamento.

3.2.2 Fase 2 - Pedido de Autorização

A segunda fase desta etapa consistiu na solicitação de autorização aos autores da escala para a sua utilização. A versão da escala utilizada para a construção do questionário foi a apresentada no artigo «*The Human Aspects of Information Security Questionnaire* (*HAIS-Q*): *Two further validation studies*» (Parsons et al., 2017), desenvolvido por Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac e Tara Zwaans.
Para possibilitar a sua utilização no âmbito deste trabalho, foi redigido um email a pedir autorização para a utilização e tradução da escala. Embora o artigo menciona-se seis autores, apenas o endereço de email da autora Kathryn Parsons estava disponível para correspondência. O pedido foi enviado no dia 14-11-2024 e encontra-se incluído no Apêndice A.
No mesmo dia, foi recebida uma resposta por parte de Agata McCormac, também autora da escala, a conceder autorização para a utilização e tradução da escala. O email de resposta está disponibilizado no Apêndice B.

3.2.3 Fase 3 - Tradução da Escala

A terceira fase desta etapa consistiu na tradução e adaptação da escala de inglês para português europeu. Este processo foi iniciado após se ter recebido autorização para

utilizar a escala no âmbito deste trabalho, por parte dos autores.
Inicialmente, realizou-se uma pesquisa por trabalhos que já tivessem efetuado essa tradução, mas não se obteve resultados. Assim, com o auxílio da plataforma DeepL[1] realizou-se a tradução dos itens da escala para português europeu.
No Apêndice C estão disponibilizados os itens originais da escala, em inglês, e no Apêndice D está a sua versão traduzida para português europeu.

3.2.4 Fase 4 - Revisão por Peritos

A quarta fase desta etapa consistia no envio das questões da escala a especialistas em cibersegurança, com o objetivo de recolher sugestões quanto à sua adequação em relação aos objetivos deste trabalho.
No entanto, durante a análise da escala selecionada, foram identificados diversos estudos que utilizaram à escala HAIS-Q para avaliar o nível de consciencialização para a cibersegurança em diversos setores. Além dos estudos realizados pelos próprios autores da escala (Parsons et al., 2013; Parsons et al., 2014; Parsons et al., 2017), encontraram-se estudos na área da educação, envolvendo estudantes (Neigel et al., 2020; Salem et al., 2021; Setiawan et al., 2024) e funcionários (Effendy et al., 2022). Foram também identificados estudos aplicados a funcionários de empresas (Cindana et al., 2018; Zulfia et al., 2019), na área da saúde, com foco em enfermeiros (Magdalinou et al., 2022), e em uma organização governamental, envolvendo funcionários públicos de diversos departamentos (Susanto et al., 2024).

Considerando a diversidade de estudos que já utilizaram a escala, considerou-se que a escala já foi amplamente validada, pelo que se optou por não pedir a especialistas a sua revisão.

3.2.5 Fase 5 - Implementação de Sugestões

A quinta fase desta etapa consistiria na análise e implementação das sugestões fornecidas pelos especialistas. No entanto, conforme mencionado na fase anterior, foram identificados diversos estudos que recorreram à escala pelo que se optou por não realizar a revisão por peritos, impossibilitando, assim, a execução desta fase.

3.2.6 Fase 6 - Aplicação do Questionário

A sexta fase desta etapa corresponde à divulgação do questionário ao público-alvo pretendido. Para a sua divulgação, foi redigido um email, que se encontra disponível no Apêndice E, dirigido aos coordenadores das licenciaturas, solicitando que partilhassem o questionário com os estudantes.
O questionário foi disponibilizado para recolha de respostas no período compreendido entre 28-02-2025 e 31-03-2025. No entanto, devido à falta de respostas o período de recolha de respostas foi aumentado até 30-04-2025.

[1] DeepL: `https://www.deepl.com/`

A plataforma utilizada para construir e divulgar o questionário foi o Google Forms[2]. No entanto, antes dessa decisão, foram analisadas e testadas outras plataformas, nomeadamente o LimeSurvey[3] e Microsoft Forms[4]. Contudo, algumas limitações observadas durante a sua utilização levaram à sua exclusão. No caso do LimeSurvey, a versão gratuita apresentava um limite de respostas bastante inferior ao número esperado, o que inviabilizou a sua utilização. No caso do Microsoft Forms, apesar de não impor restrições quanto ao número de respostas, a publicação do questionário não foi possível devido à presença de questões relacionadas com palavras-passe. Assim, optou-se pela utilização do Google Forms, que não apresentou nenhuma dessas limitações durante os testes realizados.

O questionário aplicado, disponível no Apêndice F, foi estruturado em nove secções. A primeira secção apresentou uma descrição dos objetivos e funcionamento do questionário e inclui uma questão destinada a obter o consentimento informado dos inquiridos. A segunda secção consistiu num conjunto de perguntas demográficas, com o objetivo de caracterizar o público-alvo. As secções seguintes corresponderam, individualmente, às áreas avaliadas pelo HAIS-Q.

O questionário foi disponibilizado a estudantes, do Politécnico de Leiria, pertencentes a licenciaturas de áreas não CTEAM, lecionadas na ESTG. Especificamente, foi disponibilizado para as licenciaturas em Administração Pública (Regime Diurno), Contabilidade e Finanças (Regime Diurno), Gestão (Regime Diurno e Pós-laboral), Marketing (Regime Diurno) e Solicitadoria (Regime Diurno e Pós-laboral). Para identificar estas licenciaturas consultou-se o *website*[5] oficial da instituição.

3.2.7 Fase 7 - Análise de Resultados

A sétima e última fase desta etapa consistiu na definição das questões de investigação que pretende responder com a análise das respostas recolhidas. As questões de investigação estabelecidas encontram-se apresentadas na Tabela 3.1.

Questões que o estudo pretende responder	
1	Qual o curso que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?
2	Qual o ano curricular que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?
3	Existem indícios de que estudantes mais velhos adotam melhores práticas de cibersegurança?
4	Existe algum indicador que relacione o sexo dos estudantes com a adoção de melhores práticas de cibersegurança?

[2] Google Forms `https://docs.google.com/forms`
[3] LimeSurvey: `https://www.limesurvey.org/`
[4] Microsoft Forms: `https://forms.office.com/`
[5] *Website* do Politécnico de Leiria: `www.ipleiria.pt`

5	Estudantes que não ingressaram no ensino superior pelo CNAES demonstram melhores práticas de cibersegurança?
6	O percurso académico do ensino secundário influencia as práticas de cibersegurança adotadas pelos estudantes?
7	Qual a área que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?
8	Qual a dimensão (conhecimento, atitude, e comportamento) em que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?
9	Quais são as melhores e as piores práticas adotadas pelos estudantes em cada uma das áreas avaliadas?
10	Os estudantes de cursos não pertencentes às áreas CTEAM demonstram um bom nível de consciencialização para a cibersegurança?

Tabela 3.1: *Questões de investigação.*

As questões de investigação definidas tinham como objetivo analisar as diferenças nas respostas entre os diferentes grupos de participantes (questões 1 a 6), bem como entre as diversas áreas, subáreas ou dimensões avaliadas pela escala (questões 7 a 10).

Os resultados obtidos e as respostas às questões de investigação encontram-se detalhados no Capítulo 4.

3.3 Escala HAIS-Q

A escala HAIS-Q foi a selecionada para compor o questionário destinado a avaliar o nível de consciencialização para a cibersegurança. Esta escala é descrita como um método eficaz para medir o nível de consciencialização em segurança da informação, tendo sido amplamente validada e continuamente aprimorada ao longo do tempo.

A primeira versão do HAIS-Q foi apresentada em 2013, no artigo «*The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q).*» (Parsons et al., 2013). No artigo, os autores destacam que a escala foi desenvolvida como uma ferramenta para avaliar as ameaças à segurança da informação resultantes dos comportamentos dos colaboradores nas organizações. A criação da escala baseou-se no modelo *Knowledge-Attitude-Behavior* (KAB), adaptado ao contexto da segurança da informação organizacional. O seu objetivo consistia em medir o conhecimento sobre políticas de segurança, as atitudes em relação a essas políticas e os comportamentos adotados na utilização de computadores no local de trabalho.

Em 2014 os, autores do HAIS-Q apresentaram um estudo no artigo «*Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*» (Parsons et al., 2014), com o objetivo de testar e validar o questionário desenvolvido. O estudo foi dividido em três fases. Na primeira fase, o questionário foi revisto e res-

pondido por um especialista de desenvolvimento de questionários, que avaliou a clareza das instruções e a compreensão dos termos. Ainda na mesma fase, foi solicitado a um especialista em segurança da informação que verbaliza-se os seus pensamentos enquanto respondia às perguntas, para analisar a sua compreensão dos itens, a sua confiança nas respostas e as suas reações emocionais, com o objetivo de identificar os pontos mais confusos. Na segunda fase, o questionário foi aplicado a 120 trabalhadores australianos. Como resultado, dessa fase, 10 itens do HAIS-Q foram alterados por serem considerados demasiado complicados. Na terceira e última fase, após as alterações, o questionário voltou a ser aplicado, neste caso a 500 trabalhadores australianos de diferentes setores.

Em 2017, foi apresentada a versão mais recente do HAIS-Q no artigo «*The Human Aspects of Information Security Questionnaire* (*HAIS-Q*)*: Two further validation studies*» (Parsons et al., 2017), que apresentou mais dois estudos para validar a escala. O primeiro estudo envolveu 112 estudantes universitários que inicialmente completaram um estudo sobre *phishing* e de seguida responderam ao HAIS-Q. O segundo estudo foi a aplicação do HAIS-Q a 531 trabalhadores australianos. À data de publicação do artigo, os autores mencionam que o HAIS-Q já foi respondido por 1631 pessoas, incluindo trabalhadores de diversos setores, estudantes universitários e especialistas em segurança da informação. O artigo conclui, ainda, que com base nos resultados de todos os estudos que foram efetuados, que o HAIS-Q é uma ferramenta eficaz para identificar falhas na sensibilização para a segurança da informação e para avaliar a eficácia de programas de treino antes e depois da sua implementação.

Em termos de estrutura o HAIS-Q é composto por 63 itens que avaliam sete áreas principais, cada uma subdividida em três subáreas específicas. No total, são analisadas 21 áreas de interesse, cada uma avaliada por meio de uma questão que visa avaliar o conhecimento, a atitude e o comportamento do inquirido (Parsons et al., 2013; Parsons et al., 2014; Parsons et al., 2017).

Na primeira versão do HAIS-Q (Parsons et al., 2013; Parsons et al., 2014), as áreas e subáreas avaliadas eram as seguintes:

- **Gestão de palavras-passe** - Bloqueio de postos de trabalho; Partilhar palavras-passe; e Escolher uma boa palavra-passe.
- **Utilização de email** - Reencaminhamento de emails; Abrir anexos; e Nível de responsabilidade do departamento de TI.
- **Utilização da Internet** - Instalar software não autorizado; Aceder a *websites* duvidosos; e Utilização inadequada da Internet.
- **Utilização de redes sociais** - Tempo de trabalho despendido nas redes sociais; Consequências das redes sociais; e Publicar informações sobre o trabalho nas redes sociais.
- **Comunicação de incidentes** - Comunicar indivíduos suspeitos; Comunicar o mau comportamento de colegas; e Comunicar todos os incidentes de segurança.

- **Computação móvel** - Proteger fisicamente os dispositivos eletrónicos pessoais; Envio de informações sensíveis através de redes móveis; e Verificar emails do trabalho através de uma rede gratuita.
- **Tratamento de informações** - Eliminação de documentos sensíveis; Inserção de DVDs / dispositivos USB; e Deixar material sensível sem proteção.

Ao longo do processo de desenvolvimento e validação da escala, tanto as áreas quanto as subáreas avaliadas foram sendo ajustadas, para tornar o HAIS-Q um instrumento mais eficaz para medir o nível de consciencialização para a cibersegurança.

Na Tabela 3.2 encontram-se representadas as áreas e suas respetivas subáreas avaliadas, atualmente, pelo HAIS-Q. Comparativamente, é verifica-se que a maior parte das áreas se manteve igual, exceto a área "Computação móvel" que passou a designar-se "Dispositivos móveis". Nas subáreas, aconteceu o oposto, a maior parte sofreu alterações tornando-as, assim, mais precisas e alinhadas com a atualidade.

Área	Subárea
Gestão de palavras-passe	Utilizar a mesma palavra-passe Partilhar palavras-passe Utilizar uma palavra-passe forte
Utilização do email	Clicar em links de emails enviados por remetentes conhecidos Clicar em links de emails enviados por remetentes desconhecidos Abrir anexos de emails enviados por remetentes desconhecidos
Utilização da Internet	Transferir ficheiros Aceder a websites duvidosos Introduzir informações online
Utilização de redes sociais	Definições de privacidade das redes sociais Considerar consequências Publicar sobre o trabalho
Dispositivos móveis	Proteger fisicamente dispositivos móveis Enviar informações sensíveis por Wi-Fi Espionagem visual
Tratamento da informação	Eliminação de impressos sensíveis Inserir suportes amovíveis Deixar material sensível
Comunicação de incidentes	Comunicar comportamentos suspeitos Ignorar comportamentos de segurança inadequados de colegas Comunicar todos os incidentes

Tabela 3.2: *Áreas e subáreas avaliadas pelo HAIS-Q.*

Em termos de funcionamento, cada subárea do HAIS-Q, conforme mencionado anteriormente, inclui três questões destinadas a avaliar o conhecimento, a atitude e comportamento do inquirido. A questão de **conhecimento** avalia o nível de compreensão do inquirido sobre o tópico em análise. A questão de **atitude** avalia a postura do inquirido em relação ao tópico em análise. E, a questão de **comportamento** avalia as práticas que o inquirido aplica em relação ao tópico em análise. Cada questão deve ser respondida utilizando uma escala *Likert* de 5 pontos: (1) Discordo totalmente, (2) Discordo, (3) Não concordo nem discordo, (4) Concordo, (5) Concordo totalmente.

Exemplificado o seu funcionamento, na subárea "**Utilizar uma palavra-passe forte**", pertencente área de "**Gestão de palavras-passe**":

- A afirmação "***É necessária uma combinação de letras, números e símbolos para as palavras-passe de trabalho.***" corresponde a uma questão de conhecimento, que avalia o nível de compreensão do inquirido sobre a criação de palavras-passe seguras.
- A afirmação "***É seguro ter uma palavra-passe de trabalho apenas com letras.***" corresponde a uma questão de atitude, que investiga a postura do inquirido em relação à utilização de palavras-passe.
- A afirmação "***Utilizo uma combinação de letras, números e símbolos nas minhas palavras-passe de trabalho.***" corresponde a uma questão de comportamento, que avalia as práticas relacionadas à utilização de palavras-passe que o inquirido adota.

3.4 Estratégia de Sensibilização

Nesta secção, descreve-se o desenvolvimento da etapa **Intervir**, que tem como objetivo desenvolver e implementar uma estratégia de sensibilização para a cibersegurança, tendo como público-alvo os estudantes de licenciaturas de áreas não CTEAM lecionadas na ESTG. Para tal, esse processo foi dividido em sete fases, que serão detalhadas ao longo desta secção, juntamente com as respetivas decisões tomadas.

3.4.1 Fase 1 - Definição da Estratégia

A primeira fase desta etapa consistiu na definição do tipo de estratégia a aplicar, bem como os seus objetivos e público-alvo. A estratégia de sensibilização foi implementada através de uma aula aberta dirigida a estudantes de licenciaturas não pertencentes às áreas CTEAM, lecionadas na ESTG. Adicionalmente, foi criado um vídeo explicativo com os mesmos conteúdos da aula, destinado à divulgação *online*.

Esta estratégia teve como objetivos alertar para os riscos decorrentes da falta de adoção de mecanismos de proteção, divulgar medidas que podem ser adotadas para prevenir esses riscos e desenvolver a capacidade para identificar situações de risco.

A estratégia, tal como o questionário desenvolvido na Secção 3.2, baseou-se na escala HAIS-Q. No entanto, na estratégia, apenas as áreas contempladas pela escala foram consideradas, com o objetivo de identificar, em cada uma delas, os problemas existentes, as possíveis ameaças decorrentes desses problemas e as medidas de prevenção recomendadas.

3.4.2 Fase 2 - Análise de Módulos

A segunda fase desta etapa consistiu na analise das áreas abordadas pela escala HAIS-Q, com o objetivo de identificar os principais problemas existentes em cada área. A partir desses problemas, foram identificadas algumas ameaças que podem surgir e foram listadas algumas medidas que os utilizadores podem adotar para as prevenir.

A Tabela 3.3 apresenta, de forma resumida os problemas identificados, as ameaças associadas a esses problemas e as medidas de prevenção recomendas. No Apêndice G cada problema, ameaça e medida encontra-se descrito de forma detalhada.

Problemas	**Ameaças**	**Medidas**
Gestão de Palavras-passe		
Utilizar a mesma palavra-passe em vários serviços. Utilizar palavras-passe fracas ou previsíveis. Partilhar palavras-passe.	Roubos de identidade. Ataques de força-bruta. Acessos não autorizados.	Utilizar palavras-passe fortes. Não partilhar palavras-passe. Utilizar uma palavra-passe diferente para cada serviço. Alterar frequentemente as palavras-passe. Ativar autenticação multi-fator. Utilizar gestores de palavras-passe.
Utilização do Email		
Clicar em *links* ou abrir anexos enviados por remetentes desconhecidos.	Roubo de credenciais ou dados pessoais. Instalação de *malware* nos dispositivos.	Desconfiar de emails de remetentes desconhecidos. Verificar a autenticidade do remetente. Evitar clicar em *links* ou abrir anexos de remetentes desconhecidos. Evitar expor o endereço de email publicamente. Marcar emails suspeitos como *spam*. Ficar atento a erros de ortografia e gramática.

Utilização da Internet		
Transferir qualquer tipo de ficheiros ou *software*. Aceder a *websites* duvidosos. Inserir de informações *online*.	Instalação de *malware*. Roubo de identidade.	Navegar em *websites* seguros. Não transferir ficheiros ou *software* de fontes desconhecidas. Manter antivírus e anti-*malware* atualizados.
Utilização de Redes Sociais		
Não verificar as definições de privacidade. Publicar sobre tudo sem considerar as consequências.	Engenharia social. Riscos à segurança pessoal. Impacto na reputação e oportunidades profissionais.	Ajustar as definições de privacidade. Evitar partilhar informações sensíveis. Não aceitar pedidos de amizade de desconhecidos. Rever publicações antigas. Denunciar e bloquear utilizadores abusivos.
Dispositivos Móveis		
Deixar dispositivos sem vigilância em locais públicos. Utilizar dispositivos em locais públicos. Utilizar redes públicas.	Interceção de comunicações. Espionagem visual. Roubo de dispositivos. Acessos não autorizados.	Evitar utilizar redes públicas. Utilizar uma VPN ao conectar-se a redes públicas. Evitar que pessoas próximas visualizem informações no ecrã. Bloquear o ecrã ao deixar o dispositivo sem supervisão. Evitar abrir documentos confidenciais em locais visíveis.
Tratamento de Informações		
Não eliminar corretamente materiais sensíveis. Deixar materiais sensíveis expostos e sem vigilância. Inserir dispositivos USB desconhecidos.	Instalação de *malware*. Exposição de informações.	Evitar utilizar dispositivos USB desconhecidos. Armazenar documentos sensíveis em locais seguros. Destruir adequadamente documentos confidenciais.
Comunicação de Incidentes		
Não reportar incidentes de segurança. Desvalorizar as práticas de segurança.	Propagação de ataques. Negligência nas práticas de segurança.	Adotar medidas de segurança.

Tabela 3.3: *Problemas, ameaças e possíveis medidas para cada módulo do HAIS-Q.*

3.4.3 Fase 3 - Exemplos Práticos

A terceira fase desta etapa consistiu na recolha de exemplos práticos para cada módulo da estratégia. Os exemplos apresentados, para cada módulo, incluíram notícias, demonstrações, divulgação de *links* úteis e apresentação de vídeos sensibilizadores, desenvolvidos pelo Centro Nacional de Cibersegurança (CNCS), no âmbito da campanha #LerAntesClicarDepois[6].

A Tabela 3.4 apresenta o tipo de exemplo prático selecionado para cada módulo. No Apêndice G cada exemplo prático selecionado encontra-se descrito de forma detalhada.

Módulo	Exemplos Práticos
Gestão de Palavras-passe	Uma notícia. *Links* úteis.
Utilização do Email	Uma notícia. Comparação entre um email de *phishing* e um email legítimo. Vídeo de uma campanha do CNCS.
Utilização da Internet	Vídeo demostrativo de interceção de dados ao fazer autenticação num *website* inseguro.
Utilização de Redes Sociais	Três notícias. Vídeo de uma campanha do CNCS.
Dispositivos Móveis	Duas notícias. Dois vídeos de uma campanha do CNCS.
Tratamento de Informações	Duas notícias. Vídeo de uma campanha do CNCS.
Comunicação de Incidentes	Vídeo de uma campanha do CNCS.

Tabela 3.4: *Exemplos práticos selecionados para cada módulo da estratégia.*

3.4.4 Fase 4 - Preparação da Apresentação

A quarta fase desta etapa consistiu na criação dos materiais utilizados para implementar as aulas abertas e o vídeo explicativo. A apresentação foi elaborada com base num dos *templates* disponibilizados pela plataforma Slidesgo[7] e editada no Google Slides. O vídeo foi produzido com base na apresentação elaborada.

[6] Campanha #LerAntesClicarDepois desenvolvida pelo CNCS: `https://www.cncs.gov.pt/pt/campanha-lerantesclicardepois/`

[7] Slidesgo: `https://slidesgo.com/`

A estrutura da apresentação foi adaptada de acordo com o tempo disponível para a realização da aula aberta. Assim, foram preparadas duas versões: uma para a sessão de 45 minutos, disponível no Apêndice J, e outra para a sessão de 90 minutos, disponível no Apêndice K.
Ambas as sessões seguiram uma estrutura geral comum, composta pelos seguintes momentos:

1. Apresentação de alguns conceitos, como cibersegurança, engenharia social, *deepfake*, *malware* e *phishing* (definições disponíveis no Apêndice I).
2. Enquadramento da apresentação, indicando a escala utilizada e os objetivos do estudo.
3. Apresentação dos módulos.
4. Discussão final sobre o tema.

A versão em vídeo da apresentação manteve a estrutura-base mencionada, embora com algumas adaptações.

A Tabela 3.5 apresenta, de forma comparativa, os conteúdos incluídos em cada uma das versões da estratégia de sensibilização: as sessões de 45 ou 90 minutos e a versão em vídeo.

Conteúdo	**Sessão 45 min.**	**Sessão 90 min.**	**Vídeo**
Conceitos gerais	✓	✓	✓
Enquadramento	✓	✓	
Gestão de Palavras-passe			
Problemas, ameaças e medidas	✓	✓	✓
Notícia		✓	✓
Links úteis	**	**	✓
Utilização do Email			
Problemas, ameaças e medidas	✓	✓	✓
Notícia		✓	✓
Comparação de emails	✓	✓	✓
Vídeo CNCS		✓	
Utilização da Internet			
Problemas, ameaças e medidas	✓	✓	✓
Vídeo demonstrativo		✓	✓
Utilização de Redes Sociais			
Problemas, ameaças e medidas	✓	✓	✓
Notícias		✓	✓*
Vídeo CNCS		✓	
Dispositivos Móveis			
Problemas, ameaças e medidas	✓	✓	✓
Notícias		✓	✓
Vídeos CNCS		✓	

Tratamento de Informações			
Problemas, ameaças e medidas	✓	✓	✓
Notícias		✓	✓
Vídeo CNCS		✓	
Comunicação de Incidentes			
Problemas, ameaças e medidas	✓	✓	✓
Vídeo CNCS		✓	
* Na plataforma IA os conteúdos de uma das notícias violavam as políticas de utilização pelo que não foi possível a sua inclusão. ** Divulgados durante a discussão.			

Tabela 3.5: *Conteúdos incluídos em cada sessão e no vídeo.*

Além das sessões presenciais, foi criado um vídeo com os conteúdos da apresentação e foi disponibilizado publicamente no YouTube[8]. O vídeo contém uma pessoa gerada por inteligência artificial, que apresenta e explica os conteúdos da apresentação.

O processo de criação do vídeo teve início com uma pesquisa sobre ferramentas de inteligência artificial capazes de gerar uma pessoa para apresentar os conteúdos. Dessa pesquisa, foram identificadas cinco opções: Synthesia[9], Pictory[10], Veed.io[11], Lumen5[12] e HeyGen[13]. A escolha recaiu sobre a plataforma HeyGen, por oferecer um nível mais elevado de personalização no seu plano gratuito.

Embora o narrador tenha sido criado com a plataforma HeyGen, a integração com os conteúdos da apresentação foi realizada através do programa de edição de vídeo OpenShot[14].

3.4.5 Fase 5 - Construção do Quiz

A quinta fase desta etapa consistiu no desenvolvimento de um Quiz, concebido para avaliar a retenção dos conteúdos transmitidos durante a apresentação. O Quiz foi composto por sete questões de escolha múltipla, disponíveis no Apêndice H, em que cada questão corresponde a um dos módulos da apresentação.
A plataforma utilizada para construir e disponibilizar o Quiz foi o Socrative[15], que permite criar quizzes de avaliação em tempo real de forma dinâmica e interativa.

Devido à duração limitada das sessões, o Quiz foi aplicado apenas na sessão de 90 minutos.

[8] Vídeo dos conteúdos: `https://youtu.be/9arF2JkqE1g`
[9] Synthesia: `www.synthesia.io/`
[10] Pictory: `pictory.ai`
[11] Veed.io: `www.veed.io`
[12] Lumen5: `lumen5.com`
[13] HeyGen: `www.heygen.com`
[14] OpenShot: `www.openshot.org`
[15] Socrative: `https://www.socrative.com/`

3.4.6 Fase 6 - Aplicação da Estratégia

A sexta fase desta etapa consistiu na aplicação da estratégia ao público-alvo definido. No entanto, não foi possível a sua aplicação a todas as licenciaturas não CTEAM da ESTG. Ainda assim, a estratégia foi implementada em dois cursos desse grupo: Gestão e Marketing.

No curso de Gestão a sessão de sensibilização foi realizada no dia 20 de março de 2025, no âmbito da unidade curricular de Seminário, lecionada aos estudantes do 2º ano. A sessão teve a duração de 45 minutos e foi realizada em dois turnos distintos. Nesta sessão devido à limitação de tempo não foi possível aplicar o Quiz.

No curso de Marketing a sessão decorreu no dia 24 de abril de 2025, também no contexto da unidade curricular de Seminário, lecionada aos estudantes do 2º ano. A sessão teve a duração de 90 minutos, tendo sido possível aplicar o Quiz nesta sessão.

3.4.7 Fase 7 - Análise de Resultados

A sétima e última fase desta etapa apresenta uma reflexão sobre a aplicação da estratégia de sensibilização, incluindo uma análise individual de cada sessão e uma análise dos resultados obtidos com o Quiz.

A primeira sessão sensibilização, realizada no dia 20 de março de 2025, em dois turnos do curso de Gestão, teve a duração de 45 minutos, o que impossibilitou a aplicação do Quiz e a apresentação de exemplos práticos para ilustrar as consequências da não adoção de boas práticas de cibersegurança. Ainda assim, durante a discussão foram esclarecidas dúvidas colocadas pelos estudantes e partilhados alguns *links* úteis.

A segunda sessão sensibilização, realizada no dia 24 de abril de 2025 no curso de Marketing, teve a duração de 90 minutos, o que possibilitou a aplicação do Quiz. Nesta sessão, tal como na anterior, durante a discussão foram esclarecidas dúvidas colocadas pelos estudantes e partilhados alguns *links* úteis.

A Figura 3.5 apresenta os resultados obtidos com a aplicação do Quiz na sessão de sensibilização realizada no curso de Marketing, como se pode verificar participaram 17 estudantes, que, no geral, responderam corretamente a todas as questões.

Nas sete perguntas do Quiz apenas se registaram três respostas incorretas: duas na pergunta 2 e uma na pergunta 5.
Na pergunta 2 - "***Como se pode identificar um email de phishing?***" - a resposta correta era a opção "***d*) *Todas as anteriores***". As duas respostas incorretas a esta pergunta tecnicamente não estão erradas, mas os participantes que responderam incorretamente não interpretaram que todas as opções apresentadas eram válidas.
Na pergunta 5 - "***Qual dos seguintes é um risco ao utilizar redes Wi-Fi públicas sem proteção?***" - a resposta correta era a opção "***a*) *Os dados podem ser intercetados por***

NAME	SCORE %	1	2	3	4	5	6	7
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 86%	✓ C	✓ D	✓ A	✓ D	✗ D	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 86%	✓ C	✗ B	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 86%	✓ C	✗ B	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
•••••••	✓ 100%	✓ C	✓ D	✓ A	✓ D	✓ A	✓ B	✓ C
17 Class Total		100%	88%	100%	100%	94%	100%	100%

Figura 3.5: *Resultado da aplicação do Quiz.*

atacantes". No entanto, um participante escolheu a opção "***d*) *O dispositivo pode desligar-se automaticamente da rede.***", revelando uma falha na identificação do principal risco apresentado.

Com base nos resultados obtidos com a aplicação do Quiz, pode-se afirmar que os conhecimentos sobre cibersegurança foram, de forma geral, bem transmitidos.

As sessões de sensibilização mostraram-se bastante enriquecedoras para promover a consciencialização dos estudantes sobre as boas práticas de cibersegurança. A utilização de notícias reais foi particularmente eficaz para demonstrar as possíveis consequências da não adoção dessas práticas.
Os estudantes demonstraram interesse pelo tema e participaram ativamente com perguntas e reflexões, o que reforça a importância da sensibilização para boas práticas de cibersegurança, especialmente em áreas de formação fora do espectro CTEAM.

4

Análise de Resultados

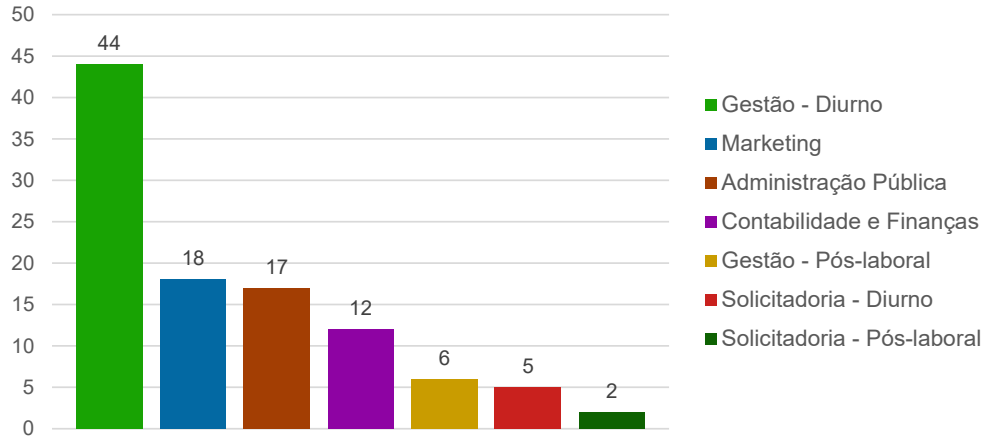
Neste capítulo, apresenta-se o desenvolvimento da etapa **Avaliar**, cujo principal objetivo consistiu na análise das respostas obtidas através do questionário de avaliação do nível de consciencialização para a cibersegurança.
A amostra recolhida é composta por 104 respostas, provenientes de estudantes de licenciaturas não pertencentes às áreas CTEAM, lecionadas na ESTG. Numa primeira fase, procedeu-se à análise das questões de caráter demográfico, com o intuito de caracterizar o público-alvo que participou no estudo (Secção 4.1). De seguida, com base nos dados estatísticos fornecidos pelo Google Forms, descreveu-se a distribuição das respostas por cada item da escala (Secção 4.2). Por fim, recorreu-se ao programa IBM SPSS para uma análise mais aprofundada dos dados recolhidos, com o objetivo de responder às questões de investigação e identificar as áreas que necessitam de estratégias de sensibilização mais eficazes (Secção 4.3).

4.1 Caracterização do Público-alvo.

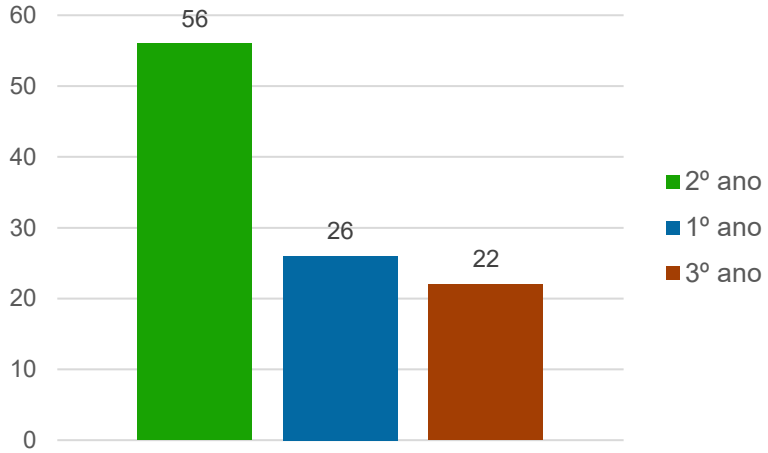
O questionário foi divulgado aos estudantes dos cursos de licenciatura em Administração Pública (Regime Diurno), Contabilidade e Finanças (Regime Diurno), Gestão (Regime Diurno e Regime Pós-laboral), Marketing (Regime Diurno) e Solicitadoria (Regime Diurno e Regime Pós-laboral).

No total, foi obtida uma amostra de 104 respostas provenientes dos estudantes de todos os cursos mencionados e abrangendo ambos os regimes de ensino: diurno e pós-laboral.

No questionário foram incluídas seis questões de caráter demográfico, que permitiram identificar o curso e o ano curricular frequentados pelos estudantes, o tipo de ingresso no ensino superior, a área de formação no ensino secundário, a faixa etária e o sexo dos participantes. A distribuição das respostas a estas questões está representada nas Figuras 4.1, 4.2 e 4.3.



(**a**) *Distribuição de respostas à pergunta "Qual o seu curso?"*

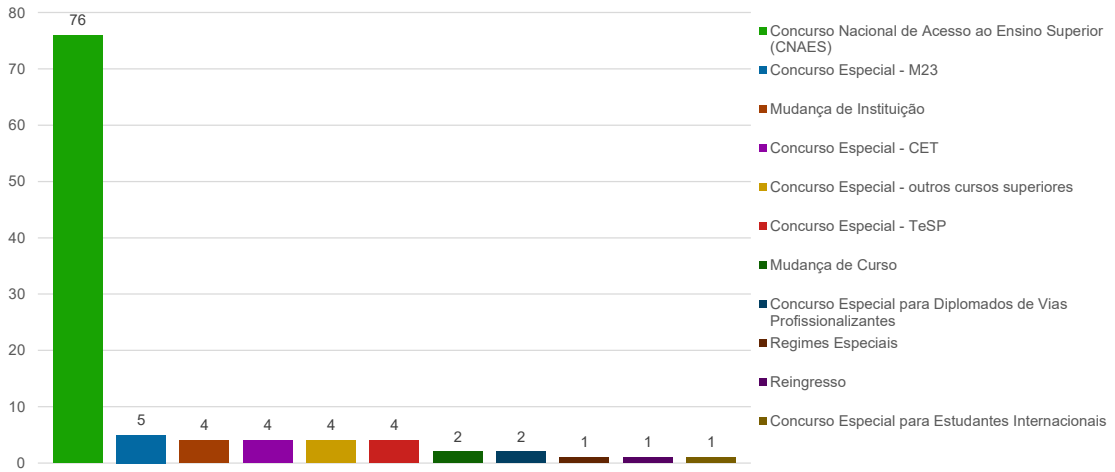


(**b**) *Distribuição de respostas à pergunta "Ano curricular."*

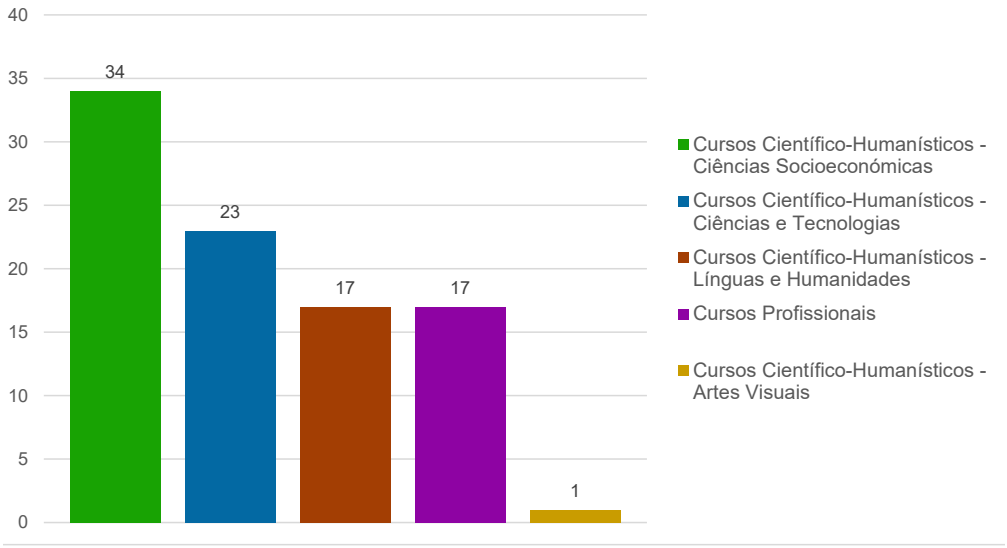
Figura 4.1: *Distribuição de respostas às questões relativas ao curso e ano curricular dos participantes.*

A questão "***Qual o seu curso?***" (Figura 4.1a), das 104 respostas obtidas, 44 (42,31%) correspondem ao curso de Gestão (regime diurno), 18 (17,31%) ao curso de Marketing, 17 (16,35%) a Administração Pública, 12 (11,54%) a Contabilidade e Finanças, 6 (5,77%) a Gestão (regime pós-laboral), 5 (4,81%) a Solicitadoria (regime diurno) e 2 (1,92%) a Solicitadoria (regime pós-laboral). Estes dados mostram que o curso com maior número de participantes foi Gestão (regime diurno), seguido de Marketing e Administração Pública. Por outro lado, o curso com menor número de respostas foi Solicitadoria, especialmente no regime pós-laboral, que teve apenas duas respostas.

Na questão "***Ano curricular.***" (Figura 4.1b), das 104 respostas obtidas, 56 (53,85%) correspondem a estudantes do 2º ano, 26 (25%) do 1º ano e 22 (21,15%) do 3º ano. Estes dados indicam que a maioria dos participantes frequenta o 2º ano curricular, enquanto o 3º ano apresenta o menor número de respostas.



(**a**) *Distribuição de respostas à pergunta "Tipo de ingresso no ensino superior."*



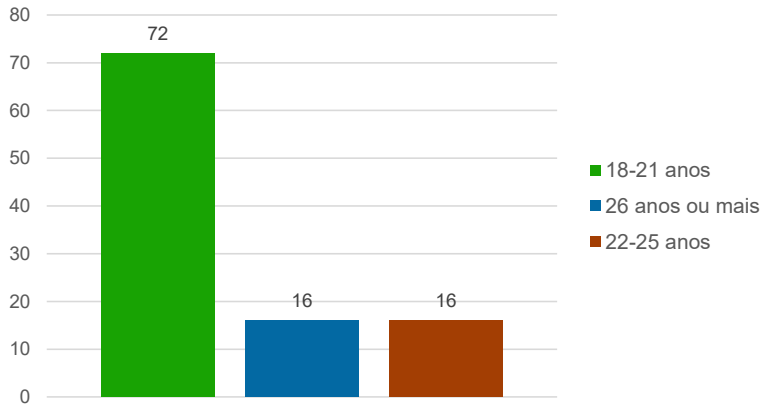
(**b**) *Distribuição de respostas à pergunta "Área do secundário."*

Figura 4.2: *Distribuição de respostas às questões relativas ao tipo de ingresso no ensino superior e área do secundário dos participantes.*

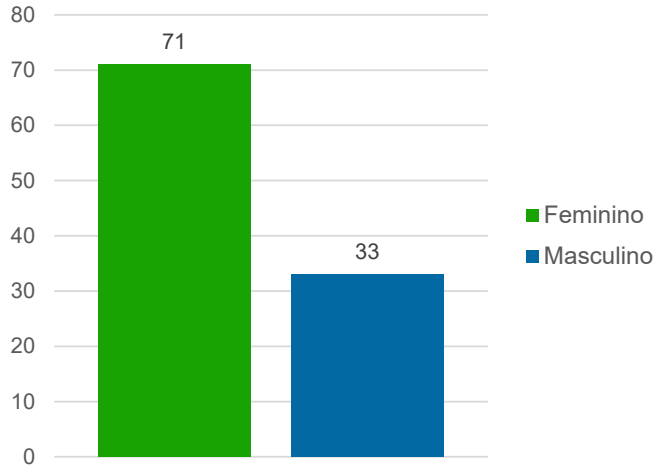
Na questão "***Tipo de ingresso no ensino superior.***" (Figura 4.2a), das 104 respostas obtidas, 76 (73,08%) correspondem ao Concurso Nacional de Acesso ao Ensino Superior (CNAES), que representa a esmagadora maioria das respostas. No entanto, também se registaram entradas no ensino superior por via de concursos especiais, nomeadamente para maiores de 23 anos (M23), Cursos de Especialização Tecnológica (CET), Cursos Técnicos Superiores Profissionais (TeSP), outros cursos superiores e por mudança de instituição ou curso.

A questão "***Área do secundário.***" (Figura 4.2b), era de resposta obrigatória apenas para os participantes que ingressaram através do CNAES, sendo opcional para os restantes. Das 104 respostas obtidas no questionário, 92 participantes responderam esta questão. Desses, 34 (36,96%) frequentaram a área de Ciências Socioeconómicas, 23 (25%) a área

de Ciências e Tecnologias, 17 (18,48%) a área de Línguas e Humanidades, 17 (18,48%) Cursos Profissionais e 1 (1,09%) a área de Artes Visuais. Estes dados indicam que a maioria dos participantes que respondeu a esta questão provém da área de Ciências Socioeconómicas do ensino secundário.



(a) *Distribuição de respostas à pergunta "Qual a sua faixa etária?"*



(b) *Sexo dos participantes.*

Figura 4.3: *Distribuição das respostas à pergunta "Qual o seu sexo?"*

Na questão "***Qual a sua faixa etária?***" (Figura 4.3a), das 104 respostas obtidas, 72 (69,23%) correspondem a participantes que têm entre os 18 e os 21 anos, 16 (15,38%) têm entre os 22 e os 25 anos e 16 (15,38%) têm 26 anos ou mais. Estes dados indicam que a maioria dos participantes se encontra na faixa etária dos 18 aos 21 anos.

Por fim, a questão "***Qual o seu sexo?***" (Figura 4.3b), das 104 respostas obtidas, 71 (68,27%) correspondem a participantes do sexo feminino e 33 (31,73%) do sexo masculino. Estes dados indicam que a maioria dos participantes é do sexo feminino.

4.2 Resultados por Item da Escala

Nesta Secção apresentam-se as respostas obtidas em cada item da escala, com base nas estatísticas disponibilizadas pelo Google Forms, plataforma utilizada para a divulgação do questionário.

A escala HAIS-Q, que serviu de base à construção do questionário, está organizada em sete áreas, cada uma composta por três subáreas. Cada subárea inclui três questões, destinadas a avaliar os conhecimentos, as atitudes e os comportamentos dos participantes em relação ao tópico em análise.

As respostas aos itens foram dadas com base numa escala de *Likert* de 5 pontos: (1) Discordo totalmente; (2) Discordo; (3) Não concordo nem discordo; (4) Concordo; e (5) Concordo totalmente. Para esta análise, as respostas com classificação maior ou igual a 4 foram consideradas positivas, 3 foram consideradas neutras e as restantes negativas. No caso, das questões de resposta inversa, a interpretação foi invertida.

Os resumos apresentados nesta secção estão organizados de acordo com a estrutura da escala, por área e respetivas subáreas.

4.2.1 Área de Incidência - Gestão de Palavras-passe

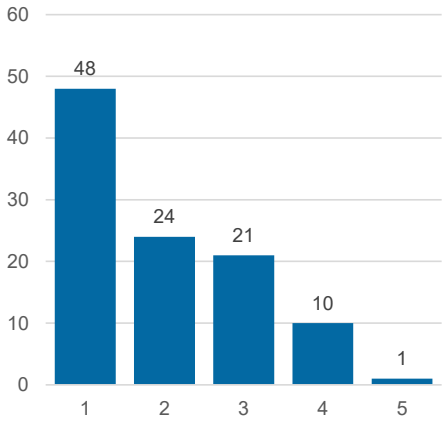
Esta área avalia os conhecimentos, as atitudes e os comportamentos, dos participantes, relativamente à utilização da mesma palavra-passe em vários serviços, à patilha de palavras-passe com outras pessoas e à complexidade das palavras-passe que utilizam. As Figuras 4.4, 4.5 e 4.6, apresentam a distribuição de respostas relativas às três subáreas descritas.

Utilizar a mesma palavra-passe

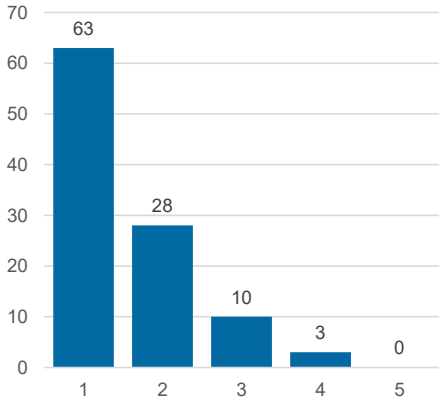
A Figura 4.4 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos relativos à utilização da mesma palavra-passe em vários serviços.

A pergunta "***1.1 - É aceitável utilizar as minhas palavras-passe das redes sociais nas minhas contas de trabalho.***" (Figura 4.4a), das 104 respostas obtidas, uma concorda totalmente, 10 concordam e 21 são neutras. Estes dados indicam um nível de conhecimento negativo em 10,58% das respostas, em 20,19% um nível de conhecimento neutro e em 69,23% um nível de conhecimento positivo.

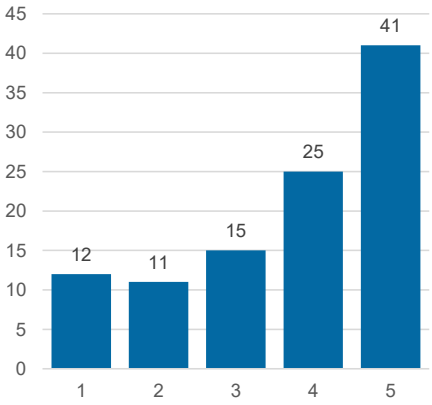
Na pergunta "***1.2 - É seguro utilizar a mesma palavra-passe para as contas das redes sociais e do trabalho.***" (Figura 4.4b), das 104 respostas obtidas, nenhuma concorda totalmente, 3 concordam e 10 são neutras. Estes dados indicam uma atitude negativa em 2,88% das respostas, em 9,62% uma atitude neutra e em 87,50% uma atitude positiva.



(**a**) *Distribuição de respostas à pergunta "1.1 - É aceitável utilizar as minhas palavras-passe das redes sociais nas minhas contas de trabalho.'*



(**b**) *Distribuição de respostas à pergunta "1.2 - É seguro utilizar a mesma palavra-passe para as contas das redes sociais e do trabalho."*



(**c**) *Distribuição de respostas à pergunta "1.3 - Utilizo uma palavra-passe diferente para as minhas contas das redes sociais e do trabalho.'*

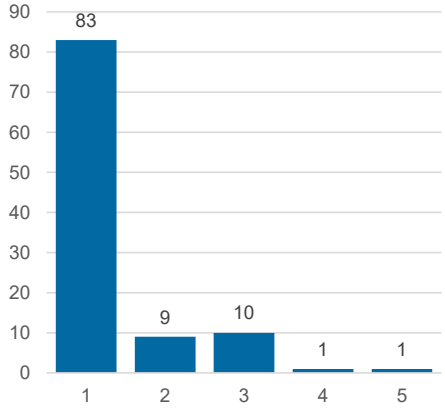
Figura 4.4: *Distribuição das respostas às questões relativas à utilização da mesma palavra-passe em vários serviços.*

Por fim, a pergunta "***1.3 - Utilizo uma palavra-passe diferente para as minhas contas das redes sociais e do trabalho.***" (Figura 4.4c), das 104 respostas obtidas, 41 concordam totalmente, 25 concordam e 15 são neutras. Estes dados indicam um comportamento positivo em 63,46% das respostas, em 14,42% um comportamento neutro e em 22,12% um comportamento negativo.

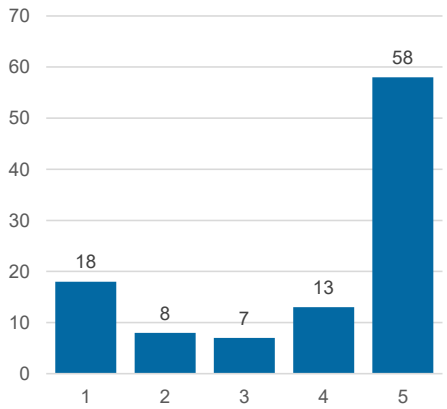
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes tem consciência que não se deve reutilizar palavras-passe entre diferentes serviços. No entanto, uma parte significativa ainda demonstra alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria reconhece que reutilizar palavras-passe não é seguro. No que diz respeito ao comportamento, a maioria dos participantes afirma que utiliza palavras-passe distintas para as contas de trabalho e redes sociais, embora uma parte dos participantes admite que não o faz.

Partilhar palavras-passe

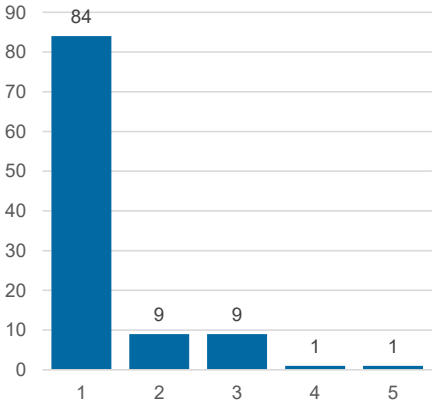
A Figura 4.5 apresenta a distribuição das respostas às três perguntas que avaliam os conhecimentos, as atitudes e os comportamentos sobre a partilha de palavras-passe.



(**a**) *Distribuição de respostas à pergunta "2.1 - Posso partilhar as minhas palavras-passe do trabalho com colegas."*



(**b**) *Distribuição de respostas à pergunta "2.2 - É uma má ideia partilhar as minhas palavras-passe do trabalho, mesmo que um colega as peça."*



(**c**) *Distribuição de respostas à pergunta "2.3 - Partilho as minhas palavras-passe do trabalho com colegas."*

Figura 4.5: *Distribuição das respostas às questões relativas à partilha de palavras-passe com terceiros.*

A pergunta "***2.1 - Posso partilhar as minhas palavras-passe do trabalho com colegas.***" (Figura 4.5a), das 104 respostas obtidas, 1 concorda totalmente, 1 concorda e 10 são neutras. Estes dados que indicam um nível de conhecimento negativo em 1,92% das respostas, em 9,62% um nível de conhecimento neutro e em 88,46% um nível de conhecimento positivo.

Na pergunta "***2.2 - É uma má ideia partilhar as minhas palavras-passe do trabalho, mesmo que um colega as peça.***" (Figura 4.5b), das 104 respostas obtidas, 58 concordam totalmente, 13 concordam e 7 são neutras. Estes dados indicam uma atitude positiva em 68,27% das respostas, em 6,73% uma atitude neutra e em 25% uma atitude negativa.

Por fim, a pergunta "***2.3 - Partilho as minhas palavras-passe do trabalho com colegas.***" (Figura 4.5c), das 104 respostas obtidas, uma concorda totalmente, uma concorda e 9 são neutras. Estes dados indicam um comportamento negativo em 1,92% das respostas, em 8,65% um comportamento neutro e em 89,42% um comportamento positivo.

Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes está ciente que não se deve partilhar palavras-passe. No que diz respeito à atitude, a maioria reconhece que partilhar palavras-passe não é uma boa prática, embora uma parte significativa não veja problema em o fazer. Relativamente ao comportamento, a esmagadora maioria afirma não partilhar palavras-passe com colegas.

Utilizar uma palavra-passe forte

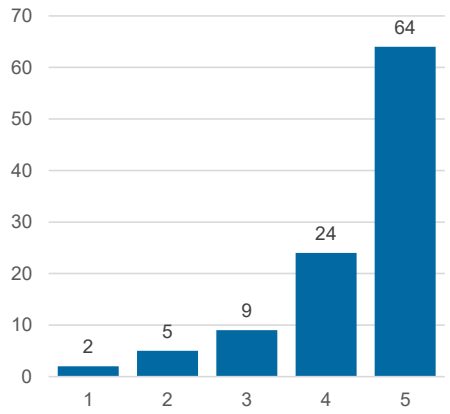
A Figura 4.6 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos relativamente ao grau de complexidade das palavras-passe utilizadas.

A pergunta "***3.1 - É necessária uma combinação de letras, números e símbolos para as palavras-passe de trabalho.***" (Figura 4.6a), das 104 respostas obtidas, 64 concordam totalmente, 24 concordam e 9 são neutras. Estes dados indicam um nível de conhecimento positivo em 84,62% das respostas, em 8,65% um nível de conhecimento neutro e em 6,73% um nível de conhecimento negativo.

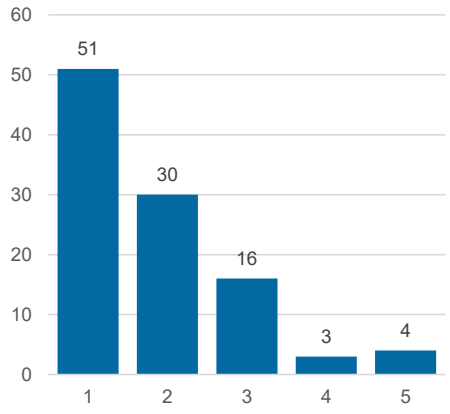
Na pergunta "***3.2 - É seguro ter uma palavra-passe de trabalho apenas com letras.***" (Figura 4.6b), das 104 respostas obtidas, 4 concordam totalmente, 3 concordam e 16 são neutras. Estes dados indicam uma atitude negativa em 6,73% das respostas, em 15,38% uma atitude neutra e em 77,88% uma atitude positiva.

Por fim, a pergunta "***3.3 - Utilizo uma combinação de letras, números e símbolos nas minhas palavras-passe de trabalho.***" (Figura 4.6c), das 104 respostas obtidas, 69 concordam totalmente, 16 concordam e 14 são neutras. Estes dados indicam um comportamento positivo em 81,73% das respostas, em 13,46% um comportamento neutro e em 4,81% um comportamento negativo.

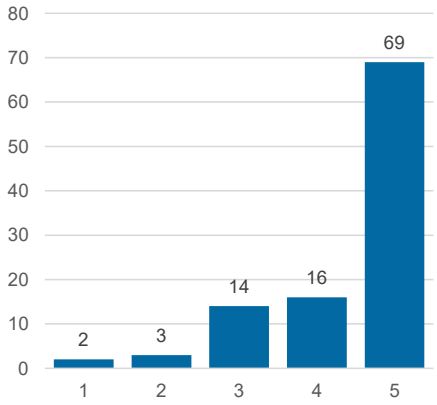
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes tem consciência que é importante utilizar uma combinação de letras, números e símbolos nas palavras-passe. Em relação à atitude a maioria reconhece que não seguro utilizar apenas uma combinação de letras. No que diz respeito ao comportamento, a esmagadora maioria afirma adotar palavras-passe que combinam vários tipo de caracteres.



(**a**) *Distribuição de respostas à pergunta "3.1 - É necessária uma combinação de letras, números e símbolos para as palavras-passe de trabalho."*



(**b**) *Distribuição de respostas à pergunta "3.2 - É seguro ter uma palavra-passe de trabalho apenas com letras."*



(**c**) *Distribuição de respostas à pergunta "3.3 - Utilizo uma combinação de letras, números e símbolos nas minhas palavras-passe de trabalho."*

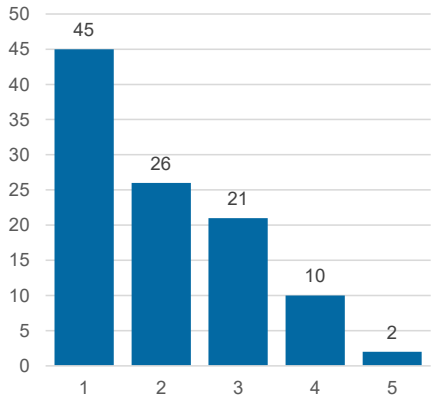
Figura 4.6: *Distribuição das respostas às questões relativas à utilização palavras-passe fortes.*

4.2.2 Área de Incidência - Utilização do email

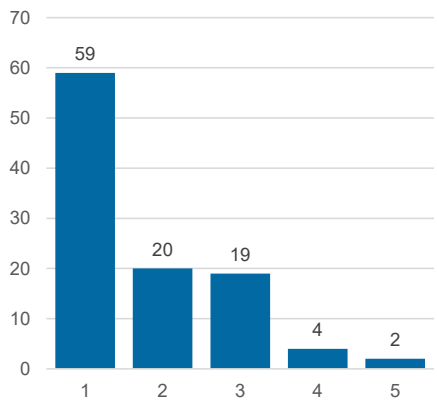
Esta área avalia os conhecimentos, as atitudes e os comportamentos, dos participantes, em relação aos emails que recebem, nomeadamente se clicam em *links* presentes em emails enviados por remetentes conhecidos ou desconhecidos, ou se abrem anexos de emails provenientes de remetentes desconhecidos.
As Figuras 4.7, 4.8 e 4.9, apresentam a distribuição de respostas relativas às três subáreas descritas.

Clicar em links de emails enviados por remetentes conhecidos

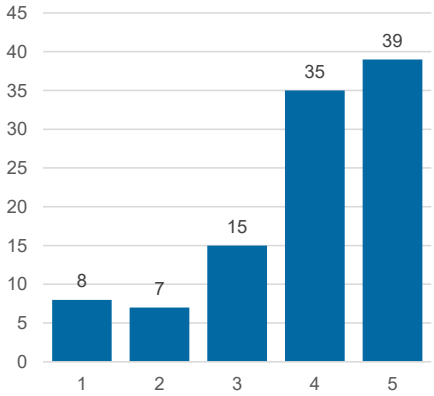
A Figura 4.7 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre clicar em *links* presentes em emails enviados por remetentes conhecidos.



(**a**) *Distribuição de respostas à pergunta "4.1 - Posso clicar em quaisquer links de emails enviados por pessoas que conheço."*



(**b**) *Distribuição de respostas à pergunta "4.2 - É sempre seguro clicar em links de emails enviados por pessoas que conheço."*



(**c**) *Distribuição de respostas à pergunta "4.3 - Nem sempre clico nos links de emails só porque vêm de alguém que conheço."*

Figura 4.7: *Distribuição das respostas às questões sobre clicar em links de emails enviados por remetentes conhecidos.*

A pergunta "***4.1 - Posso clicar em quaisquer links de emails enviados por pessoas que conheço.***" (Figura 4.7a), das 104 respostas obtidas, 2 concordam totalmente, 10 concordam e 21 são neutras. Estes dados indicam um nível de conhecimento negativo em 11,64% das respostas, em 20,19% um nível de conhecimento neutro e em 68,27% um nível de conhecimento positivo.

Na pergunta "***4.2 - É sempre seguro clicar em links de emails enviados por pessoas que conheço.***" (Figura 4.7b), das 104 respostas obtidas, 2 concordam totalmente, 4 concordam e 19 são neutras. Estes dados indicam uma atitude negativa em 5,77% das respostas, em 18,27% uma atitude neutra e em 75,96% uma atitude positiva.

Por fim, a pergunta "***4.3 - Nem sempre clico nos links de emails só porque vêm de alguém que conheço.***" (Figura 4.7b), das 104 respostas obtidas, 39 concordam totalmente, 35 concordam e 15 são neutras. Estes dados indicam um comportamento positivo em

71,15% das respostas, em 14,42% um comportamento neutro e em 14,42% um comportamento negativo.

Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que não se deve clicar em *links* enviados por remetentes conhecidos sem a devida verificação, embora uma parte significativa ainda revele alguma incerteza. Quanto à atitude, a esmagadora maioria considera que nem sempre é seguro clicar em *links*, mesmo conhecendo o remetente. Relativamente ao comportamento, a maioria afirma que nem sempre clica em *links* enviados por pessoas conhecidas.

Clicar em links de emails enviados por remetentes desconhecidos

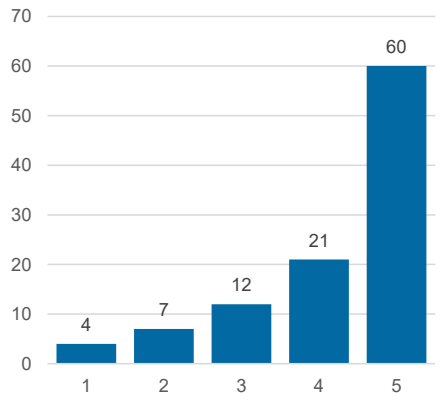
A Figura 4.8 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre clicar em *links* presentes em emails enviados por remetentes desconhecidos.

A pergunta "***5.1 - Não posso clicar num link de um email enviado por um remetente desconhecido.***" (Figura 4.8a), das 104 respostas obtidas, 60 concordam totalmente, 21 concordam e 12 são neutras. Estes dados indicam um nível de conhecimento positivo em 77,88% das respostas, em 11,54% um nível de conhecimento neutro e em 10,58% um nível de conhecimento negativo.

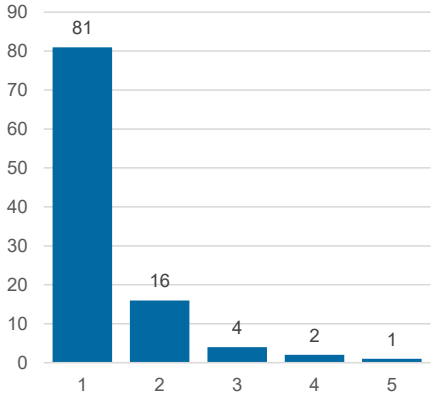
Na pergunta "***5.2 - Nada de mal pode acontecer se eu clicar em um link de um email enviado por um remetente desconhecido.***" (Figura 4.8b), das 104 respostas obtidas, uma concorda totalmente, 2 concordam e 4 são neutras. Estes dados indicam uma atitude negativa em 2,88% das respostas, em 3,85% uma atitude neutra e em 93,27% uma atitude positiva.

Por fim, a pergunta "***5.3 - Se um email enviado por um remetente desconhecido parecer interessante, clico no link.***" (Figura 4.8c), das 104 respostas obtidas, 2 concordam totalmente, uma concorda e 9 são neutras. Estes dados indicam um comportamento negativo em 2,88% das respostas, em 8,65% um comportamento neutro e em 88,46% um comportamento positivo.

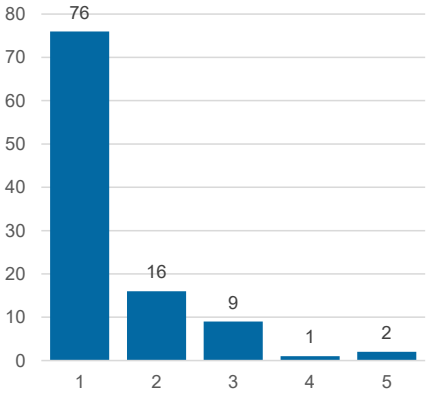
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que não se deve clicar em *links* presentes em emails provenientes de remetentes desconhecidos. No entanto, uma parte significativa demonstra alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria reconhece que não é seguro clicar em *links* presentes em emails provenientes de remetentes desconhecidos. Relativamente ao comportamento, a esmagadora maioria afirma que não clicaria num *link* presente num email desconhecido, mesmo que o conteúdo pareça interessante.



(**a**) *Distribuição de respostas à pergunta "5.1 - Não posso clicar num link de um email enviado por um remetente desconhecido."*



(**b**) *Distribuição de respostas à pergunta "5.2 - Nada de mal pode acontecer se eu clicar em um link de um email enviado por um remetente desconhecido."*



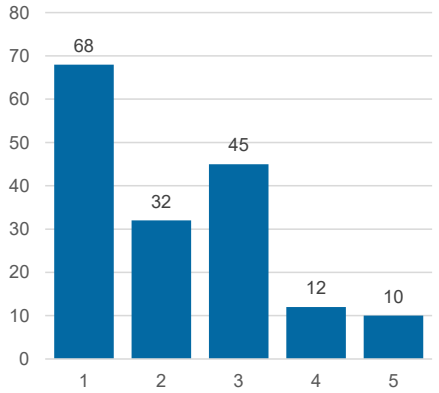
(**c**) *Distribuição de respostas à pergunta "5.3 - Se um email enviado por um remetente desconhecido parecer interessante, clico no link."*

Figura 4.8: *Distribuição das respostas às questões sobre clicar em links de emails enviados por remetentes desconhecidos.*

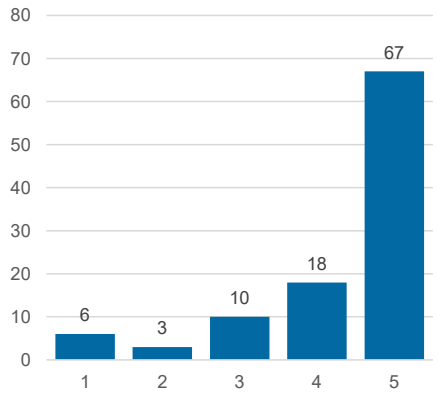
Abrir anexos de emails enviados por remetentes desconhecidos

A Figura 4.9 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre abrir anexos presentes em emails enviados por remetentes desconhecidos.

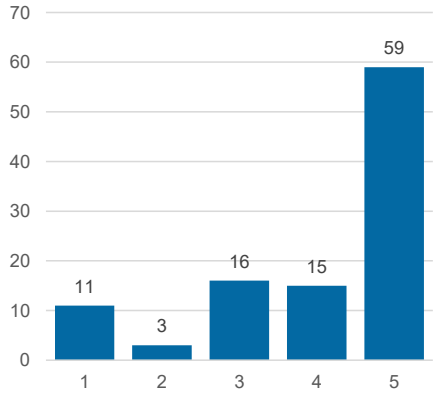
A pergunta "***6.1 - Posso abrir anexos de emails enviados por remetentes desconhecidos.***" (Figura 4.9a), das 104 respostas obtidas, 10 concordam totalmente, 12 concordam, 45 são neutras. Estes dados indicam um nível de conhecimento negativo em 13,17% das respostas, em 26,95% um nível de conhecimento neutro e em 59,88 um nível de conhecimento positivo.



(**a**) *Distribuição de respostas à pergunta "6.1 - Posso abrir anexos de emails enviados por remetentes desconhecidos."*



(**b**) *Distribuição de respostas à pergunta "6.2 - É arriscado abrir um anexo de email enviado por um remetente desconhecido."*



(**c**) *Distribuição de respostas à pergunta "6.3 - Não abro anexos de email se o remetente for desconhecido para mim."*

Figura 4.9: *Distribuição das respostas às questões sobre abrir anexos de emails enviados por remetentes desconhecidos.*

Na pergunta "***6.2 - É arriscado abrir um anexo de email enviado por um remetente desconhecido.***" (Figura 4.9b), das 104 respostas obtidas, 67 concordam totalmente, 18 concordam e 10 são neutras. Estes dados indicam uma atitude positiva em 81,73% das respostas, em 9,62% uma atitude neutra e em 8,65% uma atitude negativa.

Por fim, a pergunta "***6.3 - Não abro anexos de email se o remetente for desconhecido para mim.***" (Figura 4.9c), das 104 respostas obtidas, 59 concordam totalmente, 15 concordam e 16 são neutras. Estes dados indicam um comportamento positivo em 71,15% das respostas, em 15,38% um comportamento neutro e em 13,46% um comportamento negativo.

Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que não se devem abrir anexos provenientes de emails de origem desconhecida, embora uma parte significativa demonstre alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria considera inseguro abrir anexos de emails desconhe-

cidos, apesar de alguns participantes admitam não ter a certeza. No que diz respeito ao comportamento, a maioria afirma que não abre anexos enviados por remetentes desconhecidos, embora alguns admitam que por vezes o faz.

4.2.3 Área de Incidência - Utilização da Internet

Esta área avalia os conhecimentos, as atitudes e os comportamentos dos participantes relativamente à utilização da Internet, nomeadamente a transferência de ficheiros, a utilização de *websites* duvidosos e o preenchimento de dados *online*.

As Figuras 4.10, 4.11 e 4.12, apresentam a distribuição de respostas relativas às três subáreas descritas.

Transferir ficheiros

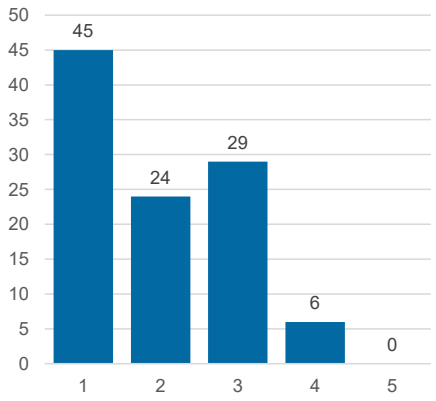
A Figura 4.10 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos relativos à transferência de ficheiros.

A pergunta "***7.1 - Posso descarregar quaisquer ficheiros para o meu computador de trabalho se me ajudarem a fazer o meu trabalho.***" (Figura 4.10a), das 104 respostas obtidas, nenhuma concorda totalmente, 6 concordam e 29 são neutras. Estes dados indicam um nível de conhecimento negativo em 5,77% das respostas, em 27,88% um nível de conhecimento neutro e em 66,35% um nível de conhecimento positivo.

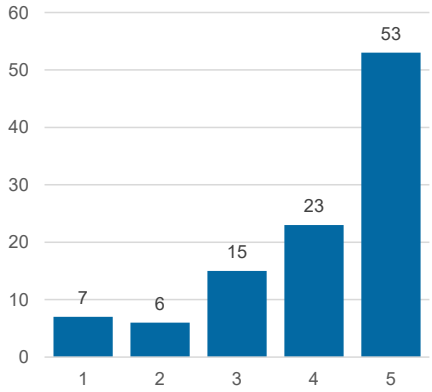
Na pergunta "***7.2 - Pode ser arriscado descarregar ficheiros no meu computador de trabalho.***" (Figura 4.10b), das 104 respostas obtidas, 53 concordam totalmente, 23 concordam e 15 são neutras. Estes dados indicam uma atitude positiva em 73,08% das respostas, em 14,42% uma atitude neutra e em 12,50% uma atitude negativa.

Por fim, a pergunta "***7.3 - Descarrego todos os ficheiros para o meu computador de trabalho que me ajudem a fazer o meu trabalho.***" (Figura 4.10c), das 104 respostas obtidas, 7 concordam totalmente, 13 concordam e 35 são neutras. Estes dados indicam um comportamento negativo em 19,23% das respostas, em 33,65% um comportamento neutro e em 47,12% um comportamento positivo.

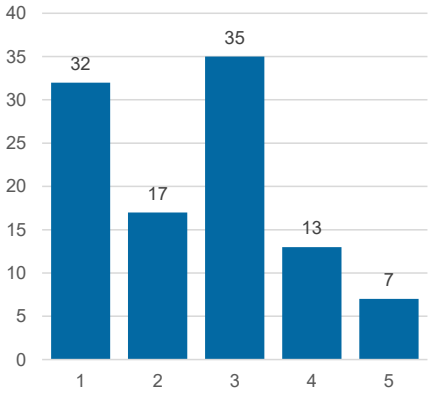
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que não se devem descarregar qualquer tipo de ficheiros para o computador de trabalho, embora uma parte significativa demonstre alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria considera inseguro transferir qualquer tipo de ficheiros para o computador de trabalho. Relativamente ao comportamento, a maioria dos participantes afirma não descarregar qualquer tipo de ficheiros para o computador de trabalho. No entanto, uma parte significativa admite que por vezes o faz.



(**a**) *Distribuição de respostas à pergunta "7.1 - Posso descarregar quaisquer ficheiros para o meu computador de trabalho se me ajudarem a fazer o meu trabalho."*



(**b**) *Distribuição de respostas à pergunta "7.2 - Pode ser arriscado descarregar ficheiros no meu computador de trabalho."*



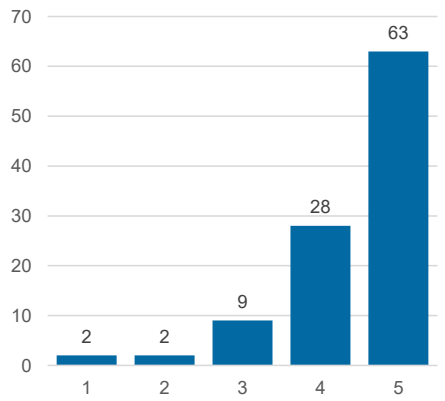
(**c**) *Distribuição de respostas à pergunta "7.3 - Descarrego todos os ficheiros para o meu computador de trabalho que me ajudem a fazer o meu trabalho."*

Figura 4.10: *Distribuição das respostas às questões sobre transferir ficheiros.*

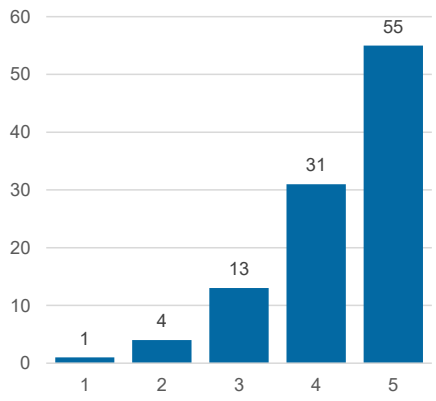
Aceder a websites duvidosos

A Figura 4.11 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos relativos ao acesso a *websites* duvidosos.

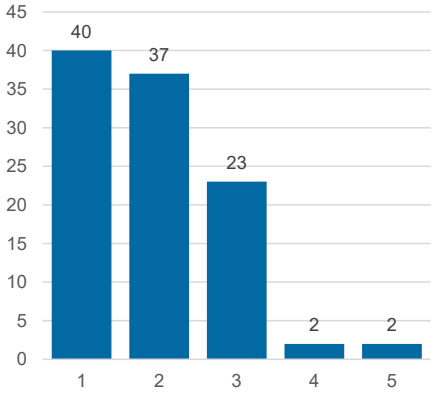
A pergunta "***8.1 - Enquanto estou no trabalho, não devo aceder a determinados websites.***" (Figura 4.11a), das 104 respostas obtidas, 63 concordam totalmente, 28 concordam e 9 são neutras. Estes dados indicam um nível de conhecimento positivo em 87,50% das respostas, em 8,65% um nível de conhecimento neutro e em 3,85% nível de conhecimento negativo.



(**a**) *Distribuição de respostas à pergunta "8.1 - Enquanto estou no trabalho, não devo aceder a determinados websites."*



(**b**) *Distribuição de respostas à pergunta "8.2 - Só porque posso aceder a um website no trabalho, não significa que seja seguro."*



(**c**) *Distribuição de respostas à pergunta "8.3 - Quando acedo à Internet no trabalho, visito qualquer website que queira."*

Figura 4.11: *Distribuição das respostas às questões sobre aceder a websites duvidosos.*

Na pergunta *"**8.2 - Só porque posso aceder a um website no trabalho, não significa que seja seguro.**"* (Figura 4.11b), das 104 respostas obtidas, 55 concordam totalmente, 31 concordam e 13 são neutras. Estes dados indicam uma atitude positiva em 82,69% das respostas, em 12,50% uma atitude neutra e em 4,81% uma atitude negativa.

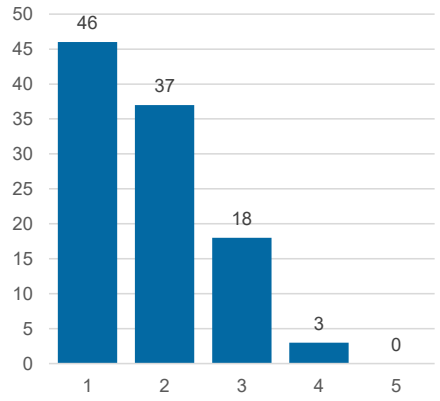
Por fim, a pergunta *"**8.3 - Quando acedo à Internet no trabalho, visito qualquer website que queira.**"* (Figura 4.11c), das 104 respostas, 2 concordam totalmente, 2 concordam e 23 são neutras. Estes dados indicam um comportamento negativo em 3,85% das respostas, em 22,12% um comportamento neutro e em 74,04% um comportamento positivo.

Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve aceder a determinados *websites* no local de trabalho. Quanto à atitude, a maioria dos participantes considera que aceder a esses *websites* não é seguro. No que diz respeito ao comportamento, a esmagadora maioria

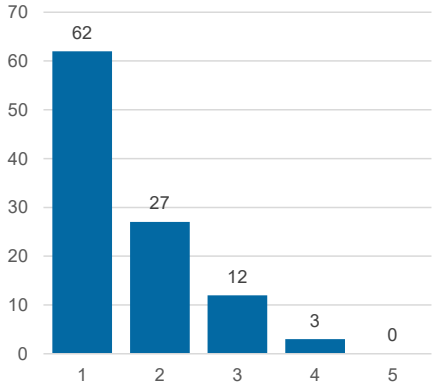
afirma que não acede a determinados *websites* no contexto profissional, embora alguns participantes admitam que por vezes o fazem.

Introduzir informações online

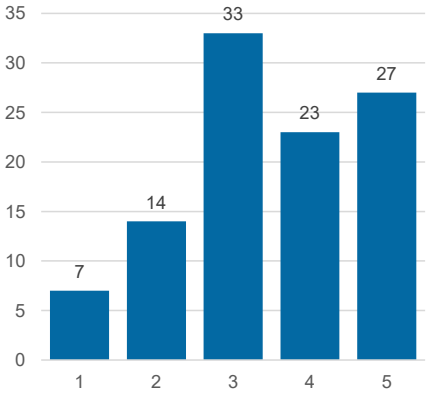
A Figura 4.12 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre o preenchimento de informações *online*.



(**a**) *Distribuição de respostas à pergunta "9.1 - Posso introduzir qualquer informação em qualquer website se isso me ajudar a fazer o meu trabalho."*



(**b**) *Distribuição de respostas à pergunta "9.2 - Se me ajudar a fazer o meu trabalho, não importa a informação que coloco num website."*



(**c**) *Distribuição de respostas à pergunta "9.3 - Verifico a segurança dos websites antes de introduzir informações."*

Figura 4.12: *Distribuição das respostas às questões sobre introduzir informações online.*

A pergunta "***9.1 - Posso introduzir qualquer informação em qualquer website se isso me ajudar a fazer o meu trabalho.***" (Figura 4.12a), das 104 respostas obtidas, nenhuma concorda totalmente, 3 concordam e 18 são neutras. Estes dados indicam um nível de conhecimento negativo em 2,88% das respostas, em 17,31% um nível de conhecimento neutro e em 79,81% um nível de conhecimento positivo.

Na pergunta "***9.2 - Se me ajudar a fazer o meu trabalho, não importa a informação que***

coloco num website." (Figura 4.12b), das 104 respostas obtidas, nenhuma concorda totalmente, 3 concordam e 12 são neutras. Estes dados indicam uma atitude negativa em 2,88% das respostas, em 11,54% uma atitude neutra e em 85,58% uma atitude positiva.

Por fim, a pergunta "***9.3 - Verifico a segurança dos websites antes de introduzir informações.***" (Figura 4.12c), das 104 respostas obtidas, 27 concordam totalmente, 23 concordam e 33 são neutras. Estes dados indicam um comportamento positivo em 48,08% das respostas, em 31,73% um comportamento neutro e em 20,19% um comportamento negativo.

Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve fornecer informações em qualquer *website*. Quanto à atitude, a maioria afirma que não colocaria informações em qualquer *website*. No que diz respeito ao comportamento, a maior parte dos participantes indica que verifica a segurança dos *websites* antes de inserir informações. No entanto, uma parte significativa admite nem sempre o faz.

4.2.4 Área de Incidência - Utilização de redes sociais

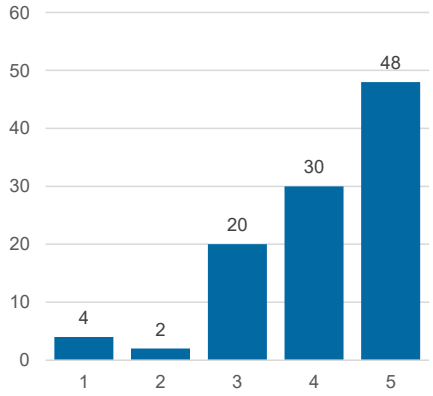
Esta área avalia os conhecimentos, as atitudes e os comportamentos dos participantes na utilização de redes sociais, com foco em aspetos como as definições de privacidade, a consideração das consequências das publicações realizadas e a partilha de conteúdos relacionados com o local de trabalho trabalho.
As Figuras 4.13, 4.14 e 4.15, apresentam a distribuição de respostas relativas às três subáreas descritas.

Definições de privacidade das redes sociais

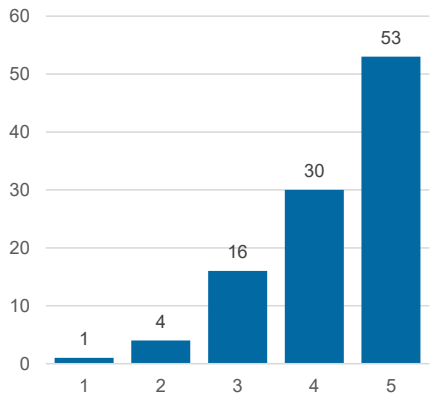
A Figura 4.13 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos em relação às definições de privacidade das redes sociais.

A pergunta "***10.1 - Devo rever periodicamente as definições de privacidade das minhas contas nas redes sociais.***" (Figura 4.13a), das 104 respostas obtidas, 48 concordam totalmente, 30 concordam, 20 são neutras. Estes dados indicam um nível de conhecimento positivo em 75,00% das respostas, em 19,23% um nível de conhecimento neutro e em 5,77% um nível de conhecimento positivo.

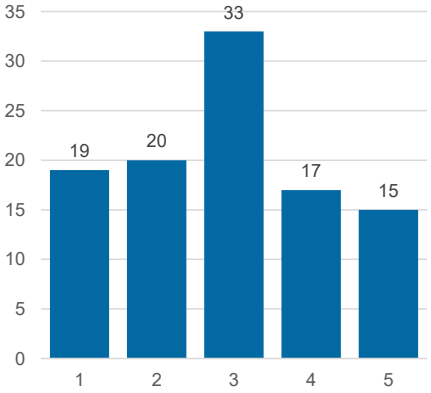
Na pergunta "***10.2 - É uma boa ideia rever regularmente as minhas definições de privacidade nas redes sociais.***" (Figura 4.13b), das 104 respostas obtidas, 53 concordam totalmente, 30 concordam e 16 são neutras. Estes dados indicam uma atitude positiva em 79,81% das respostas, em 15,38% uma atitude neutra e em 4,81% uma atitude negativa.



(**a**) *Distribuição de respostas à pergunta "10.1 - Devo rever periodicamente as definições de privacidade das minhas contas nas redes sociais."*



(**b**) *Distribuição de respostas à pergunta "10.2 - É uma boa ideia rever regularmente as minhas definições de privacidade nas redes sociais."*



(**c**) *Distribuição de respostas à pergunta "10.3 - Não revejo regularmente as definições de privacidade das minhas redes sociais."*

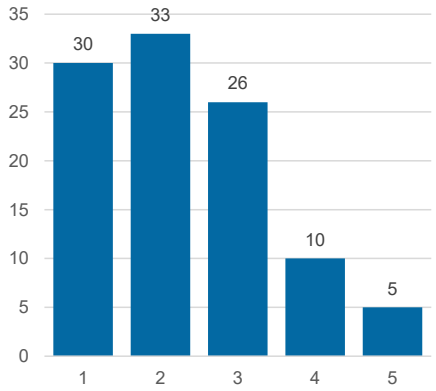
Figura 4.13: *Distribuição das respostas às questões sobre as definições de privacidade das redes sociais*

Por fim, a pergunta *"**10.3 - Não revejo regularmente as definições de privacidade das minhas redes sociais.**"* (Figura 4.13c), das 104 respostas obtidas, 15 concordam totalmente, 17 concordam e 33 são neutras. Estes dados indicam um comportamento negativo em 30,77% das respostas, em 31,73% um comportamento neutro e em 37,50% um comportamento positivo.

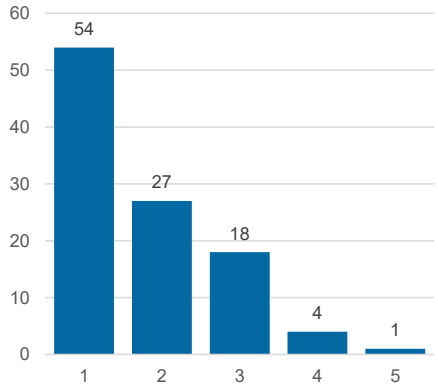
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece a importância de rever periodicamente as definições de privacidade das redes sociais. Quanto à atitude, a maioria considera que é uma boa prática rever regularmente as definições de privacidade. No que diz respeito ao comportamento, a uma parte dos participantes afirma rever com regularidade as definições de privacidade das redes sociais. No entanto, uma parte bastante significativa admite não ter o hábito de o fazer regularmente.

Considerar consequências

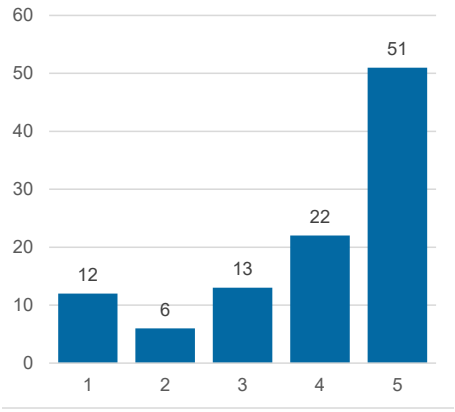
A Figura 4.14 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre considerar as consequências das publicações efetuadas nas redes sociais.



(**a**) *Distribuição de respostas à pergunta "11.1 - Não posso ser despedido por algo que publiquei nas redes sociais."*



(**b**) *Distribuição de respostas à pergunta "11.2 - Não vejo problema em publicar nas redes sociais coisas que eu normalmente não diria em público."*



(**c**) *Distribuição de respostas à pergunta "11.3 - Não publico nada nas redes sociais antes de pensar nas consequências negativas."*

Figura 4.14: *Distribuição das respostas às questões sobre considerar as consequências das redes sociais.*

A pergunta "***11.1 - Não posso ser despedido por algo que publiquei nas redes sociais.***" (Figura 4.14a), das 104 respostas obtidas, 5 concordam totalmente, 10 concordam e 26 são neutras. Estes dados indicam um nível de conhecimento negativo em 14,42% das respostas, em 25,00% um nível de conhecimento neutro e em 60,58% um nível de conhecimento positivo.

Na pergunta "***11.2 - Não vejo problema em publicar nas redes sociais coisas que eu normalmente não diria em público.***" (Figura 4.14b), das 104 respostas obtidas, uma concorda totalmente, 4 concordam e 18 são neutras. Estes dados indicam uma atitude negativa em 4,81% das respostas, em 17,31% uma atitude neutra e em 77,88% uma

atitude positiva.

Por fim, a pergunta *"**11.3 - Não publico nada nas redes sociais antes de pensar nas consequências negativas.**"* (Figura 4.14c), das 104 respostas obtidas, 51 concordam totalmente, 22 concordam e 13 são neutras. Estes dados indicam um comportamento positivo em 70,19% das respostas, em 12,50% um comportamento neutro e em 17,31% um comportamento negativo.

Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que pode ser despedido devido a publicações nas redes sociais, embora uma parte revele alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria afirma que não publicaria nas redes sociais algo que normalmente não diria em público. Relativamente ao comportamento, a maioria dos participantes afirma que evita publicar conteúdos nas redes sociais sem antes considerar as possíveis consequências.

Publicar sobre o trabalho

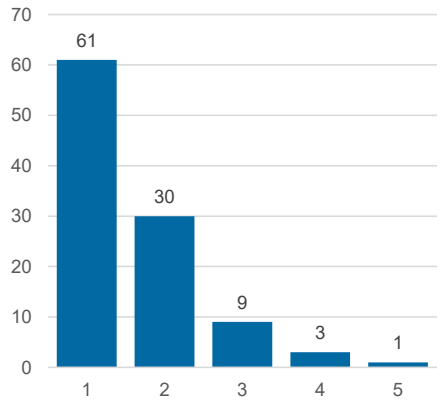
A Figura 4.15 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre publicar conteúdos nas redes sociais relacionados com o trabalho.

A pergunta *"**12.1 - Posso publicar o que quiser sobre o meu trabalho nas redes sociais.**"* (Figura 4.15a), das 104 respostas obtidas, uma concorda totalmente, 3 concordam e 9 são neutras. Estes dados indicam um nível de conhecimento negativo em 3,85% das respostas, em 8,65% um nível de conhecimento neutro e em 87,50% um nível de conhecimento positivo.

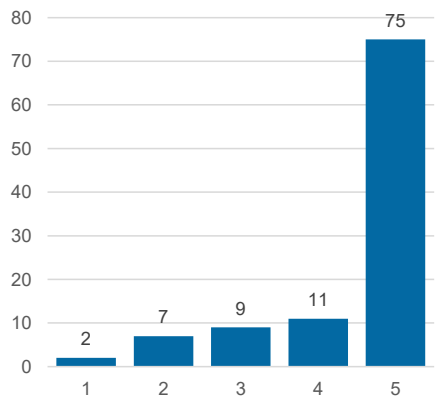
Na pergunta *"**12.2 - É arriscado publicar certas informações sobre o meu trabalho nas redes sociais.**"* (Figura 4.15b), das 104 respostas obtidas, 75 concordam totalmente, 11 concordam e 9 são neutras. Estes dados indicam uma atitude positiva em 82,69% das respostas, em 8,65% uma atitude neutra e em 8,65% uma atitude negativa.

Por fim, a pergunta *"**12.3 - Publico o que quiser sobre o meu trabalho nas redes sociais.**"* (Figura 4.15c), das 104 respostas obtidas, nenhuma concorda totalmente, 3 concordam e 16 são neutras. Estes dados indicam um comportamento negativo em 2,88% das respostas, em 15,38% um comportamento neutro e em 81,73% um comportamento positivo.

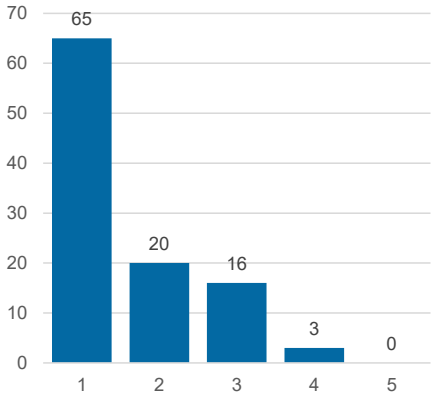
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que algumas informações, relacionadas com o local de trabalho, não devem ser publicadas nas redes sociais. Quanto à atitude, a maioria admite que é arriscado partilhar determinados conteúdos sobre o trabalho nas redes sociais. No que diz respeito ao comportamento, a esmagadora maioria afirma que não publica conteúdos relacionados com o trabalho nas redes sociais.



(**a**) *Distribuição de respostas à pergunta "12.1 - Posso publicar o que quiser sobre o meu trabalho nas redes sociais."*



(**b**) *Distribuição de respostas à pergunta "12.2 - É arriscado publicar certas informações sobre o meu trabalho nas redes sociais."*



(**c**) *Distribuição de respostas à pergunta "12.3 - Publico o que quiser sobre o meu trabalho nas redes sociais."*

Figura 4.15: *Distribuição das respostas às questões sobre publicar assuntos do trabalho nas redes sociais.*

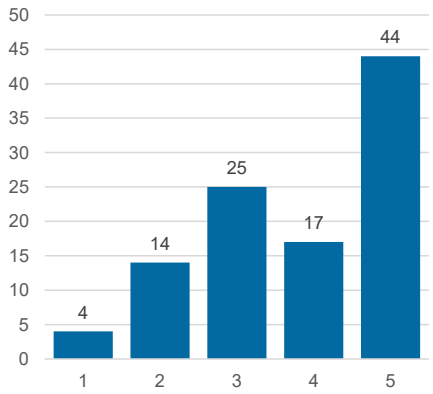
4.2.5 Área de Incidência - Dispositivos móveis

Esta área avalia os conhecimentos, as atitudes e os comportamentos dos participantes em relação à utilização de dispositivos móveis em locais públicos, nomeadamente sobre deixar os dispositivos sem vigilância, a utilização redes públicas e a espionagem visual.

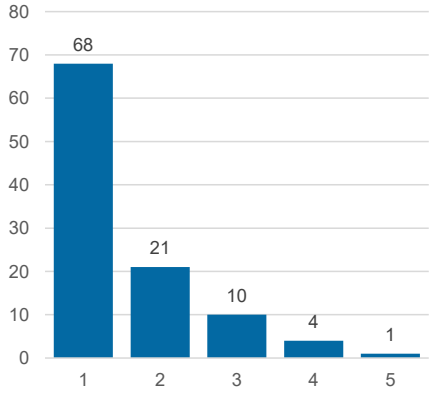
As Figuras 4.16, 4.17 e 4.18, apresentam a distribuição de respostas relativas às três subáreas descritas.

Proteger fisicamente dispositivos móveis

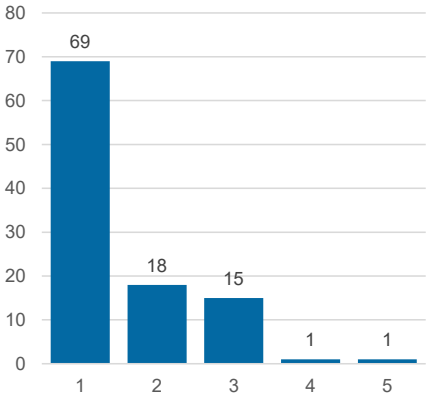
A Figura 4.16 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre deixar dispositivos sem vigilância em locais públicos.



(**a**) *Distribuição de respostas à pergunta "13.1 - Quando trabalho num local público, devo ter o meu portátil sempre comigo."*



(**b**) *Distribuição de respostas à pergunta "13.2 - Quando estou a trabalhar num café, é seguro deixar o meu portátil sem supervisão durante um minuto."*



(**c**) *Distribuição de respostas à pergunta "13.3 - Quando trabalho num local público, deixo o meu portátil sem vigilância."*

Figura 4.16: *Distribuição das respostas às questões sobre proteger fisicamente dispositivos móveis.*

A pergunta "***13.1 - Quando trabalho num local público, devo ter o meu portátil sempre comigo.***" (Figura 4.16a), das 104 respostas obtidas, 44 concordam totalmente, 17 concordam e 25 são neutras. Estes dados indicam um nível de conhecimento positivo em 58,65% das respostas, em 24,04% um nível de conhecimento neutro e em 17,31% um nível de conhecimento negativo.

Na pergunta "***13.2 - Quando estou a trabalhar num café, é seguro deixar o meu portátil sem supervisão durante um minuto.***" (Figura 4.16b), das 104 respostas obtidas, uma concorda totalmente, 4 concordam e 10 são neutras. Estes dados indicam uma atitude negativa em 4,81% das respostas, em 9,62% uma atitude neutra e em 85,58% uma atitude positiva.

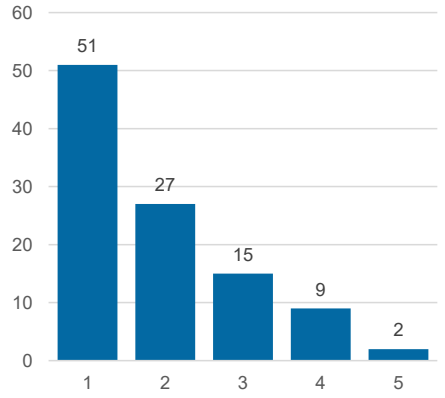
Por fim, a pergunta "***13.3 - Quando trabalho num local público, deixo o meu portátil sem vigilância.***" (Figura 4.16c), das 104 respostas obtidas, uma concorda totalmente, uma concorda e 15 são neutras. Estes dados indicam um comportamento negativo em

1,92% das respostas, em 14,42% um comportamento neutro e em 83,65% um comportamento positivo.

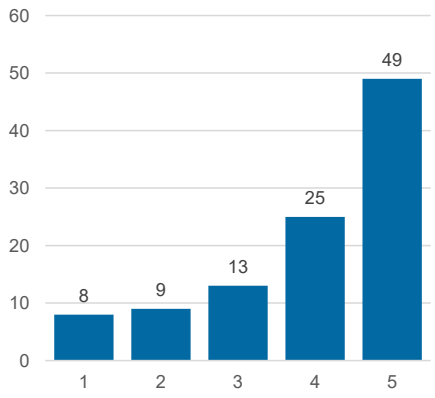
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que não se deve deixar um dispositivo sem vigilância num local público, embora alguns revelem alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria considera inseguro deixar dispositivos sem vigilância em locais públicos. Relativamente ao comportamento, a maioria afirma evitar deixar dispositivos sem vigilância em espaços públicos.

Enviar informações sensíveis por Wi-Fi

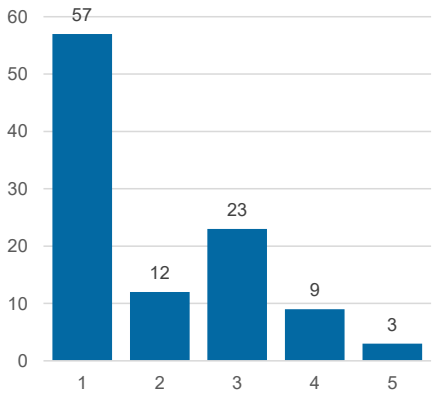
A Figura 4.17 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre a utilização de redes Wi-Fi públicas.



(**a**) *Distribuição de respostas à pergunta "14.1 - Posso enviar ficheiros de trabalho sensíveis através de uma rede Wi-Fi pública."*



(**b**) *Distribuição de respostas à pergunta "14.2 - É arriscado enviar ficheiros de trabalho sensíveis através da rede Wi-Fi pública."*



(**c**) *Distribuição de respostas à pergunta "14.3 - Envio ficheiros de trabalho sensíveis através da rede Wi-Fi pública."*

Figura 4.17: *Distribuição das respostas às questões sobre enviar informações sensíveis por Wi-Fi.*

A pergunta "***14.1 - Posso enviar ficheiros de trabalho sensíveis através de uma rede Wi-Fi pública.***" (Figura 4.17a), das 104 respostas obtidas, 2 concordam totalmente, 9 concordam e 15 são neutras. Estes dados indicam um nível de conhecimento negativo em 10,58% das respostas, em 14,42% um nível de conhecimento neutro e em 75,00% um nível de conhecimento positivo.

Na pergunta "***14.2 - É arriscado enviar ficheiros de trabalho sensíveis através da rede Wi-Fi pública.***" (Figura 4.17b), das 104 respostas obtidas, 49 concordam totalmente, 25 concordam e 13 são neutras. Estes dados indicam uma atitude positiva em 71,15% das respostas, em 12,50% uma atitude neutra e em 16,35% uma atitude negativa.

Por fim, a pergunta "***14.3 - Envio ficheiros de trabalho sensíveis através da rede Wi-Fi pública.***" (Figura 4.17c), das 104 respostas obtidas, 3 concordam totalmente, 9 concordam e 23 são neutras. Estes dados indicam um comportamento negativo em 11,54% das respostas, em 22,12% um comportamento neutro e em 66,35% um comportamento positivo.

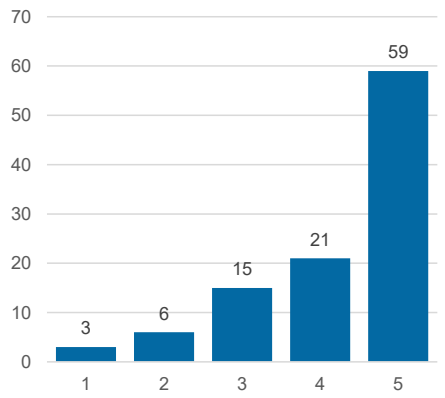
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve enviar documentos sensíveis através de redes públicas. Quanto à atitude, a esmagadora maioria dos participantes considera arriscado enviar documentos sensíveis por redes públicas. Relativamente ao comportamento, a maioria afirma que não envia documentos sensíveis através de redes públicas, mas uma parte dos participantes admite que por vezes o faz.

Espionagem Visual

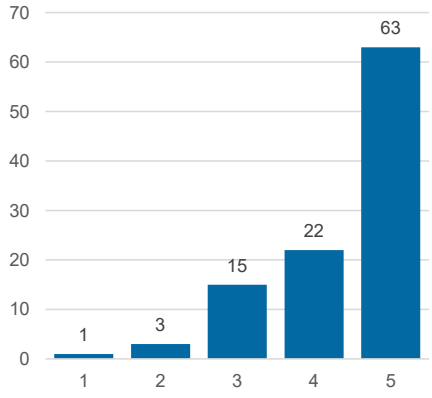
A Figura 4.18 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre a espionagem visual em locais públicos.

A pergunta "***15.1 - Ao trabalhar em um documento sensível, preciso de garantir que desconhecidos não consigam ver o ecrã do meu portátil.***" (Figura 4.18a), das 104 respostas obtidas, 59 concordam totalmente, 21 concordam e 15 são neutras. Estes dados indicam um nível de conhecimento positivo em 76,92% das respostas, em 14,42% um nível de conhecimento neutro e em 8,65% um nível de conhecimento negativo.

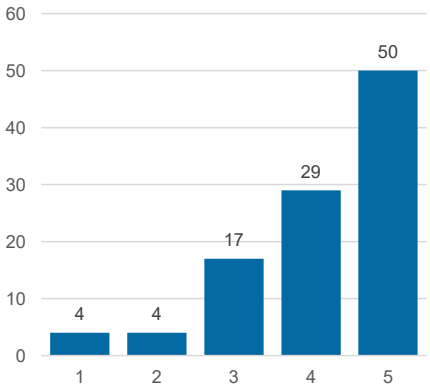
Na pergunta "***15.2 - É arriscado aceder a ficheiros de trabalho sensíveis no portátil se desconhecidos puderem ver o meu ecrã.***" (Figura 4.18b), das 104 respostas obtidas, 63 concordam totalmente, 22 concordam e 15 são neutras. Estes dados indicam uma atitude positiva em 81,73% das respostas, em 14,42% uma atitude neutra e em 3,85% uma atitude negativa.



(**a**) *Distribuição de respostas à pergunta "15.1 - Ao trabalhar em um documento sensível, preciso de garantir que desconhecidos não consigam ver o ecrã do meu portátil."*



(**b**) *Distribuição de respostas à pergunta "15.2 - É arriscado aceder a ficheiros de trabalho sensíveis no portátil se desconhecidos puderem ver o meu ecrã."*



(**c**) *Distribuição de respostas à pergunta "15.3 - Verifico se desconhecidos não conseguem ver o ecrã do meu portátil quando estou a trabalhar num documento sensível."*

Figura 4.18: *Distribuição das respostas às questões sobre espionagem visual.*

Por fim, a pergunta "***15.3 - Verifico se desconhecidos não conseguem ver o ecrã do meu portátil quando estou a trabalhar num documento sensível.***" (Figura 4.18c), das 104 respostas obtidas, 50 concordam totalmente, 29 concordam e 17 são neutras. Estes dados indicam um comportamento positivo em 75,96% das respostas, em 16,35% um comportamento neutro e em 7,69% um comportamento negativo.

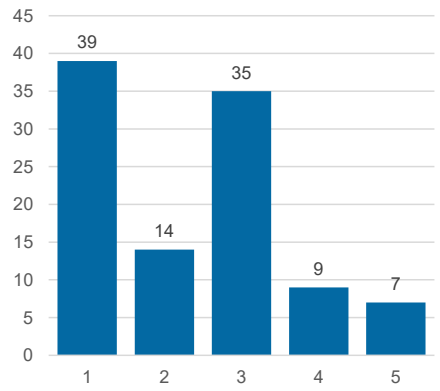
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que se deve evitar que desconhecidos vejam o ecrã ao trabalhar com documentos sensíveis. Quanto à atitude, a esmagadora maioria dos participantes considera arriscado deixar desconhecidos visualizar o ecrã ao trabalhar em documentos sensíveis. No que diz respeito ao comportamento, a esmagadora maioria afirma evitar que desconhecidos vejam o ecrã enquanto trabalham em documentos sensíveis.

4.2.6 Área de Incidência - Tratamento da informação

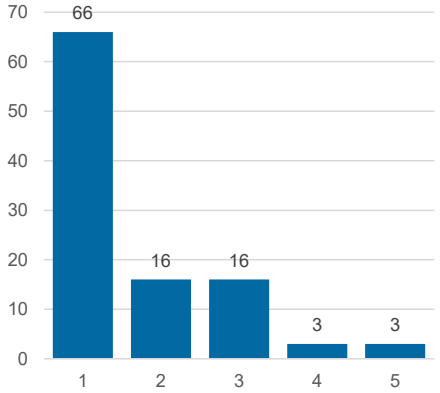
Esta área avalia os conhecimentos, as atitudes e os comportamentos, dos participantes no que diz respeito ao tratamento de informações, nomeadamente a eliminação de documentos impressos sensíveis, a utilização de dispositivos USB e exposição indevida de documentos sensíveis.
As Figuras 4.19, 4.20 e 4.21, apresentam a distribuição de respostas relativas às três subáreas descritas.

Eliminação de impressos sensíveis

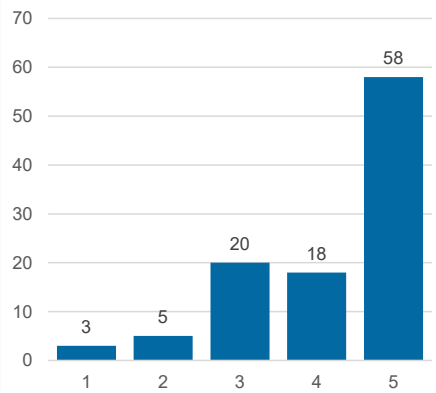
A Figura 4.19 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos em relação à eliminação de documentos impressos sensíveis.



(**a**) *Distribuição de respostas à pergunta "16.1 - Os documentos impressos sensíveis podem ser eliminados da mesma forma que os não sensíveis."*



(**b**) *Distribuição de respostas à pergunta "16.2 - É seguro deitar fora documentos impressos sensíveis, colocando-os no caixote do lixo."*



(**c**) *Distribuição de respostas à pergunta "16.3 - Quando é necessário eliminar documentos impressos sensíveis, certifico-me de que são triturados ou destruídos."*

Figura 4.19: *Distribuição das respostas às questões sobre a eliminação de documentos impressos sensíveis.*

A pergunta "***16.1 - Os documentos impressos sensíveis podem ser eliminados da mesma forma que os não sensíveis.***" (Figura 4.19a), das 104 respostas obtidas, 7 concordam totalmente, 9 concordam e 35 são neutras. Estes dados indicam um nível de conhecimento negativo em 15,38% das respostas, em 33,65% um nível de conhecimento neutro e em 50,96% um nível de conhecimento positivo.

Na pergunta "***16.2 - É seguro deitar fora documentos impressos sensíveis, colocando-os no caixote do lixo.***" (Figura 4.19b), das 104 respostas obtidas, 3 concordam totalmente, 3 concordam e 16 são neutras. Estes dados indicam uma atitude negativa em 5,77% das respostas, em 15,38% uma atitude neutra e em 78,85% uma atitude positiva.

Por fim, a pergunta "***16.3 - Quando é necessário eliminar documentos impressos sensíveis, certifico-me de que são triturados ou destruídos.***" (Figura 4.19c), das 104 respostas obtidas, 58 concordam totalmente, 18 concordam e 20 são neutras. Estes dados indicam um comportamento positivo em 73,08% das respostas, em 19,23% um comportamento neutro e em 7,69% um comportamento negativo.

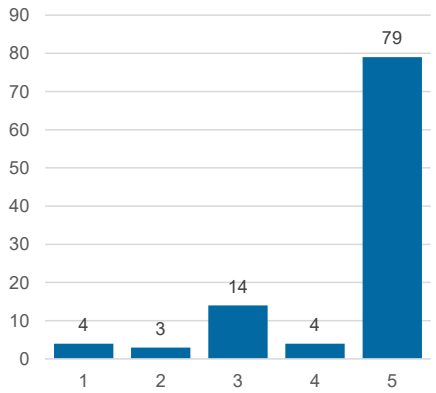
Os resultados revelam que, em termos de conhecimento, a maior parte dos participantes reconhece que documentos sensíveis não devem ser eliminados da mesma forma que os não sensíveis. No entanto, uma parte bastante significativa demonstra alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria dos participantes considera inseguro descartar documentos sensíveis sem os destruir. Relativamente ao comportamento, a esmagadora maioria dos participantes afirma que destrói os documentos sensíveis quando os descarta, mas uma parte dos participantes admite que nem sempre o faz.

Inserir suportes amovíveis

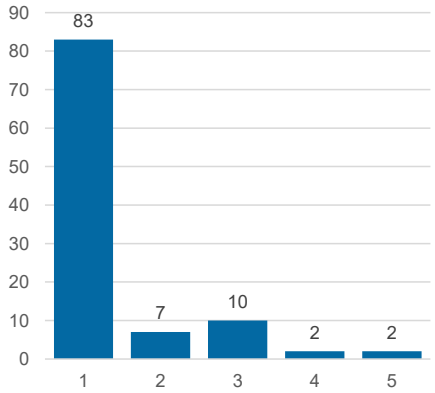
A Figura 4.20 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre a utilização de dispositivos USB.

A pergunta "***17.1 - Se eu encontrar uma pen USB num local público, não devo ligá-la ao meu computador de trabalho.***" (Figura 4.20a), das 104 respostas obtidas, 79 concordam totalmente, 4 concordam, 14 são neutras. Estes dados indicam um nível de conhecimento positivo em 79,81% das respostas, em 13,46% um nível conhecimento neutro e em 6,73% um nível de conhecimento negativo.

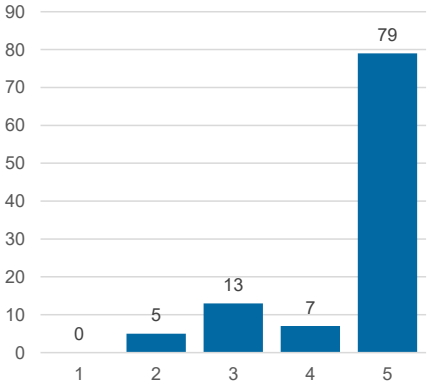
Na pergunta "***17.2 - Se eu encontrar uma pen USB num local público, nada de mal pode acontecer se a ligar ao meu computador de trabalho.***" (Figura 4.20b), das 104 respostas obtidas, 2 concordam totalmente, 2 concordam e 10 são neutras. Estes dados indicam uma atitude negativa em 3,85% das respostas, em 9,62% uma atitude neutra e em 86,54% uma atitude positiva.



(**a**) *Distribuição de respostas à pergunta "17.1 - Se eu encontrar uma pen USB num local público, não devo ligá-la ao meu computador de trabalho."*



(**b**) *Distribuição de respostas à pergunta "17.2 - Se eu encontrar uma pen USB num local público, nada de mal pode acontecer se a ligar ao meu computador de trabalho."*



(**c**) *Distribuição de respostas à pergunta "17.3 - Eu não ligaria uma pen USB encontrada num local público ao meu computador de trabalho."*

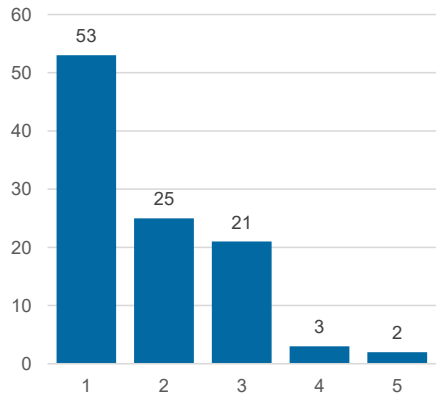
Figura 4.20: *Distribuição das respostas às questões sobre utilizar dispositivos desconhecidos.*

Por fim, a pergunta "***17.3 - Eu não ligaria uma pen USB encontrada num local público ao meu computador de trabalho.***" (Figura 4.20c), das 104 respostas obtidas, 79 concordam totalmente, 7 concordam e 13 são neutras. Estes dados indicam um comportamento positivo em 82,69% das respostas, em 12,50% um comportamento neutro e em 4,81% um comportamento negativo.

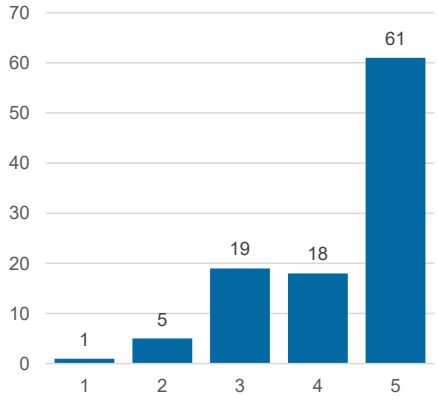
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve utilizar dispositivos USB desconhecidos. Quanto à atitude, a esmagadora maioria dos participantes considera inseguro utilizar dispositivos USB de origem desconhecida. Relativamente ao comportamento, a esmagadora maioria dos participantes afirma que não utiliza dispositivos USB desconhecidos.

Deixar material sensível

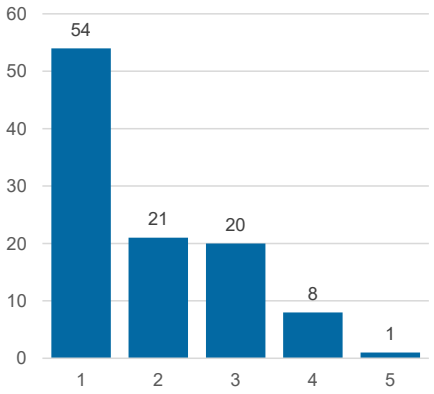
A Figura 4.21 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre deixar documento impressos sensíveis expostos.



(**a**) *Distribuição de respostas à pergunta "18.1 - Posso deixar documentos impressos com informações sensíveis na minha secretária durante a noite."*



(**b**) *Distribuição de respostas à pergunta "18.2 - É arriscado deixar documentos impressos que contenham informações sensíveis na minha secretária durante a noite."*



(**c**) *Distribuição de respostas à pergunta "18.3 - Deixo documentos impressos que contêm informações sensíveis na minha secretária quando não estou lá."*

Figura 4.21: *Distribuição das respostas às questões sobre deixar documentos sensíveis expostos.*

A pergunta "***18.1 - Posso deixar documentos impressos com informações sensíveis na minha secretária durante a noite.***" (Figura 4.21a), das 104 respostas obtidas, 2 concordam totalmente, 3 concordam e 21 são neutras. Estes dados indica um nível de conhecimento negativo em 4,81% das respostas, em 20,19% um nível de conhecimento neutro e em 75,00% um nível de conhecimento positivo.

Na pergunta "***18.2 - É arriscado deixar documentos impressos que contenham informações sensíveis na minha secretária durante a noite.***" (Figura 4.21b), das 104 respostas obtidas, 61 concordam totalmente, 18 concordam e 19 são neutras. Estes dados indi-

cam uma atitude positiva em 75,96% das respostas, em 18,27% uma atitude neutra e em 5,77% uma atitude negativa.

Por fim, a pergunta "***18.3 - Deixo documentos impressos que contêm informações sensíveis na minha secretária quando não estou lá.***" (Figura 4.21c), das 104 respostas obtidas, uma concorda totalmente, 8 concordam e 20 são neutras. Estes dados indicam um comportamento negativo em 8,65% das respostas, em 19,23% um comportamento neutro e em 72,12% um comportamento positivo.

Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve deixar documentos sensíveis expostos na secretária, mas alguns participantes demonstram algumas dúvidas neste aspeto. Quanto à atitude, a esmagadora maioria dos participantes considera inseguro deixar este tipo de documentos na secretária, enquanto alguns participantes não veem problemas em o fazer. No que diz respeito ao comportamento, a esmagadora maioria afirma não deixar documentos sensíveis na secretária sem vigilância. No entanto, alguns participantes admitem que por vezes o fazem.

4.2.7 Área de Incidência - Comunicação de incidentes

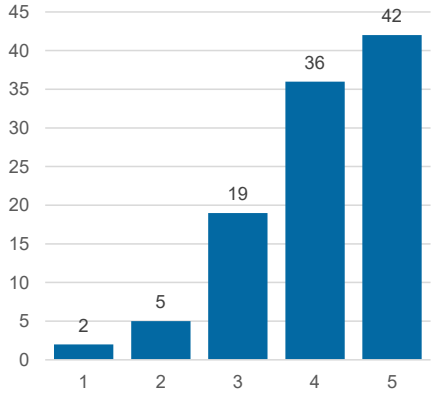
Esta área avalia os conhecimentos, as atitudes e os comportamentos dos participantes relativamente à comunicação de incidentes, nomeadamente a comunicação de comportamentos suspeitos, os comportamentos negligentes nas medidas de segurança por parte de colegas e a comunicação de incidentes de segurança.
As Figuras 4.22, 4.23 e 4.24, apresentam a distribuição de respostas relativas às três subáreas descritas.

Comunicar comportamentos suspeitos

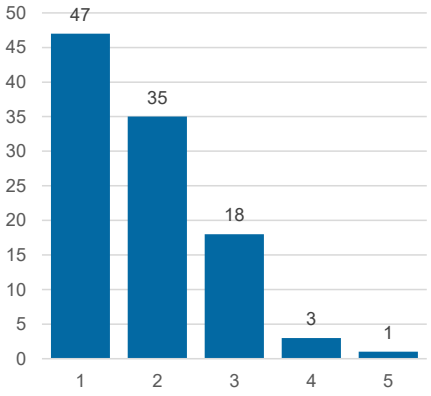
A Figura 4.22 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos em relação à comunicação de comportamentos suspeitos.

A pergunta "***19.1 - Se eu vir alguém a agir de forma suspeita no meu local de trabalho, devo comunicá-lo.***" (Figura 4.22a), das 104 respostas obtidas, 42 concordam totalmente, 36 concordam e 19 são neutras. Estes dados indicam um nível de conhecimento positivo em 75,00% das respostas, em 18,27% um nível de conhecimento neutro e em 6,73% um nível de conhecimento negativo.

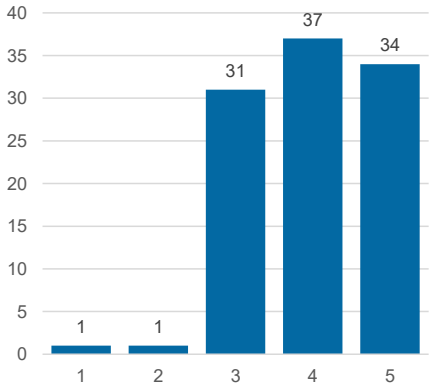
Na pergunta "***19.2 - Se eu ignorar alguém que está a agir de forma suspeita no meu local de trabalho, nada de mal pode acontecer.***" (Figura 4.22b), das 104 respostas obtidas, uma concorda totalmente, 3 concordam e 18 são neutras. Estes dados indicam uma atitude negativa em 3,85% das respostas, em 17,31% uma atitude neutra e em 78,85% uma atitude positiva.



(**a**) *Distribuição de respostas à pergunta "19.1 - Se eu vir alguém a agir de forma suspeita no meu local de trabalho, devo comunicá-lo."*



(**b**) *Distribuição de respostas à pergunta "19.2 - Se eu ignorar alguém que está a agir de forma suspeita no meu local de trabalho, nada de mal pode acontecer."*



(**c**) *Distribuição de respostas à pergunta "19.3 - Se eu visse alguém a agir de forma suspeita no meu local de trabalho, faria alguma coisa."*

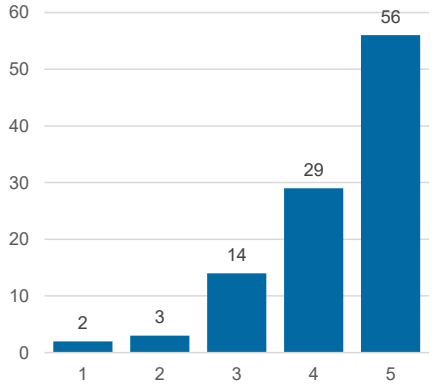
Figura 4.22: *Distribuição das respostas às questões sobre comunicar comportamentos suspeitos.*

Por fim, a pergunta "***19.3 - Se eu visse alguém a agir de forma suspeita no meu local de trabalho, faria alguma coisa.***" (Figura 4.22c), das 104 respostas obtidas, 34 concordam totalmente, 37 concordam e 31 são neutras. Estes dados indicam um comportamento positivo em 68,27% das respostas, em 29,81% um comportamento neutro e em 1,92% um comportamento negativo.

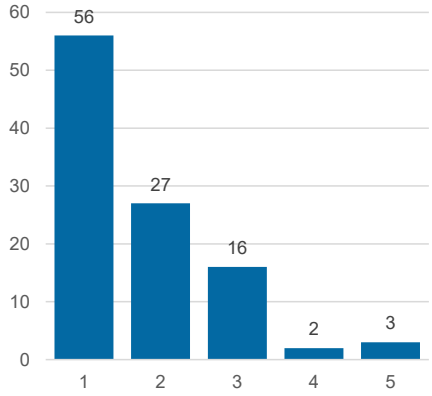
Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece a importância de comunicar comportamentos suspeitos, embora alguns ainda revelem alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria considera que ignorar comportamentos suspeitos pode ser perigoso, mas alguns participantes não vem problemas em o fazer. Relativamente ao comportamento, a maior parte dos participantes afirma que comunicaria um comportamento suspeito. No entanto, uma parte significativa dos participantes admite que talvez não o faria.

Ignorar comportamentos de segurança inadequados de colegas

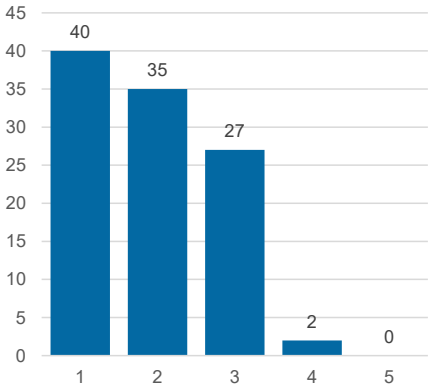
A Figura 4.23 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos em relação à negligência no cumprimento das práticas de segurança.



(**a**) *Distribuição de respostas à pergunta "20.1 - Não devo ignorar comportamentos inadequados de segurança dos meus colegas."*



(**b**) *Distribuição de respostas à pergunta "20.2 - Nada de mal pode acontecer se eu ignorar o comportamento inadequado de segurança de um colega."*



(**c**) *Distribuição de respostas à pergunta "20.3 - Se eu visse um colega a ignorar as regras de segurança, não tomaria qualquer medida."*

Figura 4.23: *Distribuição das respostas às questões sobre ignorar comportamentos de segurança.*

A pergunta "***20.1 - Não devo ignorar comportamentos inadequados de segurança dos meus colegas.***" (Figura 4.23a), das 104 respostas obtidas, 56 concordam totalmente, 29 concordam e 14 são neutras. Estes dados indicam um nível de conhecimento positivo em 81,73% das respostas, em 13,46% um nível de conhecimento neutro e em 4,81% um nível de conhecimento negativo.

Na pergunta "***20.2 - Nada de mal pode acontecer se eu ignorar o comportamento inadequado de segurança de um colega.***" (Figura 4.23b), das 104 respostas obtidas, 3 concordam totalmente, 2 concordam e 16 são neutras. Estes dados indicam uma atitude negativa em 4,81% das respostas, em 15,38% uma atitude neutra e em 79,81% uma ati-

tude positiva.

Por fim, a pergunta *"**20.3 - Se eu visse um colega a ignorar as regras de segurança, não tomaria qualquer medida.**"* (Figura 4.23c), das 104 respostas obtidas, nenhuma concorda totalmente, 2 concordam e 27 são neutras. Estes dados indicam um comportamento negativo em 1,92% das respostas, em 25,96% um comportamento neutro e em 72,12% um comportamento positivo.

Os resultados revelam que, em termos de conhecimento, a esmagadora maioria dos participantes reconhece que não se deve ignorar os comportamentos inadequados de segurança dos colegas. Quanto à atitude, a esmagadora maioria considera que ignorar os comportamentos inadequados de segurança dos colegas pode ser perigoso. No que diz respeito ao comportamento, a maioria dos participantes afirma que faria algo se observasse um colega a desrespeitar as medidas de segurança. No entanto, uma parte dos participantes admite que talvez não o faria.

Comunicar todos os incidentes

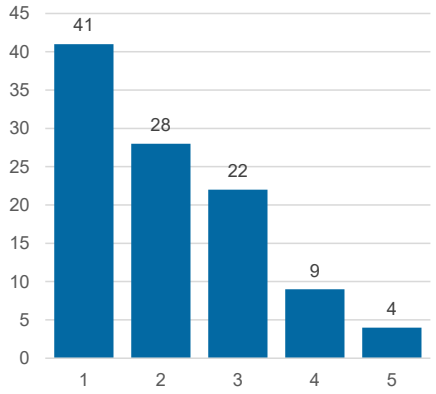
A Figura 4.24 apresenta a distribuição das respostas às três perguntas destinadas a avaliar os conhecimentos, as atitudes e os comportamentos sobre a comunicação de incidentes de segurança.

A pergunta *"**21.1 - É opcional comunicar incidentes de segurança.**"* (Figura 4.24a), das 104 respostas obtidas, 4 concordam totalmente, 9 concordam e 22 são neutras. Estes dados indicam um nível de conhecimento negativo em 12,50% das respostas, em 21,15% um nível de conhecimento neutro e em 66,35% um nível de conhecimento positivo.

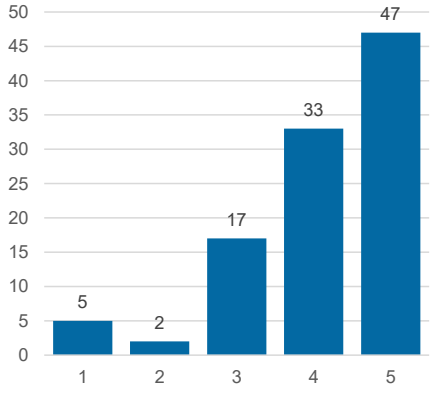
Na pergunta *"**21.2 - É arriscado ignorar os incidentes de segurança, mesmo que eu ache que não são significativos.**"* (Figura 4.24b), das 104 respostas obtidas, 47 concordam totalmente, 33 concordam e 17 são neutras. Estes dados indicam uma atitude positiva em 76,92% das respostas, em 16,35% uma atitude neutra e em 6,73% uma atitude negativa.

Por fim, a pergunta *"**21.3 - Se me apercebesse de um incidente de segurança, comunicá-lo-ia.**"* (Figura 4.24c), das 104 respostas obtidas, 56 concordam totalmente, 25 concordam e 21 são neutras. Estes dados indicam um comportamento positivo em 77,88% das respostas, em 20,19% um comportamento neutro e em 1,92% um comportamento negativo.

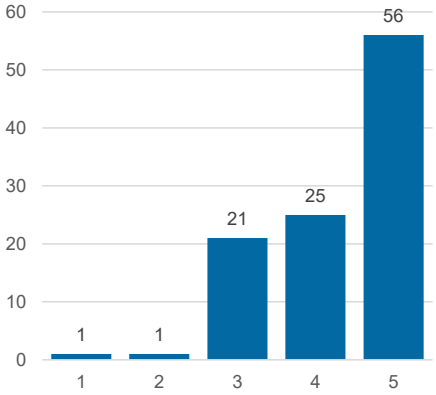
Os resultados revelam que, em termos de conhecimento, a maioria dos participantes reconhece que se deve comunicar os incidentes de segurança, mas alguns ainda revelam alguma incerteza neste aspeto. Quanto à atitude, a esmagadora maioria considera arriscado ignorar incidentes de segurança. Relativamente ao comportamento, a esmagadora maioria dos participantes afirma que comunicaria um incidente de segurança. No entanto, uma parte dos participantes admite incerteza em relação ao que faria.



(**a**) *Distribuição de respostas à pergunta "21.1 - É opcional comunicar incidentes de segurança."*



(**b**) *Distribuição de respostas à pergunta "21.2 - É arriscado ignorar os incidentes de segurança, mesmo que eu ache que não são significativos."*



(**c**) *Distribuição de respostas à pergunta "21.3 - Se me apercebesse de um incidente de segurança, comunicá-lo-ia."*

Figura 4.24: *Distribuição das respostas às questões sobre comunicar incidentes.*

4.3 Discussão de Resultados

Esta secção descreve a análise realizada com o objetivo de responder às questões de investigação deste estudo. Para tal, recorreu-se ao programa de análise estatistica IBM SPSS[1] (versão 29.0.1.0).

Os itens foram respondidos com uma escala de *Likert* de 5 pontos. As respostas com classificação igual ou superior a 4 foram consideradas positivas, as classificadas com 3 foram consideradas neutras, e as inferiores a 3 foram consideradas negativas. No entanto, nas questões de resposta inversa, foi necessário recodificar os valores para garantir a coerência da análise. Para isso, utilizou-se a funcionalidade "*Recode into Same Variables: Old and New Values*" do SPSS, onde foram atribuídos os valores invertidos correspondentes.

[1] IBM SPSS: `https://www.ibm.com/products/spss-statistics`

Com o intuito de facilitar a análise dos dados, foram criadas variáveis com os valores médios, através da funcionalidade "*Compute Variable*" do SPSS. Para cada área de incidência, foram criadas variáveis que representam: a média geral das respostas, a média das respostas relacionadas com o conhecimento, com a atitude e com o comportamento. Adicionalmente, para cada subárea foi criada uma variável correspondente à média geral das respostas dessa subárea.

De forma global, relativamente ao questionário, foram ainda criadas variáveis que refletem: a média geral das respostas, a média geral ao nível do conhecimento, da atitude e do comportamento.

A análise realizada para responder às questões de investigação foi estruturada em dois grupos. O primeiro consistiu numa análise baseada no público-alvo que respondeu ao questionário, agrupando as respostas por cada grupo de participantes, com o objetivo de comparar os resultados entre os diferentes grupos. O segundo correspondeu a uma análise global das respostas, com o intuito de comparar os resultados entre as diferentes áreas de incidência abordadas no questionário.

4.3.1 Análise por Público-alvo

Esta análise teve como objetivo identificar diferenças nas respostas entre os diversos grupos de participantes, de forma a responder às seguintes questões de investigação:

1. Qual o curso que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?
2. Qual o ano curricular que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?
3. Existem indícios de que estudantes mais velhos adotam melhores práticas de cibersegurança?
4. Existe algum indicador que relacione o sexo dos estudantes com a adoção de melhores práticas de cibersegurança?
5. Estudantes que não ingressaram no ensino superior pelo CNAES demonstram melhores práticas de cibersegurança?
6. O percurso académico do ensino secundário influencia as práticas de cibersegurança adotadas pelos estudantes?

Para responder a estas questões, recorreu-se à funcionalidade "*Compare Means and Proportions*" do SPSS, tendo sido selecionada a opção de comparação por médias.

Na Tabela 4.1 são apresentados os resultados da análise, organizados por curso dos participantes.

Área	AP (D)	CF (D)	Gestão (D)	Gestão (PL)	Marketing (D)	Sol (D)	Sol (PL)
Gestão de Palavras-passe	**4,12**	**4,35**	**4,21**	**4,65**	**4,25**	**4,18**	**4,78**
Utilizar a mesma palavra-passe	3,96	4,47	3,93	4,72	3,98	3,67	5,00
Partilhar palavras-passe	4,27	4,36	4,33	4,44	4,50	4,73	4,33
Utilizar uma palavra-passe forte	4,14	4,22	4,36	4,78	4,28	4,13	5,00
Utilização do Email	**4,31**	**4,29**	**4,22**	**4,15**	**4,23**	**4,40**	**4,50**
Clicar em links de emails enviados por remetentes conhecidos	3,94	4,39	4,06	3,67	4,00	3,73	4,17
Clicar em links de emails enviados por remetentes desconhecidos	4,59	4,42	4,36	4,50	4,63	4,67	5,00
Abrir anexos de emails enviados por remetentes desconhecidos	4,41	4,06	4,24	4,28	4,07	4,80	4,33
Utilização da Internet	**4,05**	**4,25**	**4,07**	**4,11**	**3,91**	**3,93**	**4,22**
Transferir ficheiros	3,75	3,94	4,04	3,61	3,69	3,47	4,17
Aceder a websites duvidosos	4,31	4,56	4,09	4,56	4,19	4,67	4,67
Introduzir informações online	4,08	4,25	4,07	4,17	3,85	3,67	3,83
Utilização de redes sociais	**4,24**	**3,95**	**4,02**	**4,00**	**3,99**	**4,16**	**4,83**
Definições de privacidade das redes sociais	3,71	3,72	3,84	3,72	3,80	4,07	5,00
Considerar consequências	4,22	3,64	4,00	3,89	3,70	4,07	4,50
Publicar sobre o trabalho	4,78	4,50	4,23	4,39	4,48	4,33	5,00
Dispositivos móveis	**4,41**	**4,28**	**4,10**	**4,41**	**3,85**	**4,40**	**4,94**
Proteger fisicamente dispositivos móveis	4,51	4,22	4,20	4,39	3,98	4,27	4,83
Enviar informações sensíveis por Wi-Fi	4,10	4,19	4,05	4,56	3,50	4,33	5,00
Espionagem Visual	4,61	4,42	4,04	4,28	4,07	4,60	5,00
Tratamento de informações	**4,54**	**4,47**	**4,04**	**4,76**	**4,17**	**4,49**	**4,50**
Eliminação de impressos sensíveis	4,51	4,25	3,86	4,50	3,83	3,80	5,00
Inserir suportes amovíveis	4,82	4,89	4,14	5,00	4,67	4,93	5,00
Deixar material sensível	4,27	4,28	4,14	4,78	4,00	4,73	3,50
Comunicação de incidentes	**4,39**	**4,19**	**3,94**	**4,15**	**4,14**	**4,47**	**4,83**
Comunicar comportamentos suspeitos	4,16	4,14	3,90	4,17	4,17	4,47	5,00

Ignorar comportamentos de segurança inadequados de colegas	4,55	4,17	4,03	3,94	4,31	4,47	4,83
Comunicar todos os incidentes	4,45	4,28	3,88	4,33	3,93	4,47	4,67
Média	**4,29**	**4,26**	**4,08**	**4,32**	**4,08**	**4,29**	**4,66**
Total Respostas	**17**	**12**	**44**	**6**	**18**	**5**	**2**
AP - Administração Pública; CF - Contabilidade e Finanças; Sol - Solicitadoria; D - Diurno; PL - Pós-laboral							

Tabela 4.1: *Resultados médios por curso em cada área e subárea do questionário.*

Analisando os resultados obtidos, verificou-se uma quantidade de respostas bastante distinta entre os diferentes cursos, o que dificultou a realização de uma análise comparativa consistente. Ainda assim, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- O curso de **Administração Pública** teve 17 respostas, com uma média geral de respostas de 4,29. A média mais alta foi na área "Tratamento de Informações" (4,59) e a média mais baixa foi na área "Utilização da Internet" (4,05).
- O curso de **Contabilidade e Finanças** teve 12 respostas, com uma média geral de respostas de 4,26. A média mais alta foi na área "Tratamento de Informações" (4,47) e a média mais baixa foi na área "Utilização de Redes Sociais" (3,95).
- O curso de **Gestão (Diurno)** teve 44 respostas, com uma média geral de respostas de 4,08. A média mais alta foi na área "Utilização do Email" (4,22) e a média mais baixa foi na área "Comunicação de Incidentes" (3,94).
- O curso de **Gestão (Pós-laboral)** teve 6 respostas, com uma média geral de respostas de 4,32. A média mais alta foi na área "Tratamento de Informações" (4,76) e a média mais baixa foi na área "Utilização de Redes Sociais" (4,00).
- O curso de **Marketing** teve 18 respostas, com uma média geral de respostas de 4,08. A média mais alta foi na área "Gestão de Palavras-passe" (4,25) e a média mais baixa foi na área "Dispositivos Móveis" (3,85).
- O curso de **Solicitadoria (Diurno)** teve 5 respostas, com uma média geral de respostas de 4,29. A média mais alta foi na área "Tratamento de Informações" (4,49) e a média mais baixa foi na área de "Utilização da Internet" (3,93).
- O curso de **Solicitadoria (Pós-laboral)** teve 2 respostas, com uma média geral de 4,66. A média mais alta foi na área "Dispositivos Móveis" (4,94) e a média mais baixa foi na área "Utilização da Internet" (4,22).

De forma geral, todos os cursos apresentaram médias superiores a 4, o que indica uma perceção globalmente positiva relativamente às práticas de cibersegurança. Os cursos de Gestão (Diurno) e Marketing registaram as médias gerais mais baixas (4,08), enquanto o curso de Solicitadoria (Pós-laboral) obteve a média mais elevada (4,66).

Contudo, devido à grande disparidade no número de respostas entre os cursos, não é possível realizar uma comparação totalmente fiável. Assim, não se pode responder de forma conclusiva à questão de investigação ´´***Qual o curso que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?***".

Na Tabela 4.2 são apresentados os resultados da análise realizada com base no ano curricular dos participantes.

Área	1º Ano	2º Ano	3º Ano
Gestão de Palavras-passe	**4,23**	**4,25**	**4,29**
Utilizar a mesma palavra-passe	4,05	4,08	4,03
Partilhar palavras-passe	4,36	4,39	4,38
Utilizar uma palavra-passe forte	4,28	4,28	4,45
Utilização do Email	**4,30**	**4,19**	**4,37**
Clicar em links de emails enviados por remetentes conhecidos	4,00	3,98	4,20
Clicar em links de emails enviados por remetentes desconhecidos	4,65	4,39	4,53
Abrir anexos de emails enviados por remetentes desconhecidos	4,26	4,20	4,38
Utilização da Internet	**4,06**	**4,04**	**4,09**
Transferir ficheiros	3,74	3,92	3,89
Aceder a websites duvidosos	4,33	4,18	4,38
Introduzir informações online	4,09	4,02	4,02
Utilização de redes sociais	**4,17**	**4,00**	**4,11**
Definições de privacidade das redes sociais	3,94	3,84	3,65
Considerar consequências	3,99	3,85	4,15
Publicar sobre o trabalho	4,59	4,30	4,53
Dispositivos móveis	**4,36**	**4,13**	**4,08**
Proteger fisicamente dispositivos móveis	4,35	4,25	4,09
Enviar informações sensíveis por Wi-Fi	4,17	4,02	3,95
Espionagem Visual	4,56	4,11	4,20
Tratamento de informações	**4,39**	**4,15**	**4,40**
Eliminação de impressos sensíveis	4,19	3,96	4,15
Inserir suportes amovíveis	4,79	4,35	4,70
Deixar material sensível	4,19	4,15	4,36
Comunicação de incidentes	**4,26**	**4,01**	**4,29**
Comunicar comportamentos suspeitos	4,18	3,98	4,23
Ignorar comportamentos de segurança inadequados de colegas	4,41	4,05	4,39

Comunicar todos os incidentes	4,18	3,99	4,26
Média	**4,25**	**4,11**	**4,23**
Total Respostas	**26**	**56**	**22**

Tabela 4.2: *Resultados médios por ano curricular em cada área e subárea do questionário.*

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- O **1º ano curricular** teve 26 respostas, com uma média geral de respostas de 4,25. A média mais alta foi na área "Tratamento de Informações" (4,39) e a média mais baixa foi na área "Utilização Internet" (4,06).
- O **2º ano curricular** teve 56 respostas, com uma média geral de respostas de 4,11. A média mais alta foi na área "Gestão de Palavras-passe" (4,25) e a média mais baixa foi na área "Utilização de redes sociais" (4,00).
- O **3º ano curricular** teve 22 respostas, com uma média geral de respostas de 4,23. A média mais alta foi na área "Tratamento de Informações" (4,40) e a média mais baixa foi na área "Dispositivos Móveis" (4,08).

De forma geral, todos os anos curriculares apresentaram médias superiores a 4, o que indica uma perceção positiva relativamente às práticas de cibersegurança. O 1º ano curricular registou a média mais elevada (4,25), enquanto o 2º ano obteve a média mais baixa (4,11).

Assim, com base nos dados analisados, a resposta à questão de investigação "***Qual o ano curricular que apresenta mais pontos positivos e negativos em relação às práticas de cibersegurança?***" é, nesta amostra de dados, o 1º ano curricular que revela uma adoção mais positiva das práticas de cibersegurança, enquanto o 2º ano evidencia uma maior necessidade de implementação de estratégias de sensibilização.

Na Tabela 4.3 são apresentados os resultados da análise efetuada segundo as faixas etárias dos participantes.

Área	18 aos 21 anos	22 aos 25 anos	26 anos ou mais
Gestão de Palavras-passe	**4,18**	**4,39**	**4,44**
Utilizar a mesma palavra-passe	3,93	4,17	4,57
Partilhar palavras-passe	4,41	4,46	4,19
Utilizar uma palavra-passe forte	4,21	4,54	4,56
Utilização do Email	**4,25**	**4,19**	**4,33**
Clicar em links de emails enviados por remetentes conhecidos	4,02	4,02	4,10
Clicar em links de emails enviados por remetentes desconhecidos	4,47	4,48	4,58

Abrir anexos de emails enviados por remetentes desconhecidos	4,27	4,08	4,31
Utilização da Internet	**4,07**	**4,00**	**4,04**
Transferir ficheiros	3,94	3,73	3,71
Aceder a websites duvidosos	4,19	4,46	4,38
Introduzir informações online	4,08	3,81	4,04
Utilização de redes sociais	**4,04**	**4,10**	**4,16**
Definições de privacidade das redes sociais	3,83	3,71	3,92
Considerar consequências	3,93	4,04	3,96
Publicar sobre o trabalho	4,36	4,54	4,60
Dispositivos móveis	**4,12**	**4,10**	**4,48**
Proteger fisicamente dispositivos móveis	4,24	4,06	4,44
Enviar informações sensíveis por Wi-Fi	3,93	4,08	4,50
Espionagem Visual	4,20	4,17	4,50
Tratamento de informações	**4,15**	**4,34**	**4,67**
Eliminação de impressos sensíveis	3,91	4,38	4,44
Inserir suportes amovíveis	4,41	4,67	4,94
Deixar material sensível	4,16	3,98	4,65
Comunicação de incidentes	**4,12**	**4,02**	**4,26**
Comunicar comportamentos suspeitos	4,06	4,02	4,25
Ignorar comportamentos de segurança inadequados de colegas	4,25	4,06	4,19
Comunicar todos os incidentes	4,06	3,98	4,35
Média	**4,14**	**4,16**	**4,34**
Total Respostas	**72**	**16**	**16**

Tabela 4.3: *Resultados médios por faixa etária em cada área e subárea do questionário.*

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- A faixa etária dos **18 aos 21 anos** teve 72 respostas, com uma média geral de respostas de 4,14. A média mais alta foi na área "Utilização do Email" (4,25) e a média mais baixa foi na área "Utilização da Internet" (4,07).
- A faixa etária dos **22 aos 25 anos** teve 16 respostas, com uma média geral de respostas de 4,16. A média mais alta foi na área "Gestão de Palavras-passe" (4,39) e a média mais baixa foi na área "Utilização da Internet" (4,00).
- A faixa etária de **26 anos ou mais** teve 16 respostas, com uma média geral de respostas de 4,34. A média mais alta foi na área "Tratamento de Informações" (4,67) e a média mais baixa foi na área "Utilização da Internet" (4,04).

De forma geral, todas as faixas etárias apresentaram médias superiores a 4, o que indica uma perceção positiva relativamente às práticas de cibersegurança. A faixa etária dos 26 anos ou mais registou a média mais elevada (4,34), enquanto a faixa etária dos 18 aos 21 anos apresentou a média mais baixa (4,14).

Assim, com base nos dados analisados, a resposta à questão de investigação "***Existem indícios de que estudantes mais velhos adotam melhores práticas de cibersegurança?***" é afirmativa, nesta amostra de dados, os estudantes mais velhos demonstram uma adoção mais positiva das práticas de cibersegurança.

Na Tabela 4.4 são apresentados os resultados da análise segundo o sexo dos participantes.

Área	Feminino	Masculino
Gestão de Palavras-passe	**4,29**	**4,18**
Utilizar a mesma palavra-passe	4,04	4,11
Partilhar palavras-passe	4,47	4,19
Utilizar uma palavra-passe forte	4,36	4,22
Utilização do Email	**4,33**	**4,08**
Clicar em links de emails enviados por remetentes conhecidos	4,00	4,11
Clicar em links de emails enviados por remetentes desconhecidos	4,64	4,15
Abrir anexos de emails enviados por remetentes desconhecidos	4,37	3,99
Utilização da Internet	**4,07**	**4,02**
Transferir ficheiros	3,81	3,99
Aceder a websites duvidosos	4,37	4,03
Introduzir informações online	4,03	4,04
Utilização de redes sociais	**4,17**	**3,85**
Definições de privacidade das redes sociais	3,90	3,66
Considerar consequências	4,02	3,80
Publicar sobre o trabalho	4,58	4,08
Dispositivos móveis	**4,29**	**3,92**
Proteger fisicamente dispositivos móveis	4,33	4,04
Enviar informações sensíveis por Wi-Fi	4,12	3,87
Espionagem Visual	4,42	3,85
Tratamento de informações	**4,40**	**3,97**
Eliminação de impressos sensíveis	4,15	3,87
Inserir suportes amovíveis	4,73	4,10

Deixar material sensível	4,33	3,94
Comunicação de incidentes	**4,22**	**3,93**
Comunicar comportamentos suspeitos	4,16	3,90
Ignorar comportamentos de segurança inadequados de colegas	4,31	4,01
Comunicar todos os incidentes	4,20	3,88
Média	**4,25**	**3,99**
Total Respostas	**71**	**33**

Tabela 4.4: *Resultados médios por sexo em cada área e subárea do questionário.*

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- Do sexo **feminino** existiram 71 respostas, com uma média geral de respostas de 4,25. A média mais alta foi na área "Tratamento de Informações" (4,40) e a média mais baixa foi na área "Utilização da Internet" (4,07).
- Do sexo **masculino** existiram 33 respostas, com uma média geral de respostas de 3,99. A média mais alta foi na área "Gestão de Palavras-passe" (4,18) e a média mais baixa foi na área "Utilização de Redes Sociais" (3,85).

De forma geral, os participantes do sexo feminino apresentaram uma média de respostas superior a 4, o que indica uma perceção positiva relativamente às práticas de cibersegurança. Por outro lado, os participantes do sexo masculino registaram uma média inferior a 4, sugerindo uma perceção ligeiramente menos positiva.

Assim, com base nos dados analisados, a resposta à questão de investigação "***Existe algum indicador que relacione o sexo dos estudantes com a adoção de melhores práticas de cibersegurança?***" é afirmativa, nesta amostra de dados, os estudantes do sexo feminino demonstram uma adoção mais positiva das práticas de cibersegurança.

Na Tabela 4.5 são apresentados os resultados da análise segundo o tipo de ingresso no ensino superior dos participantes.

Área	CNAES	Outros
Gestão de Palavras-passe	**4,16**	**4,51**
Utilizar a mesma palavra-passe	3,89	4,51
Partilhar palavras-passe	4,39	4,36
Utilizar uma palavra-passe forte	4,19	4,65
Utilização do Email	**4,25**	**4,26**
Clicar em links de emails enviados por remetentes conhecidos	4,04	4,02
Clicar em links de emails enviados por remetentes desconhecidos	4,47	4,51

Abrir anexos de emails enviados por remetentes desconhecidos	4,25	4,24
Utilização da Internet	**4,04**	**4,09**
Transferir ficheiros	3,91	3,75
Aceder a websites duvidosos	4,21	4,39
Introduzir informações online	4,00	4,13
Utilização de redes sociais	**4,00**	**4,25**
Definições de privacidade das redes sociais	3,74	4,05
Considerar consequências	3,91	4,06
Publicar sobre o trabalho	4,35	4,63
Dispositivos móveis	**4,08**	**4,44**
Proteger fisicamente dispositivos móveis	4,17	4,43
Enviar informações sensíveis por Wi-Fi	3,93	4,33
Espionagem Visual	4,12	4,56
Tratamento de informações	**4,15**	**4,58**
Eliminação de impressos sensíveis	3,93	4,40
Inserir suportes amovíveis	4,40	4,89
Deixar material sensível	4,12	4,44
Comunicação de incidentes	**4,05**	**4,35**
Comunicar comportamentos suspeitos	3,96	4,40
Ignorar comportamentos de segurança inadequados de colegas	4,18	4,29
Comunicar todos os incidentes	4,00	4,37
Média	**4,10**	**4,35**
Total Respostas	**76**	**28**

Tabela 4.5: *Resultados médios por tipo de ingresso em cada área e subárea do questionário.*

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- O ingresso no ensino superior pelo **CNAES** teve 76 respostas, com uma média geral de respostas de 4,10. A média mais alta foi na área "Utilização do Email" (4,25) e a média mais baixa foi na área "Utilização de Redes Sociais" (4,00).
- O ingresso no ensino superior por **outros** métodos teve 28 respostas, com uma média geral de respostas de 4,35. A média mais alta foi na área "Tratamento de Informações" (4,58) e a média mais baixa foi na área "Utilização da Internet" (4,09).

De forma geral, os participantes de ambos os tipos de ingresso no ensino superior apresentaram médias superiores a 4, indicando uma perceção positiva relativamente às práticas de cibersegurança.

Assim, com base nos dados analisados, a resposta à questão de investigação "***Estudantes que não ingressaram no ensino superior pelo CNAES demonstram melhores práticas de cibersegurança?***" é afirmativa, nesta amostra de dados, os estudantes que ingressaram por outros métodos de acesso ao ensino superior demonstram uma adoção mais positiva das práticas de cibersegurança.

Na Tabela 4.6 são apresentados os resultados da análise segundo a área de formação no ensino secundário dos participantes.

Área	Ciências e Tecnologias	Ciências Socio-económicas	Línguas e Humanidades	Artes Visuais	Cursos Profissionais
Gestão de Palavras-passe	**4,28**	**4,10**	**4,18**	**4,44**	**4,32**
Utilizar a mesma palavra-passe	3,98	3,84	3,94	3,67	4,29
Partilhar palavras-passe	4,49	4,28	4,27	5,00	4,45
Utilizar uma palavra-passe forte	4,38	4,19	4,31	4,67	4,22
Utilização do Email	**4,28**	**4,12**	**4,33**	**4,33**	**4,42**
Clicar em links de emails enviados por remetentes conhecidos	4,09	4,00	3,90	5,00	4,24
Clicar em links de emails enviados por remetentes desconhecidos	4,43	4,29	4,67	4,33	4,65
Abrir anexos de emails enviados por remetentes desconhecidos	4,32	4,08	4,41	3,67	4,37
Utilização da Internet	**4,18**	**3,96**	**4,02**	**3,44**	**4,13**
Transferir ficheiros	4,01	3,82	3,73	2,33	4,04
Aceder a websites duvidosos	4,26	4,13	4,39	3,67	4,31
Introduzir informações online	4,26	3,94	3,94	4,33	4,04
Utilização de redes sociais	**4,04**	**3,95**	**4,14**	**4,00**	**4,12**
Definições de privacidade das redes sociais	3,91	3,65	3,67	4,33	3,90
Considerar consequências	3,87	3,92	4,24	3,33	3,90
Publicar sobre o trabalho	4,35	4,29	4,53	4,33	4,57
Dispositivos móveis	**4,18**	**4,01**	**4,18**	**5,00**	**4,24**
Proteger fisicamente dispositivos móveis	4,22	4,13	4,26	5,00	4,31

Enviar informações sensíveis por Wi-Fi	4,07	3,87	3,94	5,00	4,06
Espionagem Visual	4,26	4,01	4,33	5,00	4,33
Tratamento de informações	**4,27**	**4,11**	**4,24**	**4,67**	**4,22**
Eliminação de impressos sensíveis	4,17	3,83	3,98	4,00	4,02
Inserir suportes amovíveis	4,58	4,33	4,75	5,00	4,41
Deixar material sensível	4,04	4,16	3,98	5,00	4,22
Comunicação de incidentes	**4,12**	**4,09**	**4,19**	**5,00**	**4,04**
Comunicar comportamentos suspeitos	4,06	4,08	4,10	5,00	3,90
Ignorar comportamentos de segurança inadequados de colegas	4,17	4,21	4,39	5,00	4,04
Comunicar todos os incidentes	4,12	3,98	4,08	5,00	4,18
Média	**4,19**	**4,05**	**4,18**	**4,41**	**4,21**
Total Respostas **Sem Resposta: 12**	**23**	**34**	**17**	**1**	**17**

Tabela 4.6: *Resultados médios por área de formação do ensino secundário em cada área e subárea do questionário.*

A indicação da área de formação do ensino secundário foi obrigatória apenas para os participantes que ingressaram através do CNAES, sendo opcional para os restantes participantes. Assim, para esta análise comparativa foram contabilizadas 92 respostas das 104 obtidas no questionário.

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- A área de formação em **ciências e tecnologias** teve 23 respostas com uma média geral de respostas de 4,19. A média mais alta foi nas áreas "Gestão de Palavras-passe" (4,28) e "Utilização do Email" (4,28) e a média mais baixa foi na área "Utilização de Redes Sociais" (4,04).
- A área de formação em **ciências socioeconómicas** teve 34 respostas, com uma média geral de respostas de 4,05. A média mais alta foi na área "Utilização do Email" (4,12) e a média mais baixa foi na área "Utilização de Redes Sociais" (3,95).
- A área de formação em **línguas e humanidades** teve 17 respostas, com uma média geral de respostas de 4,18. A média mais alta foi na área "Utilização do Email" (4,33) e a média mais baixa foi na área "Utilização da Internet" (4,02).
- A área de formação em **artes visuais** teve apenas uma resposta, com uma média geral de respostas de 4,41. A média mais alta foi nas áreas "Dispositivos Móveis" (5,00) e "Comunicação de Incidentes" (5,00) e a média mais baixa foi na área

"Utilização da Internet" (3,44). Devido ao número reduzido de respostas, esta área não foi considerada na resposta à questão de investigação.

- A área de formação por um **curso profissional** teve 17 respostas, com uma média geral de respostas de 4,21. A média mais alta foi na área "Utilização do Email" (4,42) e a média mais baixa foi na área "Comunicação de Incidentes" (4,04).

De forma geral, todas as áreas de formação do ensino secundário apresentaram uma média de respostas superior a 4, o que indica uma perceção positiva relativamente às práticas de cibersegurança. Os participantes provenientes de cursos profissionais registaram a média mais elevada na adoção dessas práticas, enquanto os participantes com formação em Ciências Socioeconómicas evidenciaram uma maior necessidade de estratégias de sensibilização.

Assim, a resposta à questão de investigação "***O percurso académico do ensino secundário influencia as práticas de cibersegurança adotadas pelos estudantes?***" é afirmativa, nesta amostra, observa-se uma relação entre a área de formação no ensino secundário e a perceção sobre as práticas de cibersegurança adotadas.

4.3.2 Análise Global

Esta análise teve como objetivo identificar as diferenças nas respostas entre as várias áreas avaliadas no questionário, de forma a responder às seguintes questões:

1. Qual a área que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?
2. Qual a dimensão (conhecimento, atitude, e comportamento) em que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?
3. Quais são as melhores e as piores práticas adotadas pelos estudantes em cada uma das áreas avaliadas?
4. Os estudantes de cursos não pertencentes às áreas CTEAM demonstram um bom nível de consciencialização para a cibersegurança?

Para responder a estas questões, recorreu-se à funcionalidade "*Descriptive Statistics*" do SPSS, selecionando a opção "*Descriptives*", com o objetivo de verificar as médias obtidas em cada área e subárea avaliada no questionário.

Na Tabela 4.7 são apresentadas as médias dos resultados obtidos em cada área e subárea avaliadas pelo questionário.

Área	Conhecimento	Atitude	Comportamento	Média
Gestão de Palavras-passe	**4,36**	**4,14**	**4,26**	**4,25**
Utilizar a mesma palavra-passe	4,04	4,45	3,69	4,06
Partilhar palavras-passe	4,65	3,82	4,67	4,38
Utilizar uma palavra-passe forte	4,37	4,16	4,41	4,32

Utilização do Email	**4,20**	**4,41**	**4,16**	**4,26**
Clicar em links de emails enviados por remetentes conhecidos	3,98	4,25	3,87	4,03
Clicar em links de emails enviados por remetentes desconhecidos	4,21	4,67	4,57	4,48
Abrir anexos de emails enviados por remetentes desconhecidos	4,39	4,32	4,04	4,25
Utilização da Internet	**4,22**	**4,26**	**3,69**	**4,06**
Transferir ficheiros	4,04	4,05	3,52	3,87
Aceder a websites duvidosos	4,42	4,30	4,07	4,26
Introduzir informações online	4,21	4,42	3,47	4,04
Utilização de redes sociais	**4,08**	**4,31**	**3,81**	**4,07**
Definições de privacidade das redes sociais	4,12	4,25	3,11	3,82
Considerar consequências	3,70	4,24	3,90	3,95
Publicar sobre o trabalho	4,41	4,44	4,41	4,42
Dispositivos móveis	**4,04**	**4,26**	**4,22**	**4,17**
Proteger fisicamente dispositivos móveis	3,80	4,45	4,47	4,24
Enviar informações sensíveis por Wi-Fi	4,12	3,94	4,07	4,04
Espionagem Visual	4,22	4,37	4,12	4,24
Tratamento de informações	**4,10**	**4,41**	**4,29**	**4,27**
Eliminação de impressos sensíveis	3,66	4,34	4,18	4,06
Inserir suportes amovíveis	4,45	4,61	4,54	4,53
Deixar material sensível	4,19	4,28	4,14	4,21
Comunicação de incidentes	**4,08**	**4,19**	**4,12**	**4,13**
Comunicar comportamentos suspeitos	4,07	4,19	3,98	4,08
Ignorar comportamentos de segurança inadequados de colegas	4,29	4,26	4,09	4,21
Comunicar todos os incidentes	3,89	4,11	4,29	4,10
Média	**4,15**	**4,28**	**4,08**	**4,17**

Tabela 4.7: *Resultados médios por área e subárea do questionário.*

Analisando os resultados obtidos, com base nesta amostra de dados, foram apuradas as seguintes conclusões:

- A área "**Gestão de Palavras-passe**" teve uma média geral de respostas de 4,25. A média mais alta foi a nível do conhecimento (4,36) e a mais baixa foi a nível da atitude (4,14).
- A área "**Utilização do Email**" teve uma média geral de respostas de 4,26. A média mais alta a nível da atitude (4,41) e a mais baixa foi a nível do comportamento

(4,16).

- A área "**Utilização da Internet**" teve uma média geral de respostas de 4,06. A média mais alta foi a nível da atitude (4,26) e a mais baixa foi a nível do comportamento (3,69).
- A área "**Utilização de Redes Sociais**" teve uma média geral de respostas de 4,07. A média mais alta foi a nível da atitude (4,31) e a mais baixa foi a nível do comportamento (3,81).
- A área "**Dispositivos Móveis**" teve uma média geral de respostas de 4,17. A média mais alta foi a nível da atitude (4,26) e a mais baixa foi a nível do conhecimento (4,04).
- A área "**Tratamento de Informações**" teve uma média geral de respostas de 4,27. A média mais alta foi a nível da atitude (4,41) e a mais baixa foi a nível do conhecimento (4,10).
- A área "**Comunicação de Incidentes**" teve uma média geral de respostas de 4,13. A média mais alta foi a nível da atitude (4,19) e a mais baixa a nível do conhecimento (4,08).

De forma geral, todas as áreas apresentaram uma média de respostas superior a 4, o que reflete uma perceção positiva relativamente às práticas de cibersegurança. No entanto, observam-se variações entre os diferentes níveis (conhecimento, atitude e comportamento) que merecem atenção.

Assim, em resposta à questão de investigação "***Qual a área que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?***" conclui-se que, nesta amostra, a área "Tratamento de Informações" é a que demonstra a média mais elevada na adoção de práticas de cibersegurança. Por outro lado, a área "Utilização da Internet" é a que revela uma maior necessidade de estratégias de sensibilização, especialmente a nível do comportamento.

A nível do **conhecimento** a média geral das respostas foi de 4,15, a nível da **atitude** foi de 4,28 e a nível do **comportamento** foi de 4,08. Apesar de a média em todos os níveis ser superior a 4, indicando uma perceção globalmente positiva das práticas de cibersegurança, ainda se observam variações entre os diferentes níveis que exigem alguma intervenção.

Assim, em resposta à questão de investigação "***Qual a dimensão (conhecimento, atitude, e comportamento) em que os estudantes indicam mais pontos positivos e negativos em relação à cibersegurança?***" conclui-se que, nesta amostra, os participantes apresentam uma média mais elevada na atitude, revelando uma postura positiva face às práticas de cibersegurança. No entanto, a média no comportamento é ligeiramente inferior, o que sugere que, apesar de estarem conscientes que devem adotar certas práticas, nem sempre as aplicam.

Para responder à questão de investigação "***Quais são as melhores e as piores práticas adotadas pelos estudantes em cada uma das áreas avaliadas?***" conclui-se, com base nesta amostra, que:

- Na área de "**Gestão de Palavras-passe**", a prática que mais necessita de intervenção é a reutilização da mesma palavra-passe em vários serviços. Apesar de os participantes demonstrarem consciência de que essa prática não é segura, muitos ainda não a evitam. Por outro lado, verifica-se que a maioria evita partilhar palavras-passe com outras pessoas e utilizar palavras-passe fracas. Contudo, no que diz respeito à partilha de palavras-passe, embora a maioria afirme não o fazer, ainda existem participantes que não veem problemas nessa prática.
- Na área da "**Utilização do Email**", a prática que mais necessita de intervenção é o hábito de clicar em links presentes em emails enviados por remetentes conhecidos, sem primeiro validar a sua autenticidade. Embora, os participantes tenham consciência de que esta ação pode não ser segura, mesmo tratando-se de alguém que conhecem, muitos admitem que o fazem sem hesitar. Por outro lado, a maioria dos participantes evita clicar em links ou abrir anexos provenientes de remetentes desconhecidos.
- Na área da "**Utilização da Internet**", as práticas que requerem uma maior intervenção são a transferência de ficheiros e o preenchimento de informações *online*. Muitos dos participantes não tomam cuidados ao transferirem conteúdos, e também não verificam se os *websites* onde inserem os seus dados são seguros. Por outro lado, a maioria evita aceder a *websites* de caráter duvidoso.
- Na área da "**Utilização de Redes Sociais**", as práticas que requerem mais intervenção são a falta de revisão regular das definições de privacidade e a publicação de conteúdos sem considerar as possíveis consequências. Por outro lado, a maioria dos participantes afirma que evita partilhar conteúdos relacionados com o trabalho nas redes sociais.
- Na área de "**Dispositivos Móveis**', a prática que mais necessita de intervenção é a utilização de redes Wi-Fi públicas para enviar informações. Por outro lado, a maioria dos participantes afirma que evita deixar os dispositivos em locais públicos sem vigilância e que procura impedir que outras pessoas vejam o que estão a fazer quando utilizam os dispositivos em espaços públicos.
- Na área do "**Tratamento de Informações**", a prática que mais necessita de intervenção é a eliminação de documentos impressos sensíveis, uma vez que a maioria dos participantes demonstra não ter consciência de que esses documentos devem ser destruídos de forma diferente dos não sensíveis. Por outro lado, a maioria dos participantes afirma que evita utilizar dispositivos USB de origem desconhecida e que evita deixar expostos documentos com conteúdos sensíveis."
- Na área da "**Comunicação de Incidentes**", as práticas que mais requerem intervenção são o facto de a maioria dos participantes admitir que não comunicaria comportamentos suspeitos por parte de colegas e a falta de consciência de que

todos os tipos de incidentes devem ser reportados, mesmo que pareçam insignificantes. Por outro lado, os participantes afirmam que, caso observassem um colega a ignorar as normas de segurança, procurariam tomar alguma atitude.

Em conclusão, os participantes apresentam uma média geral de respostas de 4,17, o que indica uma perceção globalmente positiva das práticas de cibersegurança. No entanto, algumas dessas práticas ainda não estão totalmente interiorizadas nem se refletem em comportamento efetivo.

Assim, a resposta à questão de investigação "***Os estudantes de cursos não pertencentes às áreas CTEAM demonstram um bom nível de consciencialização para a cibersegurança?***" é afirmativa, com base nesta amostra. Ainda assim, identificam-se áreas que requerem estratégias de sensibilização mais eficazes, nomeadamente na utilização da Internet e das redes sociais.

5
Conclusões

Esta dissertação apresentou um estudo com o objetivo de avaliar o nível de consciencialização para a cibersegurança de estudantes do Politécnico de Leiria, pertencentes a cursos de licenciatura não CTEAM, lecionados na ESTG. No estudo foi construído e aplicado um questionário baseado na escala HAIS-Q, bem como foi desenvolvida e implementada uma estratégia de sensibilização para a cibersegurança, sob a forma de aulas abertas, centrada nos tópicos abordados pela mesma escala.

O questionário avaliou os conhecimentos, as atitudes e os comportamentos dos participantes, tendo sido recolhidas 104 respostas de estudantes das licenciaturas em Administração Pública (Regime Diurno), Contabilidade e Finanças (Regime Diurno), Gestão (Regime Diurno e Pós-laboral), Marketing (Regime Diurno) e Solicitadoria (Regime Diurno e Pós-laboral). A análise das respostas permitiu concluir que os participantes apresentam, de forma geral, um bom nível de consciencialização para a cibersegurança. No entanto, foram identificadas diferenças entre os níveis de conhecimento, atitude e comportamento, sendo que o nível de comportamento se revelou ligeiramente inferior. Ou seja, embora os participantes saibam quais as práticas que devem adotar para garantir a sua segurança digital e revelem atitudes positivas nesse sentido, nem sempre colocam esse conhecimento em prática.

Entre as áreas avaliadas pela escala, os maiores problemas foram identificados na utilização da Internet e das redes sociais. Na utilização da Internet, muitos participantes não adotam precauções ao transferir ficheiros e não verificam se os *websites* onde colocam os seus dados são seguros. Relativamente às redes sociais, muitos participantes não verificam regularmente as definições de privacidade e muitas vezes partilham conteúdos sem considerar as possíveis consequências. Por outro lado, as áreas de utilização do email e de tratamento de informações apresentaram menos problemas, indicando que a maioria dos participantes está consciente dos cuidados que devem ter em relação a emails de *phishing* e que não se devem deixar documentos sensíveis expostos, nem utilizar dispositivos USB de origem desconhecida.

A estratégia de sensibilização para a cibersegurança, no formato de aulas abertas, foi implementada a estudantes do 2º ano das licenciaturas em Gestão (Regime Diurno) e Marketing (Regime Diurno). A aulas demonstraram-se eficazes na transmissão de boas práticas de cibersegurança, como comprovado pelos resultados do Quiz realizado nas sessões. A utilização de exemplos práticos contribuiu para uma melhor compreensão das possíveis consequências da negligência digital. Adicionalmente, foi disponibilizado no YouTube um vídeo contendo os mesmos conteúdos apresentados nas aulas. A disponibilização do vídeo permitiu alargar o alcance da iniciativa, promovendo o acesso a conteúdos relevantes por parte de um público mais vasto.

5.1 Limitações

A principal limitação deste estudo foi a baixa taxa de adesão ao questionário, apesar de ter sido divulgado pelos coordenadores de curso e de o prazo de resposta ter sido alargado.

A amostra obtida revelou-se bastante reduzida, o que dificultou a análise dos dados e comprometeu a possibilidade de obter uma medição mais conclusiva sobre o nível de consciencialização para a cibersegurança dos estudantes.

Outra limitação identificada foi a impossibilidade de aplicar a estratégia de sensibilização em todos os cursos que participaram no questionário. No entanto, esta limitação foi parcialmente superada através da disponibilização dos conteúdos em formato de vídeo.

5.2 Trabalho Futuro

A implementação deste trabalho foi realizada numa pequena amostra de estudantes, numa das unidades orgânicas do Politécnico de Leiria.

Desta forma, como trabalho futuro, sugere-se que o questionário de avaliação seja aplicado também em outras unidades orgânicas do Politécnico de Leiria, abrangendo mais áreas de formação e todos os ciclos de ensino. Propõe-se também que o questionário seja direcionado não apenas aos estudantes, mas também a funcionários e docentes.

Perante os resultados obtidos, recomenda-se a implementação de mais estratégias de sensibilização para a cibersegurança. Neste sentido, a realização de simulações de ameaças pode ser particularmente eficaz, uma vez que muitos participantes demonstraram possuir o conhecimento necessário, mas nem sempre o aplicam na prática.

Por exemplo, no caso das redes sociais, uma das áreas onde se identificaram mais problemas, poderia ser realizado um estudo com a criação de um perfil falso, com o objetivo de interagir com os estudantes e analisar as suas reações, de forma a avaliar o seu grau de preparação face aos riscos associados a estas plataformas. Por outro lado, no

que diz respeito à utilização do email, a área onde se observaram menos problemas, seria interessante realizar uma simulação de um ataque de *phishing*, que envolvesse o clique num *link* ou a transferência de um anexo, de modo a avaliar se os estudantes estão, de facto, bem preparados para este tipo de ameaça.

Relativamente à estratégia de sensibilização, recomenda-se a sua implementação em mais cursos e também junto dos funcionários. Quanto ao vídeo publicado no YouTube, sugere-se uma divulgação mais ampla, de forma a alcançar um público maior.

Adicionalmente, propõe-se que o questionário de avaliação seja aplicado antes e depois da implementação da estratégia, com o objetivo de validar a sua eficácia e permitir os ajustes necessários para a tornar mais eficiente.

5.3 Contribuições

Esta dissertação permitiu evidenciar o nível atual de consciencialização para a cibersegurança dos estudantes de licenciaturas de áreas não CTEAM da ESTG. A aplicação da estratégia de sensibilização contribuiu significativamente para a promover a segurança digital e para reforçar as competências digitais desses estudantes. Assim, os contributos desta dissertação são os seguintes:

1. Aplicação da escala HAIS-Q a um grupo de estudantes de áreas não CTEAM e avaliação dos resultados obtidos.
2. Organização de sessões de sensibilização junto dos alunos envolvidos no estudo.
3. Criação de um vídeo de sensibilização baseado em IA e disponibilizado no seguinte canal do YouTube: `https://youtu.be/9arF2JkqE1g`

A nível pessoal, esta dissertação aprofundou os meus conhecimentos sobre as ameaças existentes, as boas práticas de segurança que se devem adotar e a importância destas práticas na prevenção de riscos *online*. Além disso, reforçou as minhas competências de investigação e de comunicação, tendo sido convidada, durante o desenvolvimento deste trabalho, a rever dois artigos científicos em revistas internacionais, relacionados com a temática deste estudo.

Acredito que, para além do enriquecimento pessoal, este trabalho teve um impacto positivo na comunidade académica, ao promover comportamentos mais conscientes e seguros no mundo digital.

Página intencionalmente deixada em branco.

Bibliography

Amankwa, Eric e Eric Amankwa (set. de 2021). «Relevance of Cybersecurity Education at Pedagogy Levels in Schools». Em: *Journal of Information Security* 12 (4), pp. 233–249. ISSN: 2153-1234. DOI: 10.4236/JIS.2021.124013.

Aslan, Ömer et al. (mar. de 2023). «A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions». Em: *Electronics* 12 (6), p. 1333. ISSN: 2079-9292. DOI: 10.3390/ELECTRONICS12061333.

Awodiran, Muideen Adeseye et al. (2023). «Cybercrime Consciousness Among Undergraduate Students». Em: *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, pp. 301–306. DOI: 10.1109/CYMAEN57228.2023.10050982.

Bay, Morten (2016). «What is cybersecurity». Em: *French Journal for Media Research* 6, pp. 1–28.

Borky, John M. e Thomas H. Bradley (2019). «Protecting Information with Cybersecurity». Em: Springer International Publishing, pp. 345–404. ISBN: 978-3-319-95669-5. DOI: 10.1007/978-3-319-95669-5_10. URL: https://doi.org/10.1007/978-3-319-95669-5_10.

Breitinger, Frank, Ryan Tully-Doyle e Courtney Hassenfeldt (jan. de 2020). «A survey on smartphone user's security choices, awareness and education». Em: *Computers & Security* 88, p. 101647. ISSN: 0167-4048. DOI: 10.1016/J.COSE.2019.101647.

Caplan, Scott E. (set. de 2010). «Theory and measurement of generalized problematic Internet use: A two-step approach». Em: *Computers in Human Behavior* 26 (5), pp. 1089–1097. ISSN: 0747-5632. DOI: 10.1016/J.CHB.2010.03.012.

Chen, Yu Tsang et al. (abr. de 2021). «Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan». Em: *Computers & Education* 164, p. 104131. ISSN: 0360-1315. DOI: 10.1016/J.COMPEDU.2021.104131.

Cibercrime, Gabinete (mar. de 2025). *Cibercrime: Denuncias Recebidas 2024*. URL: https://cibercrime.ministeriopublico.pt/sites/default/files/2025-03/2025.03.18-denuncias-de-cibercrime-2024.pdf.

Cindana, Alvin e Yova Ruldeviyani (jul. de 2018). «Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm». Em: *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pp. 289–294. DOI: 10.1109/ICACSIS.2018.8618219.

Ciupe, Aurelia e Bogdan Orza (2024). «Reinforcing Cybersecurity Awareness through Simulated Phishing Attacks: Findings from an HEI Case Study». Em: *2024 IEEE Global Engineering Education Conference (EDUCON)*. ISSN: 21659567. DOI: 10.1109/EDUCON60312.2024.10578700.

Conselho de Ministros n.º 92/2019, Resolução do (jun. de 2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. URL: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962.

Das, Sumanjit e Tapaswini Nayak Asst-Prof (2013). «Impact of cybercrime: Issues and challenges». Em: *International Journal of Engineering Sciences & Emerging Technologies* 6 (2), pp. 142–153.

Effendy, Vina Ardelia et al. (2022). «Measurement of Employee Information Security Awareness on Data Security: A Case Study at XYZ Polytechnic». Em: *2022 1st International Conference on Information System & Information Technology (ICISIT)*, pp. 272–276. DOI: 10.1109/ICISIT54091.2022.9873077.

Goni, Osman et al. (abr. de 2022). «The Basic Concept of Cyber Crime». Em: *Journal of Technology Innovations and Energy*. DOI: 10.5281/zenodo.6499991.

Gupta, Pranshu e Ramon Mata-Toledo (2016). «CYBERCRIME: IN DISGUISE CRIMES». Em: *Journal of Information Systems & Operations Management*, pp. 1–10.

Holt, Thomas J. e Adam M. Bossler (jan. de 2015). «Cybercrime in progress: Theory and prevention of technology-enabled offenses». Em: *Routledge*, pp. 1–236. DOI: https://doi.org/10.4324/9781315775944.

Howard, David J (2018). *Development of the Cybersecurity Attitudes Scale and Modeling Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents Cybersecurity Behavior and its Antecedents*. URL: https://digitalcommons.usf.edu/etd.

Keshvadi, Sina (2023). «Enhancing Western Organizational Cybersecurity Resilience through Tailored Education for Non-Technical Employees». Em: *2023 IEEE International Humanitarian Technology Conference (IHTC)*. DOI: 10.1109/IHTC58960.2023.10508824.

Magdalinou, Andriana et al. (2022). «Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals». Em: *Studies in Health Technology and Informatics* 295, pp. 24–27. ISSN: 18798365. DOI: 10.3233/SHTI220650. URL: https://ebooks.iospress.nl/doi/10.3233/SHTI220650.

Marques, Frederico Manuel Ferreira (dez. de 2021). *ESTRATÉGIA INTEGRADA DE AVALIAÇÃO E CONSCIENCIALIZAÇÃO CIBERNÉTICA EM CONTEXTO ESCOLAR*. URL: https://iconline.ipleiria.pt/handle/10400.8/6651.

Mcnulty, Matthew e Houssain Kettani (mar. de 2020). «On cybersecurity education for non-technical learners». Em: *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, pp. 413–416. DOI: 10.1109/ICICT50521.2020.00072.

Mersinas, Konstantinos, Maria Bada e Steven Furnell (jan. de 2025). «Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions». Em: *Computers & Security* 148, p. 104025. ISSN: 0167-4048. DOI: 10.1016/J.COSE.2024.104025.

Moletsane, Tankiso e Pitso Tsibolane (mar. de 2020). «Mobile Information Security Awareness among Students in Higher Education: An Exploratory Study». Em: *2020 Conference on Information Communications Technology and Society (ICTAS)*. DOI: 10.1109/ICTAS47918.2020.233978.

Naughton, John (jan. de 2016). «The evolution of the Internet: from military experiment to General Purpose Technology». Em: *Journal of Cyber Policy* 1 (1), pp. 5–28. ISSN: 2373-8871. DOI: 10.1080/23738871.2016.1157619. URL: https://www.tandfonline.com/doi/abs/10.1080/23738871.2016.1157619.

Neigel, Alexis R. et al. (mai. de 2020). «Holistic cyber hygiene education: Accounting for the human factors». Em: *Computers & Security* 92, p. 101731. ISSN: 0167-4048. DOI: 10.1016/J.COSE.2020.101731. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404820300183.

Nurbojatmiko et al. (out. de 2020). «Information Security Awareness of Students on Academic Information System Using Kruger Approach». Em: *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. DOI: 10.1109/CITSM50537.2020.9268795.

Oliveira, Luís et al. (2023). «Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland». Em: *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 168–173. DOI: 10.1109/CSR57506.2023.10224910.

Parsons, Kathryn et al. (jan. de 2013). «The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)». Em: *ACIS 2013 Proceedings*. URL: https://aisel.aisnet.org/acis2013/31.

Parsons, Kathryn et al. (mai. de 2014). «Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)». Em: *Computers & Security* 42, pp. 165–176. ISSN: 0167-4048. DOI: 10.1016/J.COSE.2013.12.003.

Parsons, Kathryn et al. (mai. de 2017). «The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies». Em: *Computers & Security* 66, pp. 40–51. ISSN: 0167-4048. DOI: 10.1016/J.COSE.2017.01.004.

Rahman, Nurul Amirah Abdul et al. (2020). «The importance of cybersecurity education in school». Em: *International Journal of Information and Education Technology* 10.5, pp. 378–382.

Raju, Rajeswari, Nur Hidayah Abd Rahman e Atif Ahmad (jul. de 2022). «Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution». Em: *Asian Journal of University Education* 18 (3), pp. 756–766. ISSN: 18237797. DOI: 10.24191/ajue.v18i3.18967.

Sabillon, Regner et al. (2016). «Cybercrime and cybercriminals: A comprehensive study». Em: *International Journal of Computer Networks and Communications Security* 4 (6), pp. 165–176. ISSN: 2410-0595. URL: https://openaccess.uoc.edu/handle/10609/78507.

Salem, Yaman, Mohammed Moreb e Khalid S. Rabayah (jul. de 2021). «Evaluation of Information Security Awareness among Palestinian Learners». Em: *2021 International Conference on Information Technology (ICIT)*, pp. 21–26. DOI: 10.1109/ICIT52682.2021.9491639.

Setiawan, Bambang e Muhamad Ainur Rizal (jan. de 2024). «Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic». Em: *Procedia Computer Science* 234, pp. 1396–1403. ISSN: 1877-0509. DOI: 10.1016/J.PROCS.2024.03.138.

Shukla, Shubhendu Shekher et al. (2022). «A Comparative Study of Cyber Security Awareness, Competence and Behavior». Em: *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1704–1709. DOI: 10.1109/IC3I56241.2022.10072880.

Soylu, Demet et al. (abr. de 2021). «Identifying the Cybercrime Awareness of Undergraduate and Postgraduate Students: Example of Kazakhstan». Em: *2021 IEEE International Conference on Smart Information Systems and Technologies (SIST)*. DOI: 10.1109/SIST50301.2021.9465995.

Susanto, Tony Dwi e Muhammad Dafa Maulana (jan. de 2024). «Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government». Em: *Procedia Computer Science* 234, pp. 1428–1434. ISSN: 1877-0509. DOI: 10.1016/J.PROCS.2024.03.142.

Thakur, Kutub et al. (jan. de 2016). «An Investigation on Cyber Security Threats and Security Models». Em: *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, pp. 307–311. DOI: 10.1109/CSCLOUD.2015.71.

Thatcher, Jason Bennett et al. (2008). «Internal and external dimensions of computer self-efficacy: An empirical examination». Em: *IEEE Transactions on Engineering Management* 55 (4), pp. 628–644. ISSN: 00189391. DOI: 10.1109/TEM.2008.927825.

Zulfia, Aulia et al. (abr. de 2019). «Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS». Em: *2019 5th International Conference on Computing Engineering and Design (ICCED)*. DOI: 10.1109/ICCED46541.2019.9161120.

Zwilling, Moti et al. (jan. de 2022). «Cyber Security Awareness, Knowledge and Behavior: A Comparative Study». Em: *Journal of Computer Information Systems* 62 (1), pp. 82–97. ISSN: 0887-4417. DOI: 10.1080/08874417.2020.1712269.

Página intencionalmente deixada em branco.

Apêndices

Página intencionalmente deixada em branco.

A

Pedido de Autorização Enviado aos Autores da Escala

Este apêndice contém o email enviado aos autores da escala HAIS-Q, no qual se solicita autorização para a sua tradução e utilização no âmbito deste trabalho

Outlook

Request to use and translate the scale HAIS-Q

De Cristiana Isabel Santos Sousa <2230457@my.ipleiria.pt>
Data qui, 14/11/2024 15:34
Para kathryn.parsons@dsto.defence.gov.au <kathryn.parsons@dsto.defence.gov.au>
Cc Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Dear Professor Kathryn Parsons,

My name is Cristiana Sousa, and I'm currently in the 2nd year of my Master's Degree in Cybersecurity and Digital Forensics at the School of Technology and Management of the Polytechnic of Leiria. I'm working on my dissertation, under the supervision of Professor Mário Antunes, which aims to assess and evaluate the cybersecurity behaviors and attitudes of students at the Polytechnic of Leiria, a Portuguese higher education institution.

I'd like to ask your for permission to translate the HAIS-Q scale (published in 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) into portuguese and to use it in the scope of my research.

The questionnaires will only be used under the scope of my dissertation and any publication and dissemination of the results will cite the original paper indicated above.

I thank you in advance and I'll look forward to your answer.

Kind Regards,

Cristiana Sousa

B

Resposta ao Pedido de Autorização

Este apêndice contém o email em que foi concedida autorização para a tradução e utilização da escala HAIS-Q no âmbito deste trabalho.

Outlook

FW: Request to use and translate the scale HAIS-Q [SEC=OFFICIAL]

De McCormac, Agata MS <agata.mccormac@defence.gov.au>
Data qui, 14/11/2024 22:05
Para Cristiana Isabel Santos Sousa <2230457@my.ipleiria.pt>

OFFICIAL

Good morning Cristiana,

My name is Agata McCormac and I work on the same research team as Dr Parsons.

Yes, you are certainly more than welcome to translate the measure into Portuguese.

We wish you all the best with your research endeavours.

Kind Regards,

Agata McCormac
Cyber Resilience and Deterrence | Cyber Assurance and Resilience
Information Sciences Division
Defence Science and Technology Group

Department of Defence | Edinburgh
PO Box 1500 | EDINBURGH SA 5111
E: agata.mccormac@defence.gov.au
Defence acknowledges the Traditional Custodians of the Country throughout Australia. We recognise their continuing connection to land, waters and community. We pay our respects to them, their culture and to their Elders past and present.

From: Cristiana Isabel Santos Sousa <2230457@my.ipleiria.pt>
Sent: Friday, 15 November 2024 2:05 AM
To: kathryn.parsons@dsto.defence.gov.au
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>
Subject: Request to use and translate the scale HAIS-Q

Dear Professor Kathryn Parsons,

My name is Cristiana Sousa, and I'm currently in the 2nd year of my Master's Degree in Cybersecurity and Digital Forensics at the School of Technology and Management of the Polytechnic of Leiria. I'm working on my dissertation, under the supervision of Professor Mário Antunes, which aims to assess and evaluate the cybersecurity behaviors and attitudes of students at the Polytechnic of Leiria, a Portuguese higher education institution.

I'd like to ask your for permission to translate the HAIS-Q scale (published in 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) into portuguese and to use it in the scope of my research.

The questionnaires will only be used under the scope of my dissertation and any publication and dissemination of the results will cite the original paper indicated above.

I thank you in advance and I'll look forward to your answer.

Kind Regards,

Cristiana Sousa

C

Itens da Escala HAIS-Q (Inglês)

Neste apêndice são apresentadas os itens da escala HAIS-Q, no seu idioma original (inglês).

	Knowledge	**Attitude**	**Behaviour**
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my work accounts. ^	It's safe to use the same password for social media and work accounts. ^	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues. ^	It's a bad idea to share my work passwords, even if a colleague asks for it.	I share my work passwords with colleagues.^
Using a strong password	A mixture of letters, numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters. ^	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know. ^	It's always safe to click on links in emails from people I know. ^	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an email from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender. ^	If an email from an unknown sender looks interesting, I click on a link within it. ^

Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders. ^	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings.^
Considering consequences	I can't be fired for something I post on social media. ^	It doesn't matter if I post things on social media that I wouldn't normally say in public. ^	I don't post anything on social media before considering any negative c onsequences.
Posting about work	I can post what I want about work on social media. ^	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media. ^
Focus area: Mobile devices			

Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. ^	When working in a public place, I leave my laptop unattended. ^
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work files via a public Wi-Fi network. ^	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network. ^
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.^	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. ^	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. ^	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight. ^	It's risky to leave print-outs that contain sensitive information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there. ^
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. ^	If I saw someone acting suspiciously in my workplace, I would do something about it.

Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague. ^	If I noticed my colleague ignoring security rules, I wouldn't take any action. ^
Reporting all incidents	It's optional to report security incidents. ^	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.
Note: Participants are instructed to respond to each item on a five-point scale from "Strongly Disagree" to "Strongly Agree" ^Reverse scoring was used on this item			

Tabela C.1: *Itens do HAIS-Q, em inglês.*

D

Itens da Escala HAIS-Q (Português)

Neste apêndice são apresentadas os itens da escala HAIS-Q, traduzidas para português.

	Conhecimento	Atitude	Comportamento
Área de incidência: Gestão de palavras-passe			
Utilizar a mesma palavra-passe	É aceitável utilizar as minhas palavras-passe das redes sociais nas minhas contas de trabalho. ^	É seguro utilizar a mesma palavra-passe para as contas das redes sociais e do trabalho. ^	Utilizo uma palavra-passe diferente para as minhas contas das redes sociais e do trabalho.
Partilhar palavras-passe	Posso partilhar as minhas palavras-passe do trabalho com colegas. ^	É uma má ideia partilhar as minhas palavras-passe do trabalho, mesmo que um colega as peça.	Partilho as minhas palavras-passe do trabalho com colegas.^
Utilizar uma palavra-passe forte	É necessária uma combinação de letras, números e símbolos para as palavras-passe de trabalho.	É seguro ter uma palavra-passe de trabalho apenas com letras. ^	Utilizo uma combinação de letras, números e símbolos nas minhas palavras-passe de trabalho.
Área de incidência: Utilização do Email			

Clicar em *links* de emails enviados por remetentes conhecidos.	Posso clicar em quaisquer *links* de emails enviados por pessoas que conheço. ^	É sempre seguro clicar em *links* de emails enviados por pessoas que conheço.^	Nem sempre clico nos *links* de emails só porque vêm de alguém que conheço.
Clicar em *links* de emails enviados por remetentes desconhecidos	Não posso clicar num *link* de um email enviado por um remetente desconhecido.	Nada de mal pode acontecer se eu clicar em um *link* de um email enviado por um remetente desconhecido. ^	Se um email enviado por um remetente desconhecido parecer interessante, clico no *link*.^
Abrir anexos de emails enviados por remetentes desconhecidos	Posso abrir anexos de emails enviados por remetentes desconhecidos.^	É arriscado abrir um anexo de email enviado por um remetente desconhecido.	Não abro anexos de email se o remetente for desconhecido para mim.
Área de incidência: Utilização da Internet			
Transferir ficheiros	Posso descarregar quaisquer ficheiros para o meu computador de trabalho se me ajudarem a fazer o meu trabalho. ^	Pode ser arriscado descarregar ficheiros no meu computador de trabalho.	Descarrego todos os ficheiros para o meu computador de trabalho que me ajudem a fazer o meu trabalho.^
Aceder a *websites* duvidosos	Enquanto estou no trabalho, não devo aceder a determinados *websites*.	Só porque posso aceder a um *website* no trabalho, não significa que seja seguro.	Quando acedo à Internet no trabalho, visito qualquer *website* que queira. ^
Introduzir informações online	Posso introduzir qualquer informação em qualquer *website* se isso me ajudar a fazer o meu trabalho.^	Se me ajudar a fazer o meu trabalho, não importa a informação que coloco num *website*. ^	Verifico a segurança dos *websites* antes de introduzir informações.
Área de incidência: Utilização de redes sociais			
Definições de privacidade das redes sociais	Devo rever periodicamente as definições de privacidade das minhas contas nas redes sociais.	É uma boa ideia rever regularmente as minhas definições de privacidade nas redes sociais.	Não revejo regularmente as definições de privacidade das minhas redes sociais. ^

Considerar consequências	Não posso ser despedido por algo que publiquei nas redes sociais. ^	Não vejo problema em publicar nas redes sociais coisas que eu normalmente não diria em público. ^	Não publico nada nas redes sociais antes de pensar nas consequências negativas.
Publicar sobre o trabalho	Posso publicar o que quiser sobre o meu trabalho nas redes sociais. ^	É arriscado publicar certas informações sobre o meu trabalho nas redes sociais.	Publico o que quiser sobre o meu trabalho nas redes sociais. ^
Área de incidência: Dispositivos móveis			
Proteger fisicamente dispositivos móveis	Quando trabalho num local público, devo ter o meu portátil sempre comigo.	Quando estou a trabalhar num café, é seguro deixar o meu portátil sem supervisão durante um minuto. ^	Quando trabalho num local público, deixo o meu portátil sem vigilância. ^
Enviar informações sensíveis por Wi-Fi	Posso enviar ficheiros de trabalho sensíveis através de uma rede Wi-Fi pública. ^	É arriscado enviar ficheiros de trabalho sensíveis através da rede Wi-Fi pública.	Envio ficheiros de trabalho sensíveis através da rede Wi-Fi pública. ^
Espionagem Visual	Ao trabalhar em um documento sensível, preciso de garantir que desconhecidos não consigam ver o ecrã do meu portátil.	É arriscado aceder a ficheiros de trabalho sensíveis no portátil se desconhecidos puderem ver o meu ecrã.	Verifico se desconhecidos não conseguem ver o ecrã do meu portátil quando estou a trabalhar num documento sensível.
Área de incidência: Tratamento de informações			
Eliminação de impressos sensíveis	Os documentos impressos sensíveis podem ser eliminados da mesma forma que os não sensíveis. ^	É seguro deitar fora documentos impressos sensíveis, colocando-os no caixote do lixo. ^	Quando é necessário eliminar documentos impressos sensíveis, certifico-me de que são triturados ou destruídos.

Inserir suportes amovíveis	Se eu encontrar uma pen USB num local público, não devo ligá-la ao meu computador de trabalho.	Se eu encontrar uma pen USB num local público, nada de mal pode acontecer se a ligar ao meu computador de trabalho. ^	Eu não ligaria uma pen USB encontrada num local público ao meu computador de trabalho.
Deixar material sensível	Posso deixar documentos impressos com informações sensíveis na minha secretária durante a noite.^	É arriscado deixar documentos impressos que contenham informações sensíveis na minha secretária durante a noite.	Deixo documentos impressos que contêm informações sensíveis na minha secretária quando não estou lá. ^
Área de incidência: Comunicação de incidentes			
Comunicar comportamentos suspeitos	Se eu vir alguém a agir de forma suspeita no meu local de trabalho, devo comunicá-lo.	Se eu ignorar alguém que está a agir de forma suspeita no meu local de trabalho, nada de mal pode acontecer. ^	Se eu visse alguém a agir de forma suspeita no meu local de trabalho, faria alguma coisa.
Ignorar comportamentos de segurança inadequados de colegas	Não devo ignorar comportamentos inadequados de segurança dos meus colegas.	Nada de mal pode acontecer se eu ignorar o comportamento inadequado de segurança de um colega. ^	Se eu visse um colega a ignorar as regras de segurança, não tomaria qualquer medida. ^
Comunicar todos os incidentes	É opcional comunicar incidentes de segurança. ^	É arriscado ignorar os incidentes de segurança, mesmo que eu ache que não são significativos.	Se me apercebesse de um incidente de segurança, comunicá-lo-ia.
Nota: Os participantes são instruídos a responder a cada item numa escala de cinco pontos, de "Discordo totalmente" a "Concordo totalmente" ^Foi utilizada a pontuação inversa neste item			

Tabela D.1: *Itens do HAIS-Q, em português.*

E

Email de Divulgação do Questionário

Este apêndice inclui um dos emails enviados aos coordenadores das licenciaturas, com o objetivo de divulgar o questionário. Neste caso, trata-se do email enviado ao coordenador do curso de Administração Pública.

Outlook

Divulgação de Questionário "Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria "

De Cristiana Isabel Santos Sousa <2230457@my.ipleiria.pt>
Data sex, 28/02/2025 15:37
Para Coordenador Administração Pública <coord.ap.estg@ipleiria.pt>; Luis Pedroso de Lima Cabral de Oliveira <luis.oliveira@ipleiria.pt>
Cc Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Estimado Doutor Luís Cabral de Oliveira, Coordenador do Curso de Administração Pública,

O meu nome é Cristiana Sousa, e estou a realizar a minha dissertação de mestrado, sob a orientação do Prof. Mário Antunes (DEI, ESTG), no curso de Mestrado em Cibersegurança e Informática Forense, a decorrer no ano letivo 2024/2025.

A dissertação tem como objetivo avaliar, com recurso a um questionário, o nível de consciencialização em cibersegurança dos estudantes de Licenciatura da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria que **não pertencem** a cursos de áreas de Science, Technology, Engineering, Arts, and Mathematics (STEAM), designadamente os cursos de Licenciatura em Administração Pública, Contabilidade e Finanças, Gestão, Marketing e Solicitadoria.

O estudo que se pretende realizar baseia-se na aplicação da escala HAIS-Q, desenvolvida por Parsons et al. e que se encontra publicada no seguinte artigo científico:

- 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.*"

A escala HAIS-Q mede os níveis de conhecimentos, atitudes e comportamentos dos indivíduos em relação às práticas de cibersegurança. Para tal, foca-se em sete áreas, sendo que cada uma dessas áreas analisa três subáreas específicas:

1. **Gestão de palavras-passe**: Utilizar a mesma palavra-passe; Partilhar palavras-passe; e Utilizar uma palavra-passe forte.
2. **Utilização de email**: Clicar em links de emails enviados por remetentes conhecidos; Clicar em links de emails enviados por remetentes desconhecidos; e Abrir anexos de emails enviados por remetentes desconhecidos.
3. **Utilização da Internet**: Transferir ficheiros; Aceder a websites duvidosos; e Introduzir informações online.
4. **Utilização de redes sociais**: Definições de privacidade das redes sociais; Considerar consequências; e Publicar sobre o trabalho.
5. **Dispositivos móveis**: Proteger fisicamente dispositivos móveis; Enviar informações sensíveis por Wi-Fi; e Espionagem visual.
6. **Tratamento da informação**: Eliminação de impressos sensíveis; Inserir suportes amovíveis; e Deixar material sensível.
7. **Comunicação de incidentes**: Comunicar comportamentos suspeitos; Ignorar comportamentos de segurança inadequados de colegas; e Comunicar todos os incidentes.

Cada subárea é avaliada através de **três questões**:

1. Uma **questão de conhecimento** para avaliar o nível de compreensão do inquirido sobre o tópico em análise.
2. Uma **questão de atitude** para avaliar a postura do inquirido em relação ao tópico em análise.
3. Uma **questão de comportamento** para avaliar as práticas que o inquirido aplica em relação ao tópico em análise.

Este questionário é uma tradução direta das questões originais do HAIS-Q, onde se apresenta tanto a versão traduzida como a versão original em inglês para facilitar a sua compreensão. A estrutura detalhada das questões originais pode ser consultada no link fornecido.

Venho por este meio solicitar a divulgação deste estudo aos seus estudantes, que consiste em responder a um questionário, o que deverá levar aproximadamente 10 minutos.

A participação neste estudo é **completamente voluntária**. Pode recusar-se a responder a qualquer pergunta que não queira e interromper o questionário em qualquer momento.

Todas as respostas são **confidenciais** e **anónimas**, ou seja, não serão analisadas individualmente, mas dentro do conjunto de todas as respostas obtidas, para cumprir o objetivo do estudo.

O questionário pode ser acedido através do seguinte link: https://forms.gle/d7fTgLjgZ9Yn3Pbu6

Muito agradeço a submissão da sua resposta até ao dia 31-03-2025.

A estudante,
Cristiana Sousa

F

Questionário de Avaliação

Este apêndice inclui o questionário aplicado com o objetivo de avaliar os conhecimentos, atitudes e comportamentos dos estudantes em relação às práticas de cibersegurança.

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

Este questionário insere-se nos trabalhos conducentes à realização da minha dissertação de mestrado, sob a orientação do Prof. Mário Antunes (DEI, ESTG), no curso de Mestrado em Cibersegurança e Informática Forense, a decorrer no ano letivo 2024/2025.

O questionário tem como objetivo avaliar o nível de consciencialização em cibersegurança dos estudantes de Licenciatura da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria que **não pertencem** a cursos de áreas de *Science, Technology, Engineering, Arts, and Mathematics* (STEAM), designadamente os cursos de Licenciatura em Administração Pública, Contabilidade e Finanças, Gestão, Marketing e Solicitadoria.

O estudo que se pretende realizar baseia-se na aplicação da escala HAIS-Q, desenvolvida por Parsons et al. e que se encontra publicada no seguinte artigo científico:

- *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."*

A escala HAIS-Q mede os níveis de conhecimentos, atitudes e comportamentos dos indivíduos em relação às práticas de cibersegurança. Para tal, foca-se em sete áreas, sendo que cada uma dessas áreas analisa três subáreas específicas:

1. **Gestão de palavras-passe**: Utilizar a mesma palavra-passe; Partilhar palavras-passe; e Utilizar uma palavra-passe forte.
2. **Utilização de email**: Clicar em links de emails enviados por remetentes conhecidos; Clicar em links de emails enviados por remetentes desconhecidos; e Abrir anexos de emails enviados por remetentes desconhecidos.
3. **Utilização da Internet**: Transferir ficheiros; Aceder a websites duvidosos; e Introduzir informações online.
4. **Utilização de redes sociais**: Definições de privacidade das redes sociais; Considerar consequências; e Publicar sobre o trabalho.
5. **Dispositivos móveis**: Proteger fisicamente dispositivos móveis; Enviar informações sensíveis por Wi-Fi; e Espionagem visual.
6. **Tratamento da informação**: Eliminação de impressos sensíveis; Inserir suportes amovíveis; e Deixar material sensível.
7. **Comunicação de incidentes**: Comunicar comportamentos suspeitos; Ignorar comportamentos de segurança inadequados de colegas; e Comunicar todos os incidentes.

Cada subárea é avaliada através de **três questões**:

1. Uma **questão de conhecimento** para avaliar o nível de compreensão do inquirido sobre o tópico em análise.
2. Uma **questão de atitude** para avaliar a postura do inquirido em relação ao tópico em análise.

3. Uma **questão de comportamento** para avaliar as práticas que o inquirido aplica em relação ao tópico em análise.

Este questionário é uma tradução direta das questões originais do HAIS-Q, onde se apresenta tanto a versão traduzida como a versão original em inglês para facilitar a sua compreensão. A estrutura detalhada das questões originais pode ser consultada no link fornecido.

Venho por este meio solicitar a sua participação neste estudo que consiste em responder ao presente questionário, o que deverá levar aproximadamente 10 minutos.

A sua participação neste estudo é **completamente voluntária**. Pode recusar-se a responder a qualquer pergunta que não queira e interromper o questionário em qualquer momento.

Todas as suas respostas são **confidenciais** e **anónimas**, ou seja, não serão analisadas individualmente, mas dentro do conjunto de todas as respostas obtidas, para cumprir o objetivo do estudo.

Muito agradeço a submissão da sua resposta até ao dia 31-03-2025.

A estudante,
Cristiana Sousa

* Indica uma pergunta obrigatória

Concorda em participar neste estudo? *

- ◯ Sim, eu concordo em participar neste estudo
- ◯ Não, eu recuso participar neste estudo

Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

* Indica uma pergunta obrigatória

Dados dos participantes

Qual o seu curso? *

- ◯ Administração Pública
- ◯ Contabilidade e Finanças
- ◯ Gestão - Diurno
- ◯ Gestão - Pós-laboral
- ◯ Marketing
- ◯ Solicitadoria - Diurno
- ◯ Solicitadoria - Pós-laboral

Ano curricular *

- ◯ 1º ano
- ◯ 2º ano
- ◯ 3º ano

Tipo de ingresso no ensino superior *

- ◯ Concurso Nacional de Acesso ao Ensino Superior (CNAES)
- ◯ Concurso Especial para Estudantes Internacionais
- ◯ Reingresso
- ◯ Mudança de Instituição
- ◯ Mudança de Curso
- ◯ Concurso Especial - M23
- ◯ Concurso Especial - CET
- ◯ Concurso Especial - TeSP
- ◯ Concurso Especial - outros cursos superiores
- ◯ Concurso Especial para Diplomados de Vias Profissionalizantes
- ◯ Regimes Especiais

Área do secundário

Responder **apenas** se escolheu a opção **Concurso Nacional de Acesso ao Ensino Superior (CNAES)** na pergunta anterior.

- ◯ Cursos Científico-Humanísticos - Ciências e Tecnologias
- ◯ Cursos Científico-Humanísticos - Ciências Socioeconómicas
- ◯ Cursos Científico-Humanísticos - Línguas e Humanidades
- ◯ Cursos Científico-Humanísticos - Artes Visuais
- ◯ Cursos Artísticos Especializados
- ◯ Cursos Profissionais

Qual o seu sexo? *

- ◯ Feminino
- ◯ Masculino
- ◯ Prefiro não dizer

Qual a sua faixa etária? *

- ◯ Menos de 18 anos
- ◯ 18-21 anos
- ◯ 22-25 anos
- ◯ 26 anos ou mais

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

2230457@my.ipleiria.pt Mudar de conta

Não partilhado

* Indica uma pergunta obrigatória

Área de Incidência - Gestão de Palavras-Passe

1 - Utilizar a mesma palavra-passe

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

1.1 - É aceitável utilizar as minhas palavras-passe das redes sociais nas minhas contas de trabalho. *

It's acceptable to use my social media passwords on my work accounts.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

1.2 - É seguro utilizar a mesma palavra-passe para as contas das redes sociais e do trabalho. *

It's safe to use the same password for social media and work accounts.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

1.3 - Utilizo uma palavra-passe diferente para as minhas contas das redes sociais e do trabalho. *

I use a different password for my social media and work accounts.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

2 - Partilhar palavras-passe

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

2.1 - Posso partilhar as minhas palavras-passe do trabalho com colegas. *

I am allowed to share my work passwords with colleagues.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

2.2 - É uma má ideia partilhar as minhas palavras-passe do trabalho, mesmo que um colega as peça. *

It's a bad idea to share my work passwords, even if a colleague asks for it.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

2.3 - Partilho as minhas palavras-passe do trabalho com colegas. *

I share my work passwords with colleagues.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

3 - Utilizar uma palavra-passe forte

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

3.1 - É necessária uma combinação de letras, números e símbolos para as palavras-passe de trabalho. *

A mixture of letters, numbers and symbols is necessary for work passwords.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

3.2 - É seguro ter uma palavra-passe de trabalho apenas com letras. *

It's safe to have a work password with just letters.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

3.3 - Utilizo uma combinação de letras, números e símbolos nas minhas palavras-passe de trabalho. *

I use a combination of letters, numbers and symbols in my work passwords.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

* Indica uma pergunta obrigatória

Área de incidência - Utilização do email

4 - Clicar em links de emails enviados por remetentes conhecidos

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

4.1 - Posso clicar em quaisquer links de emails enviados por pessoas que conheço. *

I am allowed to click on any links in emails from people I know.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

4.2 - É sempre seguro clicar em links de emails enviados por pessoas que conheço. *

It's always safe to click on links in emails from people I know.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

4.3 - Nem sempre clico nos links de emails só porque vêm de alguém que conheço. *

I don't always click on links in emails just because they come from someone I know.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

5 - Clicar em links de emails enviados por remetentes desconhecidos

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

5.1 - Não posso clicar num link de um email enviado por um remetente desconhecido. *

I am not permitted to click on a link in an email from an unknown sender.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

5.2 - Nada de mal pode acontecer se eu clicar em um link de um email enviado por um remetente desconhecido *

Nothing bad can happen if I click on a link in an email from an unknown sender.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

5.3 - Se um email enviado por um remetente desconhecido parecer interessante, clico no link. *

If an email from an unknown sender looks interesting, I click on a link within it.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

6 - Abrir anexos de emails enviados por remetentes desconhecidos

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

6.1 - Posso abrir anexos de emails enviados por remetentes desconhecidos. *

I am allowed to open email attachments from unknown senders.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

6.2 - É arriscado abrir um anexo de email enviado por um remetente desconhecido. *

It's risky to open an email attachment from an unknown sender.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

6.3 - Não abro anexos de email se o remetente for desconhecido para mim. *

I don't open email attachments if the sender is unknown to me.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

2230457@my.ipleiria.pt Mudar de conta

Não partilhado

* Indica uma pergunta obrigatória

Área de incidência - Utilização da Internet

7 - Transferir ficheiros

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

7.1 - Posso descarregar quaisquer ficheiros para o meu computador de trabalho se me ajudarem a fazer o meu trabalho. *

I am allowed to download any files onto my work computer if they help me to do my job.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

7.2 - Pode ser arriscado descarregar ficheiros no meu computador de trabalho. *

It can be risky to download files on my work computer.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

7.3 - Descarrego todos os ficheiros para o meu computador de trabalho que me ajudem a fazer o meu trabalho. *

I download any files onto my work computer that will help me get the job done.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

8 - Aceder a websites duvidosos

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

8.1 - Enquanto estou no trabalho, não devo aceder a determinados websites. *

While I am at work, I shouldn't access certain websites.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

8.2 - Só porque posso aceder a um website no trabalho, não significa que seja seguro. *

Just because I can access a website at work, doesn't mean that it's safe.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

8.3 - Quando acedo à Internet no trabalho, visito qualquer website que queira. *

When accessing the Internet at work, I visit any website that I want to.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

9 - Introduzir informações online

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

9.1 - Posso introduzir qualquer informação em qualquer website se isso me ajudar a fazer o meu trabalho. *

I am allowed to enter any information on any website if it helps me do my job.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

9.2 - Se me ajudar a fazer o meu trabalho, não importa a informação que coloco num website. *

If it helps me to do my job, it doesn't matter what information I put on a website.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

9.3 - Verifico a segurança dos websites antes de introduzir informações. *

I assess the safety of websites before entering information.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

* Indica uma pergunta obrigatória

Área de incidência - Utilização de redes sociais

10 - Definições de privacidade das redes sociais

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

10.1 - Devo rever periodicamente as definições de privacidade das minhas contas nas redes sociais. *

I must periodically review the privacy settings on my social media accounts.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

10.2 - É uma boa ideia rever regularmente as minhas definições de privacidade nas redes sociais. *

It's a good idea to regularly review my social media privacy settings.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

10.3 - Não revejo regularmente as definições de privacidade das minhas redes sociais. *

I don't regularly review my social media privacy settings.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

11 - Considerar consequências

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

11.1 - Não posso ser despedido por algo que publiquei nas redes sociais. *

I can't be fired for something I post on social media.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

11.2 - Não vejo problema em publicar nas redes sociais coisas que eu normalmente não diria em público. *

It doesn't matter if I post things on social media that I wouldn't normally say in public.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

11.3 - Não publico nada nas redes sociais antes de pensar nas consequências negativas. *

I don't post anything on social media before considering any negative consequences.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

12 - Publicar sobre o trabalho

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

12.1 - Posso publicar o que quiser sobre o meu trabalho nas redes sociais. *

I can post what I want about work on social media.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

12.2 - É arriscado publicar certas informações sobre o meu trabalho nas redes sociais. *

It's risky to post certain information about my work on social media.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

12.3 - Publico o que quiser sobre o meu trabalho nas redes sociais. *

I post whatever I want about my work on social media.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

2230457@my.ipleiria.pt Mudar de conta

Não partilhado

* Indica uma pergunta obrigatória

Área de incidência - Dispositivos móveis

13 - Proteger fisicamente dispositivos móveis

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

13.1 - Quando trabalho num local público, devo ter o meu portátil sempre comigo. *

When working in a public place, I have to keep my laptop with me at all times.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

13.2 - Quando estou a trabalhar num café, é seguro deixar o meu portátil sem supervisão durante um minuto. *

When working in a café, it's safe to leave my laptop unattended for a minute.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

13.3 - Quando trabalho num local público, deixo o meu portátil sem vigilância. *

When working in a public place, I leave my laptop unattended.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

14 - Enviar informações sensíveis por Wi-Fi

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

14.1 - Posso enviar ficheiros de trabalho sensíveis através de uma rede Wi-Fi pública. *

I am allowed to send sensitive work files via a public Wi-Fi network.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

14.2 - É arriscado enviar ficheiros de trabalho sensíveis através da rede Wi-Fi pública. *

It's risky to send sensitive work files using a public Wi-Fi network.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

14.3 - Envio ficheiros de trabalho sensíveis através da rede Wi-Fi pública. *

I send sensitive work files using a public Wi-Fi network.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

15 - Espionagem visual

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

15.1 - Ao trabalhar em um documento sensível, preciso de garantir que desconhecidos não consigam ver o ecrã do meu portátil. *

When working on a sensitive document, I must ensure that strangers can't see my laptop screen.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

15.2 - É arriscado aceder a ficheiros de trabalho sensíveis no portátil se desconhecidos puderem ver o meu ecrã. *

It's risky to access sensitive work files on a laptop if strangers can see my screen.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

15.3 - Verifico se desconhecidos não conseguem ver o ecrã do meu portátil quando estou a trabalhar num documento sensível. *

I check that strangers can't see my laptop screen if I'm working on a sensitive document.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Página 7 de 9

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

2230457@my.ipleiria.pt Mudar de conta

Não partilhado

* Indica uma pergunta obrigatória

Área de incidência - Tratamento de informações

16 - Eliminação de impressos sensíveis

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

16.1 - Os documentos impressos sensíveis podem ser eliminados da mesma forma que os não sensíveis. *

Sensitive print-outs can be disposed of in the same way as non-sensitive ones.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

16.2 - É seguro deitar fora documentos impressos sensíveis, colocando-os no caixote do lixo. *

Disposing of sensitive print-outs by putting them in the rubbish bin is safe.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

16.3 - Quando é necessário eliminar documentos impressos sensíveis, certifico-me de que são triturados ou destruídos. *

When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

17 - Inserir suportes amovíveis

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

17.1 - Se eu encontrar uma pen USB num local público, não devo ligá-la ao meu computador de trabalho. *

If I find a USB stick in a public place, I shouldn't plug it into my work computer.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

17.2 - Se eu encontrar uma pen USB num local público, nada de mal pode acontecer se a ligar ao meu computador de trabalho. *

If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

17.3 - Eu não ligaria uma pen USB encontrada num local público ao meu computador de trabalho. *

I wouldn't plug a USB stick found in a public place into my work computer.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

18 - Deixar material sensível

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

18.1 - Posso deixar documentos impressos com informações sensíveis na minha secretária durante a noite. *

I am allowed to leave print-outs containing sensitive information on my desk overnight.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

18.2 - É arriscado deixar documentos impressos que contenham informações sensíveis na minha secretária durante a noite. *

It's risky to leave print-outs that contain sensitive information on my desk overnight.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

18.3 - Deixo documentos impressos que contêm informações sensíveis na minha secretária quando não estou lá. *

I leave print-outs that contain sensitive information on my desk when I'm not there.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Seguinte

Limpar formulário

Avaliação de Comportamentos e Atitudes de Cibersegurança na Comunidade do IPLeiria

* Indica uma pergunta obrigatória

Área de incidência - Comunicação de incidentes

19 - Comunicar comportamentos suspeitos

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

19.1 - Se eu vir alguém a agir de forma suspeita no meu local de trabalho, devo comunicá-lo. *

If I see someone acting suspiciously in my workplace, I should report it.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

19.2 - Se eu ignorar alguém que está a agir de forma suspeita no meu local de trabalho, nada de mal pode acontecer. *

If I ignore someone acting suspiciously in my workplace, nothing bad can happen.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

19.3 - Se eu visse alguém a agir de forma suspeita no meu local de trabalho, faria alguma coisa. *

If I saw someone acting suspiciously in my workplace, I would do something about it.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

20 - Ignorar comportamentos de segurança inadequados de colegas

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

20.1 - Não devo ignorar comportamentos inadequados de segurança dos meus colegas. *

I must not ignore poor security behaviour by my colleagues.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

20.2 - Nada de mal pode acontecer se eu ignorar o comportamento inadequado de segurança de um colega. *

Nothing bad can happen if I ignore poor security behaviour by a colleague.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

20.3 - Se eu visse um colega a ignorar as regras de segurança, não tomaria qualquer medida. *

If I noticed my colleague ignoring security rules, I wouldn't take any action.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

21 - Comunicar todos os incidentes

Escolha a opção que mais se adequa: (1) Discordo totalmente, (2) Discordo, (3) Nem concordo nem discordo, (4) Concordo, (5) Concordo totalmente

21.1 - É opcional comunicar incidentes de segurança. *

It's optional to report security incidents.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

21.2 - É arriscado ignorar os incidentes de segurança, mesmo que eu ache que não são significativos. *

It's risky to ignore security incidents, even if I think they're not significant.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

21.3 - Se me apercebesse de um incidente de segurança, comunicá-lo-ia. *

If I noticed a security incident, I would report it.

	1	2	3	4	5	
Discordo totalmente	○	○	○	○	○	Concordo totalmente

Anterior Enviar Página 9 de 9 Limpar formulário

G

Análise das Áreas da Escala

Este apêndice contém uma análise detalhada das áreas do HAIS-Q, no qual identifica problemas, ameaças, possíveis medidas e exemplos práticos para cada uma delas.

G.1 Módulo 1 - Gestão de Palavras-passe

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com a utilização de palavras-passe.

Problemas:

- Utilizar palavras-passe fracas ou previsíveis.
- Utilizar a mesma palavra-passe para vários serviços.
- Partilha de palavras-passe com colegas, amigos ou familiares.

Ameaças:

- **Roubo de identidade** - Utilizar a mesma palavra-passe para várias contas se uma dessas for comprometida, o atacante pode tentar utilizar a mesma palavra-passe para aceder a outras contas do utilizador.
- **Ataques de força bruta** - Utilizar uma palavra-passe fraca ou previsível facilita os ataques de força bruta, onde os atacantes que tentam todas as combinações possíveis ou recorrem a programas para o fazer.
- **Acessos não autorizados** - Armazenar palavras-passe no navegador ou dispositivo sem proteção adequada. Se o dispositivo for roubado ou comprometido, as credenciais armazenadas podem ser extraídas.

Medidas:

- Utilizar palavras-passe fortes, com pelo menos 12 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.

- Não partilhar palavras-passe com terceiros.
- Utilizar uma palavra-passe diferente para cada serviço.
- Alterar frequentemente as palavras-passe ou caso desconfie de comprometimento.
- Ativar autenticação multi-fator sempre que possível.
- Utilizar gestores de palavras-passe em vez de as armazenar no navegador.

Exemplos práticos:

Noticia: Ataque de ransomeware, em Maio de 2021, à empresa Colonial Pipeline devido ao comprometimento de uma palavra-passe de uma conta VPN que não tinha autenticação multi-fator ativa.
Fontes:
https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
https://www.jornaldenegocios.pt/empresas/energia/detalhe/colonial-pipeline-pagou-5-milhoes-de-dolares-a-hackers-que-atacaram-oleoduto

Links úteis:

- Verificar se um endereço de email já esteve presente em alguma fuga de dados. (https://haveibeenpwned.com/)
- Verificar a segurança das palavras-passe utilizadas, indicando quanto tempo demoraria a ser descoberta. (https://www.security.org/how-secure-is-my-password/)

G.2 Módulo 2 – Utilização do Email

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com a utilização do email.

Problemas:

- Clicar em links enviados por remetentes desconhecidos.
- Abrir anexos enviados por remetentes desconhecidos.

Ameaças:

- **Roubo de credenciais ou dados pessoais** - Clicar num *link* malicioso num email falso (*phishing*) que imita uma entidade legítima.
- **Instalação de *malware* nos dispositivos** - Abrir anexos de emails desconhecidos ou clicar em *links* em mensagens de spam.

Medidas:

- Desconfiar de emails de remetentes desconhecidos ou suspeitos.
- Verificar a autenticidade do remetente e o domínio do email.

- Evitar clicar em *links* e abrir anexos de remetentes desconhecidos. Antes de clicar em um *link* passar o cursor sobre ele para visualizar o URL.
- Evitar expor o endereço de email em fóruns ou redes sociais para reduzir o risco de spam.
- Marcar emails suspeitos como spam para que o sistema os filtre automaticamente.
- Ficar atento a erros de ortografia e gramática, frequentemente presentes em emails de *phishing*.

Exemplos práticos:

Noticia: Notícia, fevereiro de 2020, sobre uma empresária que foi vítima de um ataque de *phishing*, possivelmente *spear phishing*. Esta empresária recebeu um email, supostamente do seu assistente, para pagar uma fatura da renovação de um imóvel. Com a vítima ter por hábito investir em imóveis não suspeitou do email e pagou 400 mil dólares ao atacante. Mais tarde, o seu contabilista é que notou que o email não correspondia ao email do assistente.

Fonte:

https://www.cbsnews.com/news/barbara-corcoran-loses-388700-dollars-phishing-scam-shark-tank/

Comparação email *phishing* vs email legítimo:

Os emails apresentados na Figura G.1, correspondem a um email de *phishing* (Figura G.1a) e a um email legítimo (Figura G.1b).

No caso do email de *phishing* (Figura G.1a), verifica-se a presença de um sentido de urgência, alegando que, devido a uma atividade suspeita, a conta foi temporariamente restringida e poderá ser bloqueada caso os dados não sejam confirmados através de um link fornecido, no prazo de 24 horas.

Já o email legítimo (Figura G.1b) apresenta um sentido meramente informativo, notificando a deteção de um acesso incomum, com indicação da data e hora da ocorrência. Caso tenha sido o próprio utilizador a realizar o acesso, não é necessária qualquer ação. Caso contrário, o utilizador é orientado a seguir os passos indicados. Adicionalmente, o email avisa para não clicar em links e reforça que não são solicitadas informações sensíveis.

Vídeo campanha do CNCS sobre phishing:

https://youtu.be/mxOcGFRXVLY?si=tRH7XreXfo_Uug-W

Assunto: ⚠ Atualização Urgente da Sua Conta - Ação Necessária

De: Suporte Técnico suporte@seguranca-bancaria.com
Para: [Seu Endereço de Email]

Caro(a) Cliente,

Detectámos uma atividade suspeita na sua conta e, por motivos de segurança, o seu acesso foi temporariamente restrito. Para evitar o bloqueio definitivo, é necessário que confirme os seus dados imediatamente.

Por favor, clique no link abaixo e siga as instruções para reativar a sua conta:

🔗 Aceder à minha conta

Caso não complete este procedimento nas próximas 24 horas, a sua conta será suspensa por tempo indeterminado.

Agradecemos a sua atenção e colaboração.

Atenciosamente,
Equipa de Segurança
Banco XYZ

(**a**) *Email de phishing*

Assunto: Alerta de Segurança: Atividade Incomum na Sua Conta

De: Banco XYZ noreply@bancoxyz.pt
Para: [Seu Endereço de Email]

Caro(a) [Nome do Cliente],

Detetámos uma tentativa de acesso incomum à sua conta bancária no dia **[data]**, às **[hora]**, a partir de um dispositivo ou localização que não reconhecemos.

Se foi o(a) senhor(a) que tentou aceder, não é necessária qualquer ação. No entanto, se não reconhece esta atividade, recomendamos que tome as seguintes medidas imediatamente:

1️⃣ **Aceda diretamente ao site do Banco XYZ digitando** www.bancoxyz.pt **no seu navegador.**
2️⃣ **Inicie sessão na sua conta e verifique se há movimentos não autorizados.**
3️⃣ **Se necessário, altere a sua palavra-passe e ative medidas adicionais de segurança, como a autenticação de dois fatores.**

⚠ **Nunca clique em links ou forneça dados pessoais por email.** O Banco XYZ nunca solicita informações sensíveis por email, SMS ou telefone.

Se precisar de assistência, entre em contacto connosco através do número oficial **[Número de Suporte]** ou dirija-se à agência mais próxima.

Atenciosamente,
Equipa de Segurança Bancária
Banco XYZ

(**b**) *Email legítimo*

Figura G.1: *Email de phishing vs. email legítimo.*

G.3 Módulo 3 – Utilização da Internet

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com a utilização da Internet.

Problemas:

- Transferir qualquer tipo de ficheiros ou software.
- Aceder a *websites* duvidosos.
- Inserir de informações online.

Ameaças:

- **Instalação de *malware*** - Transferir ficheiros ou software de fontes não confiáveis. Aceder a *websites* com conteúdos suspeitos ou potencialmente maliciosos.
- **Roubo de identidade** - Inserir informações pessoais ou sensíveis em *websites* não seguros.

Medidas:

- Navegar em *websites* seguros, verificar se utilizam HTTPS.
- Não transferir ficheiros ou software de fontes desconhecidas.
- Manter antivírus e anti-*malware* atualizados.

Exemplos práticos:

Demonstração: Vídeo a demonstrar uma tentativa de autenticação num site sem HTTPS, com captura de pacotes com WireShark[1], de forma ver que as credenciais são passadas em texto limpo.
Site:
http://www.monumentos.gov.pt/Site/Account/Login.aspx

G.4 Módulo 4 – Utilização de Redes Sociais

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com a utilização de redes sociais.

Problemas:

- Não verificar as definições de privacidade.
- Publicar sobre tudo sem considerar as consequências.

Ameaças:

[1] WireShark: `www.wireshark.org`

- **Engenharia social** - Publicação de conteúdos sem considerar as consequências. Divulgação de informações pessoais, como morada e número de telefone. Pode permitir que atacantes usem esses dados para criar perfis falsos ou cometer fraudes.
- **Riscos à segurança pessoal** - Publicar informações detalhadas sobre rotina, localização ou bens pode atrair pessoas mal-intencionadas.
- **Impacto na reputação e oportunidades profissionais** - Publicações inadequadas ou controversas podem prejudicar a imagem pessoal.

Medidas:

- Ajustar as definições de privacidade para restringir o acesso às publicações apenas a amigos ou pessoas conhecidas.
- Evitar partilhar informações sensíveis, como o número de telefone, dados financeiros ou localização em tempo real.
- Não aceitar pedidos de amizade de desconhecidos.
- Rever publicações antigas para remover conteúdos que possam ser considerados controversos ou sensíveis.
- Denunciar e bloquear utilizadores abusivos.

Exemplos práticos:

Notícia 1: Uma notícia[2] para demonstrar como a excessiva divulgação de dados, pode ser explorada para fraudes sofisticadas. A notícia, de janeiro de 2024, é sobre uma empresa britânica de design e engenharia, que sofreu um ataque de *deepfake*. O ataque aconteceu, porque um funcionário recebeu um email aparentemente enviado pelo diretor financeiro, a solicitar uma transferência confidencial. Embora tenha desconfiado do email, o funcionário acabou por ceder, e transferiu cerca de vinte cinco milhões de dólares, após participar numa videoconferência. No entanto, as pessoas com quem conversou não eram reais.
Fonte:
https://www.jornaldenegocios.pt/empresas/detalhe/como-um-deepfake-custou-25-milhoes-de-dolares-a-empresa-por-detras-da-opera-de-sydney

Notícia 2: Notícia, de dezembro de 2024, a alertar sobre a existência de páginas e perfis falsos do patriarca de Lisboa, Rui Valério, a pedir donativos.
Fonte:
https://observador.pt/2024/12/02/patriarcado-alerta-para-perfil-falso-do-patriarca-de-lisboa-a-pedir-donativos/

Notícia 3: Notícia, de novembro de 2024, a alertar sobre a existência de páginas e perfis

[2] **Nota:** Não foi possível incluir a notícia no vídeo, pois o seu conteúdo violava as políticas de utilização da plataforma IA utilizada para criar a pessoa a explicar os conteúdos.

falsos do Bispo Dom Virgílio Antunes a pedir dinheiro para uma suposta campanha solidária.
Fonte:
https://rr.pt/noticia/religiao/2024/11/12/perfil-falso-de-bispo-de-coimbra-tera-tentado-burlar-pessoas/401255/

Vídeo, do CNCS, de boas práticas na utilização de redes sociais:
https://www.youtube.com/watch?v=9OdEQlvAOb4

G.5 Módulo 5 – Dispositivos móveis

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com os dispositivos móveis.

Problemas:

- Deixar dispositivos sem vigilância em locais públicos.
- Utilizar dispositivos em locais públicos para consultar informações confidenciais.
- Utilizar redes públicas para enviar informações sensíveis.

Ameaças:

- **Interceção de comunicações** - Utilizar redes públicas sem proteção adequada, os dados podem ser intercetados.
- **Espionagem visual** - Em locais públicos, as pessoas podem observar o ecrã e obter informações.
- **Roubo de dispositivos** - Em locais públicos, os dispositivos podes ser furtados, expondo os dados armazenados.
- **Acessos não autorizados** - Deixar o dispositivo desbloqueado e sem vigilância pode permitir que acedam aos dados.

Medidas:

- Evitar utilizar a redes públicas.
- Utilizar uma VPN ao conectar-se a redes públicas, para encriptar os dados de navegação.
- Evitar que pessoas próximas visualizem informações no ecrã.
- Bloquear o ecrã ao deixar o dispositivo sem supervisão.
- Evitar abrir documentos confidenciais em locais visíveis.

Exemplos práticos:

Noticia 1: Notícia, de janeiro de 2025, sobre uma mulher que fez compras online utilizando uma rede Wi-Fi pública, o que levou à comprometimento da sua conta bancária.

Descobrindo, mais tarde, ao aceder à sua aplicação bancária que todo o seu dinheiro tinha desaparecido.
Fonte:
https://www.dailymail.co.uk/news/article-14311199/Online-shop-scam-Melbourne-hospital.html

Notícia 2: Notícia sobre uma pessoa que teve o seu telemóvel roubado, na altura a vítima não considerou um problema, por ter o dispositivo bloqueado. No entanto, mais tarde, descobriu que o dinheiro foi retirado da sua conta bancária. Durante a investigação, verificou-se que o código da conta foi inserido corretamente, o que sugere que a vítima foi alvo de espionagem visual. O atacante provavelmente observou a vítima enquanto inseria o código e, posteriormente, roubou o telemóvel, utilizando o código para aceder à conta.
Fonte:
https://www.bbc.com/news/business-64240140

Vídeo, do CNCS, sobre espionagem visual:
https://www.youtube.com/watch?v=FLv0Hd9_xY0

Vídeo, do CNCS, sobre a utilização de redes públicas:
https://www.youtube.com/watch?v=lJxjBVNfVFE

G.6 Módulo 6 – Tratamento de Informações

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com o tratamento de informações, mais concretamente documentos físicos e dispositivos USB.

Problemas:

- Não eliminar corretamente materiais sensíveis.
- Deixar materiais sensíveis expostos e sem vigilância.
- Inserir dispositivos USB desconhecidos.

Ameaças:

- **Instalação de *malware*** - Ligar dispositivos USB desconhecidos a computadores ou outros equipamentos.
- **Exposição de informações confidenciais** - Deixar documentos sensíveis em áreas públicas ou descarta-los sem destruição adequada. Pode levar a acessos não autorizados a dados pessoais, financeiros ou profissionais.

Medidas:

- Evitar utilizar dispositivos USB desconhecidos.

- Armazenar documentos sensíveis em locais seguros.
- Destruir adequadamente documentos confidenciais, utilizando, por exemplo, trituradores de papel.

Exemplos práticos:

Noticia 1: Notícia, de 2016, sobre um incidente, na Austrália, onde foram deixados dispositivos USB, em caixas de correio dos residentes, que continham *malware*, que ao serem ligadas aos computadores ativam ofertas fraudulentas e programas maliciosos.
Fonte:
https://www.bbc.com/news/technology-37431335

Notícia 2: Notícia, de 2024, sobre a Segurança Social descartar documentos confidenciais sem serem destruídos e ainda os deixar sem vigilância na via pública quando estavam a ser carregados para uma carrinha.
Fonte:
https://www.rtp.pt/noticias/pais/a-prova-dos-factos-seguranca-social-deixa-documentos-confidenciais-expostos_v1580821

Vídeo, do CNCS, sobre utilizar dispositivos USB desconhecidos:
https://www.youtube.com/watch?v=81lBT0Yubmw

G.7 Módulo 7 – Comunicação de Incidentes

Esta secção apresenta os problemas, ameaças, possíveis medidas de proteção e exemplos práticos relacionados com a comunicação de incidentes.

Problemas:

- Não reportar incidentes de segurança.
- Desvalorizar as práticas de segurança.

Ameaças:

- **Propagação de ataques** - Um ataque não comunicado pode espalhar-se pela rede, infetando mais dispositivos e comprometendo sistemas essenciais.
- **Negligência nas práticas de segurança** - Desconsiderar as boas práticas de segurança, considerando-as exageros ou inconvenientes, aumenta a probabilidade de falhas de segurança.

Medidas:

- **Adotar medidas de segurança como** - Palavras-passe fortes; utilizar antivírus; utilizar VPN em redes públicas; não utilizar dispositivos USB desconhecidos; e comunicar qualquer irregularidade.

Exemplos práticos:

Vídeo, do CNCS, sobre as boas práticas de segurança:
https://youtu.be/NugciPptTvg?si=d3UtTItYlcldASmg

H

Perguntas do Quiz

Este apêndice apresenta as perguntas utilizadas na elaboração do Quiz destinado a avaliar a retenção dos conhecimentos transmitidos durante a aula aberta.

1. O que deve fazer se suspeitar que um ataque informático ocorreu na sua organização?
   a) Ignorar, pois pode ser apenas um erro do sistema.
   b) Reiniciar o computador para tentar resolver o problema sozinho.
   c) Comunicar imediatamente ao responsável pela segurança informática.
   d) Publicar nas redes sociais para alertar os colegas.

   Resposta correta: c)

2. Como se pode identificar um email de *phishing*?
   a) O remetente é desconhecido ou suspeito.
   b) Contém erros ortográficos ou gramaticais.
   c) Inclui *links* que não correspondem ao domínio real da empresa.
   d) Todas as anteriores.

   Resposta correta: d)

3. Por que motivo não se deve ligar dispositivos USB desconhecidos ao computador?
   a) Podem conter *malware* que compromete o sistema.
   b) A porta USB pode deixar de funcionar depois de o remover.
   c) O sistema pode não reconhecer o dispositivo.
   d) Os USB desconhecidos não funcionam corretamente.

   Resposta correta: a)

4. Qual é uma das formas mais seguras de navegar na Internet?
   a) Utilizar sempre redes Wi-Fi públicas para evitar custos de dados móveis.

b) Desativar o antivírus para melhorar a velocidade da navegação.
c) Instalar software de qualquer fonte disponível na Internet.
d) Verificar se os sites utilizam HTTPS antes de inserir informações pessoais.

Resposta correta: d)

5. Qual dos seguintes é um risco ao utilizar redes Wi-Fi públicas sem proteção?
   a) Os dados podem ser intercetados por atacantes.
   b) Consumo elevado de bateria do dispositivo.
   c) A rede pode ser lenta.
   d) O dispositivo pode desligar-se automaticamente da rede.

   Resposta correta: a)

6. Qual é uma das principais razões pelo qual não se deve utilizar a mesma palavra-passe em vários serviços?
   a) É mais difícil de lembrar.
   b) Pode ser comprometida e utilizada para aceder a outras contas.
   c) Não é permitido pela maioria dos sites.
   d) Não há problema em reutilizar se for uma palavra-passe forte.

   Resposta correta: b)

7. Qual é uma boa prática para proteger a sua privacidade nas redes sociais?
   a) Aceitar pedidos de amizade de qualquer pessoa.
   b) Partilhar a localização em tempo real em todas as publicações.
   c) Configurar a privacidade do perfil para permitir que apenas amigos vejam as publicações.
   d) Publicar informações pessoais para manter os amigos informados.

   Resposta correta: c)

I

Definições dos Conceitos Apresentados

Neste apêndice apresentam-se as definições dos conceitos utilizados na apresentação da estratégia de sensibilização.

Cibersegurança: Conjunto de medidas e ações destinadas a proteger redes, sistemas e pessoas, com o objetivo de prevenir, monitorizar, detetar, analisar e corrigir ameaças. Visa garantir a confidencialidade, integridade e disponibilidade da informação.

Engenharia Social: Estratégia para manipular e enganar pessoas, com o objetivo de obter informações sensíveis. O atacante finge ser uma marca conhecida, colega ou amigo.

Deepfake: Utiliza inteligência artificial para recriar pessoas em vídeos extremamente realista e difíceis de identifica como falsos, com o objetivo de criar situações falsas para enganar pessoas.

Phishing: Técnica de engenharia social que utiliza emails, mensagens de texto e chamadas de voz que parecem legítimos, com o objetivo de levar as pessoas a divulgar informações sensíveis ou clicar em ligações desconhecidas.

Tipos de phishing:

- **Spear Phishing** - Ataque direcionado a um alvo específico, onde o atacante recolhe informação sobre o alvo e personaliza as mensagens enviadas.
- **Smishing** - Ataque que utiliza mensagens de texto (SMS), onde os atacantes fingem ser uma empresa ou pessoa respeitável.
- **Vishing** - Ataque que utiliza chamadas telefónicas, onde os atacantes fingem ser entidades de confiança e tentam persuadir a vítimas a revelar informações sensíveis.
- **Quishing** - Ataque que utiliza códigos QR, onde os atacantes criam e divulgam

códigos QR que contêm links maliciosos.

Malware: Programa malicioso que causa danos a computadores ou redes. Pode ser instalado por um atacante que conseguiu acesso à rede ou por alguém que inocentemente clicou num link malicioso ou transferiu um anexo infetado.

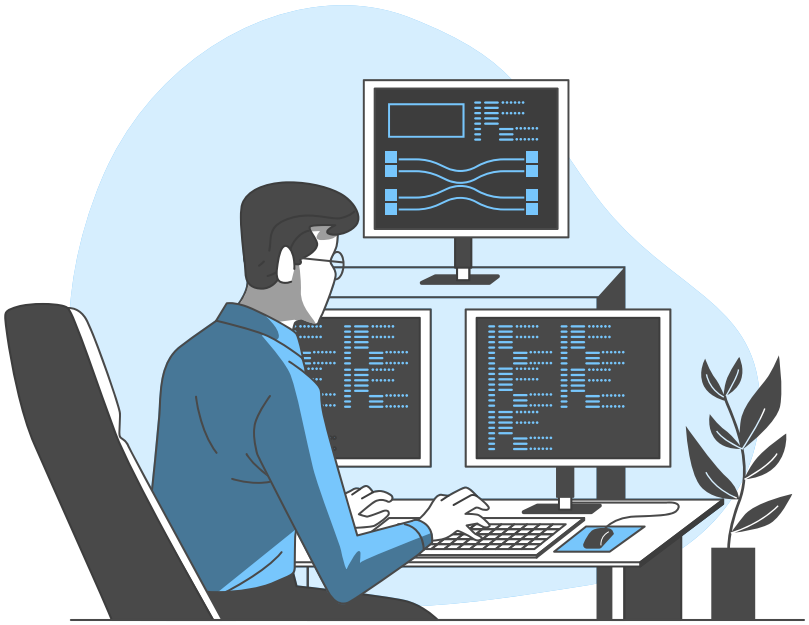
Exemplos de malware:

- **Ransomware** - Ataque que bloqueia o acesso a dispositivos, dados e sistemas, onde os atacantes exigem o pagamento de um resgate para desbloquear o acesso.
- **Spyware** - Programa que se instala num dispositivo sem o consentimento do utilizador. Monitoriza comportamentos, recolhe informações, altera as definições e diminui o desempenho do dispositivo.

J
Apresentação da Sessão de 45 minutos

Este apêndice contém a apresentação utilizada na sessão de 45 minutos efetuada no curso de Gestão.

POLITÉCNICO DE LEIRIA



Cibersegurança

Comportamentos de Risco

Cristiana Sousa
Estudante do Mestrado em
Cibersegurança e Informática Forense

Conceitos

01 Cibersegurança

02 Engenharia Social

03 Deepfake

04 Malware

Enquadramento

01

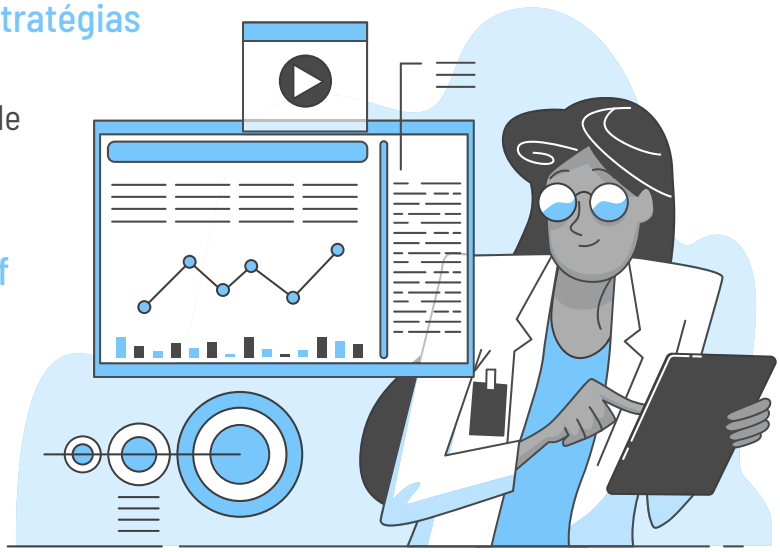
Avaliar e implementar estratégias de consciencialização

Estudantes de licenciatura de áreas não técnicas

02

Escala Human Aspects of Information Security Questionnaire (HAIS-Q)

Avalia sete áreas da cibersegurança



Gestão de Palavras-passe

Utilizar a mesma palavra-passe em vários serviços

- **Risco:** Roubo de identidade

Palavras-passe fracas ou previsíveis

- **Risco:** Facilitam ataques de força-bruta

Medidas:

Palavra-passe **diferente** para cada serviço.
Palavras-passe **fortes**.
Gestores de palavras-passe. Ex.: KeePassXC, NordPass, Bitwarden, ...

Utilização do Email

Phishing

- **Riscos:** Roubo de dados pessoais ou instalação de *malware*.
- **Causa:** Clicar em links ou abrir anexos.

Sabias que?

O **smishing** é por mensagens SMS.
O **vishing** é por chamadas telefónicas.
O **quishing** é por códigos QR.
O ***spear phishing*** é personalizado para um alvo específico. O atacante recolhe informações sobre a vítima e utiliza essas informações para tornar a mensagem mais convincente.

Cuidados

01 Desconfiar de emails

02 Ficar atento à escrita

03 Marcar emails como *spam*

Exemplos práticos – Email phishing?

Assunto: ⚠ Atualização Urgente da Sua Conta - Ação Necessária

De: Suporte Técnico suporte@seguranca-bancaria.com
Para: [Seu Endereço de Email]

Caro(a) Cliente,

Detectámos uma atividade suspeita na sua conta e, por motivos de segurança, o seu acesso foi temporariamente restrito. Para evitar o bloqueio definitivo, é necessário que confirme os seus dados imediatamente.

Por favor, clique no link abaixo e siga as instruções para reativar a sua conta:

Aceder à minha conta

Caso não complete este procedimento nas próximas 24 horas, a sua conta será suspensa por tempo indeterminado.

Agradecemos a sua atenção e colaboração.

Atenciosamente,
Equipa de Segurança
Banco XYZ

Exemplos práticos – Email phishing?

Assunto: ⚠ Atualização Urgente da Sua Conta - Ação Necessária

De: Suporte Técnico suporte@seguranca-bancaria.com
Para: [Seu Endereço de Email]

Caro(a) Cliente,

Detectámos uma atividade suspeita na sua conta e, por motivos de segurança, o seu acesso foi temporariamente restrito. Para evitar o bloqueio definitivo, é necessário que confirme os seus dados imediatamente.

Por favor, clique no link abaixo e siga as instruções para reativar a sua conta:

Aceder à minha conta

Caso não complete este procedimento nas próximas 24 horas, a sua conta será suspensa por tempo indeterminado.

Agradecemos a sua atenção e colaboração.

Atenciosamente,
Equipa de Segurança
Banco XYZ

Indicadores de phishing

- Sentido de **urgência**.
- **Conta restrita** com possibilidade de ficar **bloqueada**.
- Indicação para **clicar num link**.

Exemplos práticos – Email phishing?

Assunto: Alerta de Segurança: Atividade Incomum na Sua Conta

De: Banco XYZ noreply@bancoxyz.pt
Para: [Seu Endereço de Email]

Caro(a) [Nome do Cliente],

Detetámos uma tentativa de acesso incomum à sua conta bancária no dia **[data]**, às **[hora]**, a partir de um dispositivo ou localização que não reconhecemos.

Se foi o(a) senhor(a) que tentou aceder, não é necessária qualquer ação. No entanto, se não reconhece esta atividade, recomendamos que tome as seguintes medidas imediatamente:

1. **Aceda diretamente ao site do Banco XYZ digitando www.bancoxyz.pt no seu navegador.**
2. **Inicie sessão na sua conta e verifique se há movimentos não autorizados.**
3. **Se necessário, altere a sua palavra-passe e ative medidas adicionais de segurança, como a autenticação de dois fatores.**

⚠ **Nunca clique em links ou forneça dados pessoais por email.** O Banco XYZ nunca solicita informações sensíveis por email, SMS ou telefone.

Se precisar de assistência, entre em contacto connosco através do número oficial **[Número de Suporte]** ou dirija-se à agência mais próxima.

Atenciosamente,
Equipa de Segurança Bancária
Banco XYZ

Exemplos práticos – Email phishing?

Assunto: Alerta de Segurança: Atividade Incomum na Sua Conta

De: Banco XYZ noreply@bancoxyz.pt
Para: [Seu Endereço de Email]

Caro(a) [Nome do Cliente],

Detetámos uma tentativa de acesso incomum à sua conta bancária no dia **[data]**, às **[hora]**, a partir de um dispositivo ou localização que não reconhecemos.

Se foi o(a) senhor(a) que tentou aceder, não é necessária qualquer ação. No entanto, se não reconhece esta atividade, recomendamos que tome as seguintes medidas imediatamente:

1. **Aceda diretamente ao site do Banco XYZ digitando www.bancoxyz.pt no seu navegador.**
2. **Inicie sessão na sua conta e verifique se há movimentos não autorizados.**
3. **Se necessário, altere a sua palavra-passe e ative medidas adicionais de segurança, como a autenticação de dois fatores.**

⚠ **Nunca clique em links ou forneça dados pessoais por email.** O Banco XYZ nunca solicita informações sensíveis por email, SMS ou telefone.

Se precisar de assistência, entre em contacto connosco através do número oficial **[Número de Suporte]** ou dirija-se à agência mais próxima.

Atenciosamente,
Equipa de Segurança Bancária
Banco XYZ

Indicadores de legítimo

- Sentido **informativo**.
- Indicação de **data e hora da ocorrência**.
- Indicação para **não clicar** em links e que **não solicitam** informações sensíveis.
- Indicação dos **passos a seguir** caso não seja o autor da ocorrência.

Utilização da Internet

Transferir ficheiros ou software de fontes desconhecidas

- **Risco:** Instalação de malware.

Não verificar a segurança do *websites*

- **Ricos:** Roubo de dados.

Medidas:

Só transferir ficheiros ou software de **fontes oficiais**.
Verificar se os ***websites* são seguros** (HTTPS) antes de inserir informações.

Utilização de Redes Sociais

Não verificar definições de privacidade

- **Risco:** Facilita ataques de engenharia social.

Não considerar as consequências

- **Risco:** Impacto na reputação.

Medidas:

Ajustar definições de **privacidade**.
Evitar partilhar informações sensíveis.
Rever publicações antigas.

Dispositivos Móveis

Utilizar redes públicas

- **Risco:** Interceção de comunicações.

Utilizar dispositivos em locais públicos

- **Riscos:** Espionagem visual, roubo de dispositivos ou acessos não autorizados.

Medidas:

Utilizar VPN ao conectar-se a redes públicas.
Evitar que pessoas próximas **visualizem informações** no ecrã.
Bloquear o ecrã ao deixar o dispositivo sem vigilância.

Tratamento de Informações

Utilizar dispositivos USB desconhecidos

- **Risco:** Instalação de *malware*.

Deixar documentos expostos e não os destruir ao descartá-los

- **Risco:** Exposição de informações confidenciais.

Medidas:

Não utilizar dispositivos USB desconhecidos.
Armazenar documentos sensíveis em locais seguros.
Destruir adequadamente documentos confidenciais.

Comunicação de Incidentes

Não comunicar incidentes

- **Risco:** Propagação de ataques.

Desvalorizar práticas de segurança

- **Risco:** Aumenta a probabilidade de falhas de segurança.

Medidas:

Comunicar qualquer irregularidade.
Adotar medidas de segurança.

Questões?

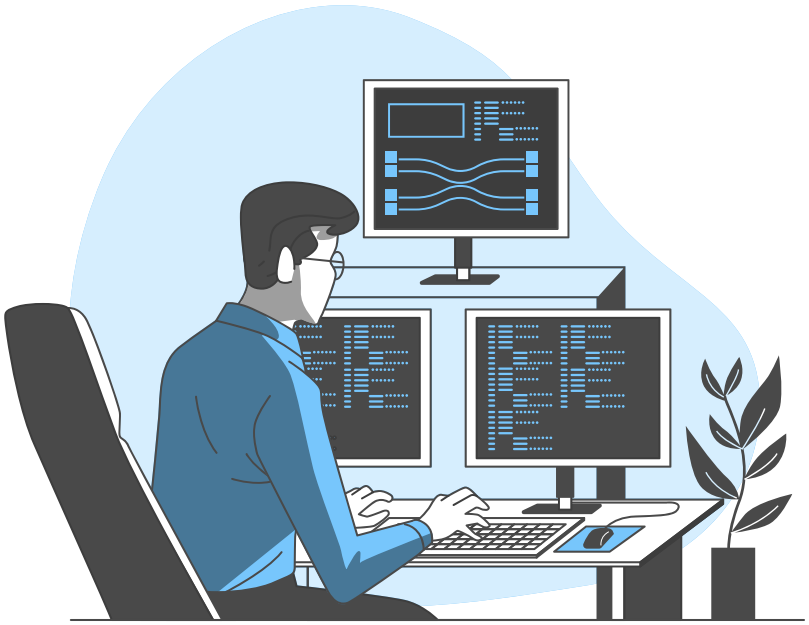
Obrigado!

K

Apresentação da Sessão de 90 minutos

Este apêndice contém a apresentação utilizada na sessão de 90 minutos efetuada no curso de Marketing.

POLITÉCNICO DE LEIRIA



Cibersegurança

Comportamentos de Risco

Cristiana Sousa
Estudante do Mestrado em
Cibersegurança e Informática Forense

Cibersegurança

01 **Medidas & Ações**
Proteger redes, sistemas e pessoas

02 **Objetivo**
Prevenir, monitorizar, detetar, analisar e corrigir ameaças

Engenharia Social

01

Estratégia

Manipular e enganar pessoas
para obter informações sensíveis

02

Atacante

Finge ser uma marca
conhecida, colega ou amigo

Engenharia Social – Deepfake

Inteligência Artificial

Recria pessoas em
vídeos

Resultado

Vídeos realistas e difíceis
de identificar como falsos

Objetivo

Criar situações falsas
para enganar pessoas

Engenharia Social – Phishing

Spear Phishing

- Alvo específico
- Recolhe informação sobre o alvo
- Personaliza as mensagens enviadas

Smishing

- Utiliza mensagens de texto (SMS)
- Atacantes fingem ser uma empresa ou pessoa respeitável

Vishing

- Utiliza chamadas telefónicas
- Atacantes fingem ser entidades de confiança
- Persuadem a vítimas a revelar informações sensíveis

Quishing

- Utiliza códigos QR
- Atacantes criam e divulgam códigos QR que contêm links maliciosos

Malware

01 **Programa malicioso**
Causa danos a computadores ou redes

02 **Instalado por atacante**
Conseguiu acesso à rede

03 **Instalado por pessoas**
Clicou num link malicioso ou transferiu um anexo infectado

Malware

Ransomware

- Bloqueia o acesso a dispositivos, dados e sistemas
- Exige pagamento de um resgate para desbloquear o acesso

Spyware

- Instala-se num dispositivo sem o consentimento do utilizador
- Monitoriza comportamentos, recolhe informações, altera as definições e diminui o desempenho

Enquadramento

01

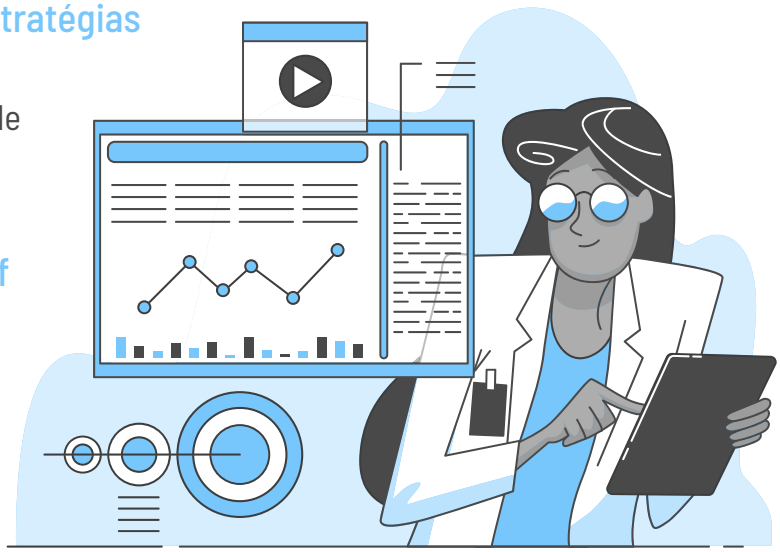
Avaliar e implementar estratégias de consciencialização

Estudantes de licenciatura de áreas não técnicas

02

Escala Human Aspects of Information Security Questionnaire (HAIS-Q)

Avalia sete áreas da cibersegurança



Gestão de Palavras-passe

Utilizar a mesma palavra-passe em vários serviços

- **Risco:** Roubo de identidade

Palavras-passe fracas ou previsíveis

- **Risco:** Facilitam ataques de força-bruta

Medidas:

Palavra-passe **diferente** para cada serviço.
Palavras-passe **fortes**.
Gestores de palavras-passe. Ex.: KeePassXC, NordPass, Bitwarden, ...
Utilizar autenticação **multi-fator**.

Exemplos práticos - Notícias

Maio de 2021

- **Empresa:** Colonial Pipeline (Empresa de produtos petrolíferos dos Estados Unidos).
- **Ataque:** Ransomware.
- **Causa:** Palavra-passe comprometida de uma conta VPN, que não tinha autenticação multi-fator ativa.
- **Consequências**: Empresa pagou cerca de **5 milhões de dólares** aos hackers.
- **Recuperação:** Após o pagamento o sistema demorou a ser restaurado e a empresa teve de recorrer aos bakups do sistema para retomar o funcionamento pleno.

Fontes: Reuters e Jornal de Negócios

Utilização do Email

Phishing

- **Riscos:** Roubo de dados pessoais ou instalação de *malware*.
- **Causa:** Clicar em links ou abrir anexos.

Medidas

Desconfiar de emails de remetentes desconhecidos.
Ficar atento à forma como está **escrito**.
Marcar emails como spam.

Boas práticas

Fonte: https://youtu.be/mxOcGFRXVLY?si=tRH7XreXfo_Uug-W

Exemplos práticos – Notícias

Fevereiro de 2020

- **Vítima:** Barbara Corcoran, empresária e investidora do programa Shark Tank.
- **Ataque:** Phishing.
- **Método:** **Email falso** enviado em nome do seu assistente, com uma **fatura fraudulenta** para renovação de uma imóvel.
- **Motivo do Engano**: Barbara investe em imóveis e não suspeitou do pedido.
- **Consequências:** Pagou cerca de **400 mil dólares** sem verificar a autenticidade do email.
- **Descoberta da Fraude:** Contabilista notou um **erro no endereço de email** do assistente.

Fonte: CBS News

Exemplos práticos – Email phishing?

Assunto: ⚠ Atualização Urgente da Sua Conta - Ação Necessária

De: Suporte Técnico suporte@seguranca-bancaria.com
Para: [Seu Endereço de Email]

Caro(a) Cliente,

Detectámos uma atividade suspeita na sua conta e, por motivos de segurança, o seu acesso foi temporariamente restrito. Para evitar o bloqueio definitivo, é necessário que confirme os seus dados imediatamente.

Por favor, clique no link abaixo e siga as instruções para reativar a sua conta:

🔗 Aceder à minha conta

Caso não complete este procedimento nas próximas 24 horas, a sua conta será suspensa por tempo indeterminado.

Agradecemos a sua atenção e colaboração.

Atenciosamente,
Equipa de Segurança
Banco XYZ

Exemplos práticos – Email phishing?

Assunto: ⚠ Atualização Urgente da Sua Conta - Ação Necessária

De: Suporte Técnico suporte@seguranca-bancaria.com
Para: [Seu Endereço de Email]

Caro(a) Cliente,

Detectámos uma atividade suspeita na sua conta e, por motivos de segurança, o seu acesso foi temporariamente restrito. Para evitar o bloqueio definitivo, é necessário que confirme os seus dados imediatamente.

Por favor, clique no link abaixo e siga as instruções para reativar a sua conta:

Aceder à minha conta

Caso não complete este procedimento nas próximas 24 horas, a sua conta será suspensa por tempo indeterminado.

Agradecemos a sua atenção e colaboração.

Atenciosamente,
Equipa de Segurança
Banco XYZ

Indicadores de phishing

- Sentido de **urgência**.
- **Conta restrita** com possibilidade de ficar **bloqueada**.
- Indicação para **clicar num link**.

Exemplos práticos – Email phishing?

Assunto: Alerta de Segurança: Atividade Incomum na Sua Conta

De: Banco XYZ noreply@bancoxyz.pt
Para: [Seu Endereço de Email]

Caro(a) [Nome do Cliente],

Detetámos uma tentativa de acesso incomum à sua conta bancária no dia **[data]**, às **[hora]**, a partir de um dispositivo ou localização que não reconhecemos.

Se foi o(a) senhor(a) que tentou aceder, não é necessária qualquer ação. No entanto, se não reconhece esta atividade, recomendamos que tome as seguintes medidas imediatamente:

1. **Aceda diretamente ao site do Banco XYZ digitando** www.bancoxyz.pt **no seu navegador.**
2. **Inicie sessão na sua conta e verifique se há movimentos não autorizados.**
3. **Se necessário, altere a sua palavra-passe e ative medidas adicionais de segurança, como a autenticação de dois fatores.**

⚠ **Nunca clique em links ou forneça dados pessoais por email.** O Banco XYZ nunca solicita informações sensíveis por email, SMS ou telefone.

Se precisar de assistência, entre em contacto connosco através do número oficial **[Número de Suporte]** ou dirija-se à agência mais próxima.

Atenciosamente,
Equipa de Segurança Bancária
Banco XYZ

Exemplos práticos – Email phishing?

Assunto: Alerta de Segurança: Atividade Incomum na Sua Conta

De: Banco XYZ noreply@bancoxyz.pt
Para: [Seu Endereço de Email]

Caro(a) [Nome do Cliente],

Detetámos uma tentativa de acesso incomum à sua conta bancária no dia **[data]**, às **[hora]**, a partir de um dispositivo ou localização que não reconhecemos.

Se foi o(a) senhor(a) que tentou aceder, não é necessária qualquer ação. No entanto, se não reconhece esta atividade, recomendamos que tome as seguintes medidas imediatamente:

1. **Aceda diretamente ao site do Banco XYZ digitando www.bancoxyz.pt no seu navegador.**
2. **Inicie sessão na sua conta e verifique se há movimentos não autorizados.**
3. **Se necessário, altere a sua palavra-passe e ative medidas adicionais de segurança, como a autenticação de dois fatores.**

⚠ **Nunca clique em links ou forneça dados pessoais por email.** O Banco XYZ nunca solicita informações sensíveis por email, SMS ou telefone.

Se precisar de assistência, entre em contacto connosco através do número oficial **[Número de Suporte]** ou dirija-se à agência mais próxima.

Atenciosamente,
Equipa de Segurança Bancária
Banco XYZ

Indicadores de legítimo

- Sentido **informativo**.
- Indicação de **data e hora da ocorrência**.
- Indicação para **não clicar** em links e que **não solicitam** informações sensíveis.
- Indicação dos **passos a seguir** caso não seja o autor da ocorrência.

Utilização da Internet

Transferir ficheiros ou software de fontes desconhecidas

- **Risco:** Instalação de malware.

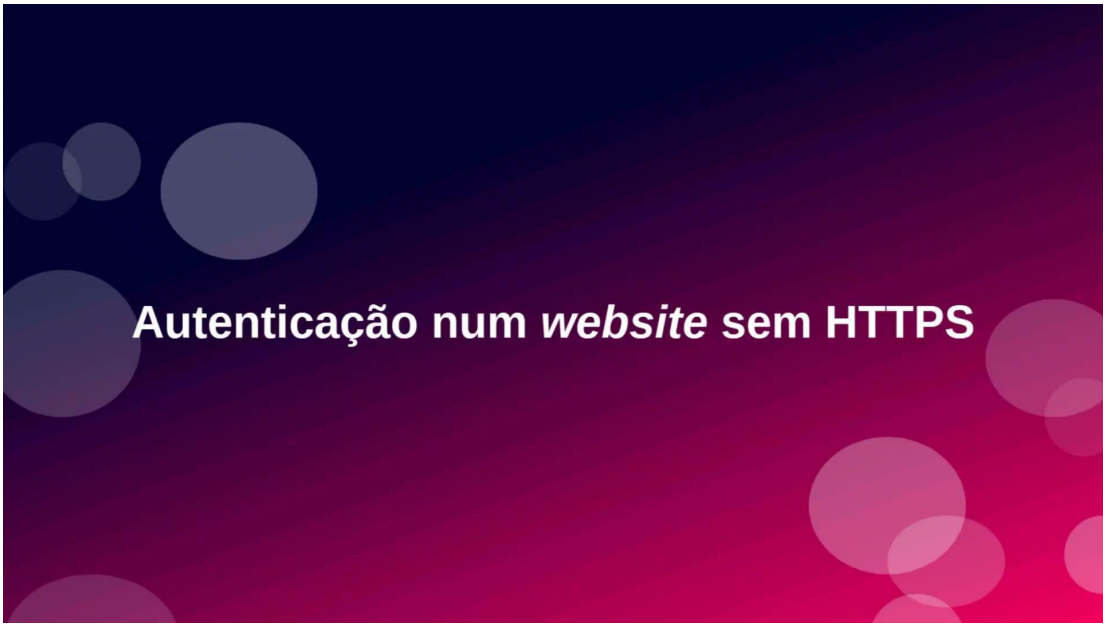
Não verificar a segurança do *websites*

- **Ricos:** Roubo de dados.

Medidas:

Só transferir ficheiros ou software de **fontes oficiais**.
Verificar se os ***websites* são seguros** (HTTPS) antes de inserir informações.

Exemplos práticos – Demonstração



Utilização de Redes Sociais

Não verificar definições de privacidade

- **Risco:** Facilita ataques de engenharia social.

Não considerar as consequências

- **Risco:** Impacto na reputação.

Medidas:

Ajustar definições de **privacidade**.
Evitar partilhar informações sensíveis.
Rever publicações antigas.

Boas práticas

Fonte: https://www.youtube.com/watch?v=9OdE0lvAOb4

Exemplos práticos – Notícias

Novembro de 2024

- **Ataque:** **Perfil falso** do Bispo Dom Virgílio Antunes (Diocese de Coimbra).
- **Objetivo:** **Pedir dinheiro** para uma suposta **campanha solidária**.
- **Riscos para vítimas**: Doações fraudulentas e engano de fiéis e seguidores.

Fonte: Renascença

Dezembro de 2024

- **Ataque:** **Perfil falso** do Patriarca de Lisboa, Rui Valério.
- **Objetivo:** **Pedir donativos**.
- **Riscos para vítimas**: Doações fraudulentas e engano de fiéis e seguidores.

Fonte: Observador

Exemplos práticos – Notícias

Janeiro de 2024

- **Empresa:** Arup (Empresa britânica de design e engenharia).
- **Ataque:** Deepfake.
- **Método:** Funcionário recebeu um **email falso** enviado em nome do diretor financeiro a **solicitar** uma **transferência confidencial**.
- **Motivo do Engano**: O funcionário suspeitou do email, mas participou numa **videoconferência** com supostos **colegas** e o **diretor finaceiro**. No entanto as **pessoas eram geradas por IA** e não eram reais.
- **Consequências:** Funcionário transferiu cerca de **25 milhões de dólares**.

Fonte: Jornal de Negócios

Dispositivos Móveis

Utilizar redes públicas

- **Risco:** Interceção de comunicações.

Utilizar dispositivos em locais públicos

- **Riscos:** Espionagem visual, roubo de dispositivos ou acessos não autorizados.

Medidas:

Utilizar VPN ao conectar-se a redes públicas.
Evitar que pessoas próximas **visualizem informações** no ecrã.
Bloquear o ecrã ao deixar o dispositivo sem vigilância.

Boas práticas – Espionagem visual

Fonte: https://www.youtube.com/watch?v=FLv0Hd9_xY0

Boas práticas – Redes públicas

Fonte: https://www.youtube.com/watch?v=lJxjBVNfVFE

Exemplos práticos – Notícias

Janeiro de 2025

- **Vítima:** Barbara Turner, 54 anos.
- **Ataque:** Roubo de dados bancários.
- **Método:** **Interceção de dados** ao realizar uma compra online numa **rede WiFi pública**.
- **Consequências:** **Conta bancária comprometida** e roubo de dinheiro da conta.

Fonte: Daily Mail

Maio de 2022

- **Vítima:** Jacopo de Simone.
- **Ataque:** Possível espionagem visual.
- **Método:** Vítima teve o **telemóvel roubado** mas como estava bloqueado não imaginou problemas.
- **Consequências:** **Roubo de dinheiro** da conta bancária através da aplicação.
- **Ivestigação:** O **código** da conta bancária foi **inserido corretamente**, indicando um possível ataque de espionagem visual.

Fonte: BBC

Tratamento de Informações

Utilizar dispositivos USB desconhecidos

- **Risco:** Instalação de *malware*.

Deixar documentos expostos e não os destruir ao descartá-los

- **Risco:** Exposição de informações confidenciais.

Medidas:

Não utilizar dispositivos USB desconhecidos.
Armazenar documentos sensíveis em locais seguros.
Destruir adequadamente documentos confidenciais.

Boas práticas – Dispositivos USB

Fonte: https://www.youtube.com/watch?v=81lBTOYubmw

Exemplos práticos – Notícias

Austrália (2016)

- **Ataque:** Dispositivos USB com malware, deixados nas caixas de correio dos residentes.
- **Objetivo:** Ao serem ligados ao computador ativavam ofertas fraudulentas e programas maliciosos.

Fonte: BBC

Portugal (2024)

- **Falha:** Segurança Social descarta documentos confidenciais sem serem destruídos e deixa-os na via pública sem vigilância durante o carregamento para uma carrinha.

Fonte: RTP

Comunicação de Incidentes

Não comunicar incidentes

- **Risco:** Propagação de ataques.

Desvalorizar práticas de segurança

- **Risco:** Aumenta a probabilidade de falhas de segurança.

Medidas:

Comunicar qualquer irregularidade.
Adotar medidas de segurança.

Boas práticas

Fonte: https://youtu.be/NugciPptTvg?si=d3UtTItYIcldASmg

Questões?

Obrigado!

Página intencionalmente deixada em branco.