Instituto Superior de Ciências Policiais e Segurança Interna

Pedro Miguel Nunes Barreiros Afonso
Aspirante a Oficial de Polícia

Dissertação de Mestrado em Segurança Pública

XXXVI Curso de Formação de Oficiais de Polícia

Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS

Orientador:

Professor Especialista Pedro Moita

Lisboa, 13 de maio de 2024

Instituto Superior de Ciências Policiais e Segurança Interna

Pedro Miguel Nunes Barreiros Afonso
Aspirante a Oficial de Polícia

Dissertação de Mestrado em Segurança Pública

XXXVI Curso de Formação de Oficiais de Polícia

Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Segurança Pública, elaborada sob a orientação do Professor Especialista Pedro Moita.

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXVI CFOP
Orientador:	Professor Especialista Pedro Moita
Título:	Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS
Autor:	Pedro Miguel Nunes Barreiros Afonso
Local de Edição:	Lisboa
Data de Edição:	13 de maio de 2024

Dedicatória

Ao meu Pai.

Agradecimentos

Começo por expressar a minha sincera gratidão a todos os que tornaram possível a realização da presente dissertação. Seria impossível concluir este trabalho sem o apoio, orientação e incentivo de todos vós.

Em primeiro lugar, agradeço o apoio de toda a minha família, especialmente, à minha mãe, irmã e avó. Pelos ensinamentos, pelo carinho e, sobretudo, pela educação que me foi passada por vós ao longo da minha vida. Sem o vosso contributo, nada do que sou hoje seria possível. Muito obrigado!

À minha namorada, por me aclarar o caminho e por todo o apoio que ao longo da dissertação se tornou indispensável. Sem ti não era possível!

Ao meu orientador, Professor Especialista Pedro Moita, pela sua orientação contínua ao longo desta jornada, fornecendo sempre os seus *feedbacks* e devidas correções, que, se constituíram muito valiosas para a concretização deste trabalho.

Aos meus camaradas e amigos de curso, que dispensam apresentações, evidentemente. Por todas as conversas, todas as aventuras e momentos. Acredito que fizeram de mim melhor pessoa. Contem comigo para tudo!

Aos meus amigos de sempre, que apesar da distância, os laços continuam os mesmos. Obrigado por tudo!

Ao XXXVI CFOP, por todos os momentos vividos com todos vós, ao longo destes 5 anos. Obrigado!

Terminando da mesma forma que comecei: agradeço a todos os que de alguma forma fizeram parte deste processo, por todo o apoio e compreensão!

Obrigado a todos!

Epígrafe

"*It's the job that's never started as takes longest to finish.*"

- Samwise Gamgee *in* "*LOTR*", J.R.R. Tolkien

Resumo

Manifestamente reconhecido, o ciberespaço é um domínio presente no quotidiano de qualquer pessoa, invariavelmente, no que diz respeito à sua vida pessoal ou profissional. No trabalho diário dos polícias, este domínio é, também, inevitável. A PSP tem vindo, nos últimos anos, a adaptar-se ao ritmo acelerado da evolução tecnológica e da mutação de formas de crime, sendo a criação de um núcleo dedicado a este fenómeno a prova disso. Contudo, a falta de formação especializada na prevenção dos seus próprios profissionais, é uma realidade alarmante que deve ser contornada.

O cerne do estudo centrou-se na análise dos comportamentos e atitudes que os polícias têm, em relação à cibersegurança. Recorreu-se a uma abordagem da metodologia de pesquisa quantitativa, através de questionário, por forma a recolher dados relativos aos comportamentos e atitudes de cibersegurança dos polícias do COMETLIS.

Os resultados revelaram que os inquiridos têm atitudes adequadas aquando da utilização do ciberespaço. Complementarmente, foi possível revelar que, o fator "faixa etária" tem influência nos respetivos comportamentos relativos à cibersegurança, enquanto o fator da classe policial não apresentou diferenças significativas. Por último, os polícias consideram útil a implementação de um *Quick Reference Guide* de cibersegurança na PSP. Constatou-se, deste modo, que os polícias do COMETLIS estão consciencializados da importância de se protegerem de ameaças no ciberespaço.

Este estudo contribui para uma compreensão do estado atual da cibersegurança e ciber-higiene dos polícias do COMETLIS, que, apesar de positivo, aponta, também, para a necessidade contínua de formação e sensibilização nesta matéria.

Palavras-chave: Atitudes e Comportamentos; Cibercrime; Ciberespaço; Cibersegurança; Consciencialização

Abstract

Clearly recognised, cyberspace is a domain that is present in everyone's daily life, invariably in terms of their personal or professional life. In the daily work of police officers, this domain is also unavoidable. In recent years, the PSP has been adapting to the rapid pace of technological evolution and changing forms of crime, and the creation of a centre dedicated to this phenomenon is proof of this. However, the lack of specialised training in prevention for its own professionals is an alarming reality that needs to be addressed.

The core of the study focused on analysing the behaviour and attitudes that police officers have towards cybersecurity. A quantitative research methodology approach was used, using a questionnaire to collect data on the cybersecurity behaviours and attitudes of COMETLIS police officers.

The results revealed that the respondents have appropriate attitudes when using cyberspace. In addition, it was possible to reveal that the "age group" factor has an influence on their cybersecurity behaviour, while the police rank factor did not show any significant differences. Finally, police officers consider it useful to implement a Quick Reference Guide on cybersecurity in the PSP. This shows that COMETLIS police officers are aware of the importance of protecting themselves from threats in cyberspace.

This study contributes to an understanding of the current state of cybersecurity and cyber-hygiene among COMETLIS police officers, which, although positive, also points to the ongoing need for training and awareness-raising in this area.

Keywords: Attitudes and Behaviours; Awareness; Cybercrime; Cybersecurity; Cyberspace

Lista de Siglas e Abreviaturas

ANSR	Autoridade Nacional de Segurança Rodoviária
APAV	Associação Portuguesa de Apoio à Vítima
CERT	Computer Emergency Response Team
CERT.PT	Computer Emergency Response Team Portugal
CESEDEN	Centro Superior de Estudios de la Defensa Nacional
CFA	Curso de Formação de Agentes
CFC	Curso de Formação de Chefes
CFOP	Curso de Formação de Oficiais
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
COMETLIS	Comando Metropolitano de Lisboa
CSIRT	Computer Security Incident Response Team
CSIRT.MAI	Computer Security Incident Response Team / Ministério da Administração Interna
DDoS	Distributed Denial-of-Service
DGPJ	Direção-Geral da Política de Justiça
DN/PSP	Direção Nacional da Polícia de Segurança Pública
ECTEG	European Cybercrime Training and Education Group
ENISA	European Union Agency for Cybersecurity
ENSC	Estratégia Nacional de Segurança no Ciberespaço
EUA	Estados Unidos da América
GNR	Guarda Nacional Republicana
IA	Inteligência Artificial
IC	Investigação Criminal
IDN	Instituto de Defesa Nacional
IGAI	Inspeção Geral da Administração Interna
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
MAI	Ministério da Administração Interna
N.º	Número
PGR	Procuradoria-Geral da República
PIIC	Plataforma para o Intercâmbio de Informação Criminal

PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
RNCSIRT	Rede Nacional / Computer Security Incident Response Team
RNSI	Rede Nacional de Segurança Interna
SCoT	Sistema de Contraordenações do Trânsito
SEI	Sistema Estratégico de Informação
SGMAI	Secretaria-Geral da Administração Interna
SIGAE	Sistema de Informação e Gestão de Armas e Explosivos
SIGESP	Sistema Integrado de Gestão de Segurança Privada
SMS	Short Message Service
SSI	Sistema de Segurança Interna
STIC	Sistemas e Tecnologias de Informação e Comunicação
TIC	Tecnologias de Informação e Comunicação
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
USB	Universal Serial Bus
VOIP	Voice over Internet Protocol

Índice Geral

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Índice de Equações

Introdução

Atualmente, é incontornável a ligação que é feita entre as tecnologias e a vida quotidiana em sociedade, fenómeno esse que se traduz numa dependência tecnológica, não só na vida pessoal de cada cidadão, mas também no ambiente profissional de muitos. O ciberespaço tornou-se parte integrante do tecido da sociedade moderna, uma sociedade que, apesar de mais avançada que nunca, se torna, também, numa sociedade de "risco", como caracteriza Ulrich Beck, na sua obra "Sociedade de Risco", 1992. Tal, deve-se ao facto de que é gerada uma noção de risco, fruto da preocupação com o próprio futuro da sociedade, uma vez que, a inovação da tecnologia, traz consigo, da mesma forma, a inovação de crimes.

As mutações da tecnologia hodierna servem de ferramenta, inevitavelmente, a novas formas de ilícitos criminais, consubstanciando-se num problema social de relevo (Rodrigues, 2009). Assim, o Estado, e, consequentemente, a Polícia, vão ao logo do tempo sentindo a evolução desta sociedade contemporânea e, obrigatoriamente, adaptando a sua forma e atividade no mesmo sentido.

É nesta senda que constatamos que, a Polícia de Segurança Pública, como qualquer organização policial contemporânea, tem como realidade a flexibilidade de adaptação da sua atividade a novas tecnologias e ferramentas de auxílio ao serviço que presta, em prol dos outros. Elias (2018), corrobora esta mesma ideologia, referindo que a Polícia se encontra, hoje, numa fase de mudanças significativas, em grande parte devido ao desenvolvimento das tecnologias e das novas abordagens de organização e gestão das instituições policiais.

As novas formas de crime, como é o caso do fenómeno da cibercriminalidade, não estão dependentes da "proximidade física entre a vítima e o agressor/criminoso", uma vez que no domínio do ciberespaço são irrelevantes os limites ou as fronteiras, tornando estes crimes, crimes transacionais, fazendo com que "para um criminoso na rede, seja tão fácil atacar um alvo em territórios longínquos, como vitimar um vizinho" (Elias, 2019).

Para Zwilling et al. (2022), tendo em consideração o contexto social em que se vive, hoje, cada vez mais, a população ocupa o seu tempo *online*, constatando-se, por consequência, num incremento do número e da complexidade dos ciberataques realizados, pelo que Richardson et al. (2020), concluem que se torna crucial o desenvolvimento de

todo o tipo de competências no ramo da cibersegurança, de modo a responder aos perigos no ciberespaço.

No *Relatório Cibersegurança em Portugal: Riscos & Conflitos* (CNCS, 2023a), são apresentadas estatísticas significativas, no que diz respeito à "perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança" (p. 12), onde é possível constatar o seu aumento em 2023, face ao ano anterior.

O objeto deste trabalho de investigação é a cibersegurança, a um nível preventivo, dando foco aos profissionais da Polícia de Segurança Pública, nomeadamente, ao efetivo policial do Comando Metropolitano de Lisboa. Uma vez que a Polícia não está isenta de ataques informáticos, tendo já sido alvo de diversos ciberataques e de tentativas de ataques às plataformas internas, bem como à rede interna, por variadas razões, afigurou-se pertinente e relevante estudar aquilo que são os comportamentos e as atitudes preventivos que os profissionais da PSP têm, ou não, nesta matéria. Na conceção de Elias (2018), um dos pilares da Segurança Interna é, precisamente, a prevenção criminal, consubstanciando-se num fenómeno crucial em todos os Estados de direito democrático.

Assim, no seguinte capítulo, será apresentada a formulação do problema de investigação, de modo a enquadrar tematicamente o problema em questão, bem como a justificação e relevância do tema, a problemática da presente investigação, onde consta a pergunta de partida da mesma, os objetivos propostos a alcançar, as hipóteses de investigação formuladas e, por último, a estrutura que segue a investigação.

Capítulo I – Formulação do Problema de Investigação

1.1. Justificação e Relevância do Tema

Tendo em conta uma revisão inicial da literatura, assim como a atualidade da matéria, e dado que não se conhecem estudos sobre o conhecimento do efetivo da PSP em assuntos de cibersegurança, nomeadamente da ciber-higiene dos próprios polícias, parece relevante e oportuno analisar o panorama atual destes profissionais, dada a especificidade e sensibilidade dos dados que, diariamente, operam.

Devido ao aumento do risco cibernético, as regras/normas de ciber-higiene são elevadas, especialmente para aqueles que têm acesso a informações vitais (O'Connell, 2012), como é o caso dos polícias.

De facto, é habitual afirmar-se que a ciber-higiene é um conjunto de medidas adequadas de segurança e proteção que evitam a maior parte das tentativas de incidentes e cibercrimes, no entanto, na maioria das instituições/organizações, a ciber-higiene não é implementada da forma mais correta. Mansfield-Devine (2016), refere que os ataques que as organizações sofrem, devem-se ao facto de que estas não fazem o uso correto das normas básicas de segurança na rede e nos dispositivos, não compreendendo, portanto, onde se encontram as suas fraquezas.

É assim, que Sabillón et al. (2019), concluem que, embora os utilizadores do ciberespaço adotem as mais variadas medidas de ciber-higiene, estes, vão ser sempre o fator mais vulnerável na cibersegurança. Tal acontece, porque as decisões securitárias mais relevantes recaem, frequentemente, no utilizador, daí que a sensibilização para a cibersegurança seja um ponto crucial para o bom funcionamento de uma organização.

A presente temática é pertinente, uma vez que permite: analisar o panorama atual da cibersegurança na PSP a um nível preventivo; analisar a sensibilização da Polícia para a cibersegurança e ciber-higiene; e, por último, um levantamento da exequibilidade da implementação de um *Quick Reference Guide* de Cibersegurança (um breve manual de auxílio).

No mesmo sentido, a pertinência desta investigação adensa-se por ligar-se a um dos eixos estratégicos da *Estratégia PSP 2024-2026*, da Direção Nacional da Polícia de Segurança Pública, nomeadamente o Eixo 3.5. Neste eixo, a PSP apresenta a sua vontade

em "investir na digitalização, automatização e desmaterialização das áreas de suporte à atividade operacional[1]", pelo que se torna necessário conhecer os riscos a que estão expostos os profissionais de Polícia aquando da utilização destas tecnologias, de modo a não periclitar os dados/informações institucionais e pessoais.

1.2. Problemática da Investigação

A seleção do assunto de investigação é de extrema importância, visto que é essencial que o tema escolhido desperte o interesse pessoal e que, ao mesmo tempo, esteja dentro de um campo científico, no domínio das Ciências Policiais. Ora, o presente estudo, insere-se numa das linhas temáticas de investigação constantes da agenda de investigação do ICPOL, nomeadamente, na linha temática "Polícia e Sociedade", no subtema "Tecnologias/Inteligência artificial", sendo parte integrante da "Utilização de tecnologia/IA na produção de segurança".

Deste modo, tendo em consideração o parágrafo anterior, após o aprofundamento da pesquisa e investigação, bem como a atualidade da temática, surgiu o interesse de trabalhar a área da cibersegurança e ciber-higiene.

Assim, urge, neste momento, estabelecer uma pergunta de partida, para que se atinja o pretendido com esta investigação. Ora, para Campenhoudt, Marquet e Quivy (2019), a pergunta de partida é o melhor instrumento para a eficácia de uma investigação, pois, a partir dela exprime-se o mais especificamente possível aquilo que se pretende estudar e conhecer.

Uma vez que Silva (2019), conclui que "A PSP terá que se adaptar a esta nova realidade […] enraizar a formação e a consciencialização do seu público interno […]" (p. 23), estabeleceu-se, no caso da presente investigação, a seguinte pergunta de partida:

No uso das tecnologias, o efetivo policial do COMETLIS, está devidamente consciencializado para se proteger e evitar ciberataques?

Dada a existência de múltiplos incidentes, envolvendo polícias, uma vez que, estes, recorrem a tecnologia informática no decorrer do seu serviço, sentiu-se a necessidade de dar resposta a esta pergunta de investigação. Assim, é de salientar a importância e

[1] Anexo I.

atualidade do assunto para a própria instituição, já que os dados e informações que, constantemente, são tratados por estes polícias, são de sensibilidade acrescida.

1.3. Objetivos da Investigação

Na concretização deste estudo, propomo-nos a alcançar diversos objetivos, sejam estes mais genéricos, sejam mais específicos, uma vez que, num trabalho de investigação, é de realçar a pertinência da definição de objetivos, de forma a não se perder a ideia principal da investigação (Quivy & Campenhoudt, 1998).

Assim, tendo em consideração o contexto e a problemática da investigação, o presente estudo tem como objetivo geral:

- no âmbito da cibersegurança e ciber-higiene, determinar o atual nível atitudinal e comportamental dos polícias do COMETLIS.

Em complemento, são também definidos os seguintes objetivos específicos:

- perceber se os polícias do COMETLIS têm noção da importância da cibersegurança, isto é, se cumprem as normas básicas de proteção, aquando da utilização das tecnologias inerentes à função que desempenham;
- entender se o efetivo policial do COMETLIS consideraria útil e viável um *Quick Reference Guide*, no campo da cibersegurança, implementado na PSP;
- compreender o eventual interesse da inclusão de formação especifica de cibersegurança nos cursos de formação da PSP (consciencializando-os das vulnerabilidades a que estão expostos no ciberespaço).

1.4. Hipóteses de Investigação

Como referem Quivy e Campenhoudt (1998), “um trabalho não pode ser considerado uma verdadeira investigação se não se estrutura em torno de uma ou de várias hipóteses” (p. 119). Efetivamente, segundo Sousa e Baptista (2011), as hipóteses de investigação equiparam-se a ideias de respostas prováveis à problemática do estudo em causa, que, conforme Marconi e Lakatos (2017), durante a investigação, são suscetíveis de serem testadas cientificamente, ou não.

Deste modo, as hipóteses transmitem à investigação um "fio condutor" que, eficazmente, fará com que o decorrer do trabalho consista "em testar as hipóteses, confrontando-as com dados da observação" (Quivy & Campenhoudt, 1998, p. 120), Isto, faz das hipóteses uma ferramenta rigorosa, dado o seu valor científico ao distanciar-se da vontade humana.

Uma vez que a presente investigação tem um cariz quantitativo, Fortin (2000), afirma que as hipóteses terão de ser baseadas em relações entre duas ou mais variáveis. Webster (2007), contribui, ainda, referindo que "uma hipótese é uma suposição ou inferência sobre o valor de um parâmetro desconhecido" (p. 192).

Assim, tendo em vista a consecução dos objetivos da presente investigação, e, com base na revisão da literatura acerca da temática da mesma, foram definidas quatro hipóteses de investigação, que se apresentam de seguida.

Hadlington (2018), considera que a conclusão fundamental da exploração das atitudes dos profissionais é, essencialmente, o sentido de responsabilidade acrescida que estes têm em relação a responsabilidades em matéria de cibersegurança numa determinada organização. Ora, tendo isto em apreço, denotou-se pertinente compreender o nível atitudinal dos polícias do COMETLIS, uma vez que, diariamente, operam com dados sensíveis, e que em momento algum podem ser corrompidos.

H1: As atitudes dos polícias do COMETLIS em relação à cibersegurança são corretas e adequadas no âmbito das suas funções.

Os fatores do género e idade podem vir a influenciar os comportamentos que cada um tem acerca da cibersegurança, pelo que se afigura necessário exponenciar a consciencialização da mesma, nos colaboradores e profissionais nas organizações, no que respeita aos comportamentos inseguros (Hadlington, 2018). Partindo desta mesma ideia, pretende-se, com as duas hipóteses seguintes, verificar se, em função da idade ou da carreira atual dos polícias do COMETLIS, existem diferenças significativas nos comportamentos de cada um.

H2a: Existem diferenças significativas de comportamentos de cibersegurança e ciber-higiene entre as faixas etárias dos polícias do COMETLIS.

H2b: Existem diferenças significativas de comportamentos de cibersegurança e ciber-higiene nas diferentes carreiras dos polícias do COMETLIS.

Manuais breves, como *Quick Refernce* Guides, relacionados com a cibersegurança e a ciber-higiene, são essenciais para a segurança das organizações (CNCS, 2022), pelo que se pretende com a última hipótese de investigação, entender a possível utilidade e viabilidade de implementação de um *Quick Reference Guide* na Polícia de Segurança Pública.

H3: Os polícias do COMETLIS consideram útil um *Quick Reference Guide* de cibersegurança implementado na PSP.

1.5. Estrutura da Investigação

Quanto à estrutura da presente dissertação, de maneira a dar resposta ao problema de investigação, a mesma foi dividida em três partes, correspondentes a três capítulos distintos.

A primeira parte diz respeito à formulação do problema, onde é elaborado um enquadramento temático e se justifica a escolha do tema, bem como a sua relevância para as Ciências Policiais. É, igualmente, efetuada uma pergunta de partida neste capítulo, tal como os objetivos do estudo, designadamente o objetivo geral e os específicos.

No segundo capítulo, é feito um enquadramento teórico-conceitual respeitante ao tema da cibersegurança e seus conceitos conexos, nomeadamente o ciberespaço e o cibercrime. É realizado, ainda, neste capítulo, uma abordagem à evolução do cibercrime num panorama nacional e internacional, apresentando dados estatísticos, em relação a essa matéria.

Posteriormente, no capítulo seguinte, é introduzido ao trabalho de investigação, a realidade atual da Polícia de Segurança Pública, em contexto de cibersegurança. São apresentadas as tecnologias de informação e comunicação utilizadas por parte desta polícia, e referem-se, ainda, as competências do Núcleo de Cibercriminalidade e os seus objetivos futuros. Por fim, neste capítulo, explana-se o fator humano da cibersegurança, para além das medidas de mitigação de incidentes de cibersegurança, como a ciber-higiene e a consciencialização para este assunto.

No quarto capítulo, verifica-se o método de investigação e todas as opções metodológicas realizadas, no âmbito da dissertação em causa. Nele, é elaborada a caracterização dos participantes, apresenta-se o instrumento de recolha de dados utilizado,

bem como os procedimentos adotados e, ainda, é explanado o instrumento de análise de dados.

No penúltimo capítulo da presente dissertação, posteriormente à recolha e análise dos dados obtidos, foram explicitadas, através da apresentação e discussão dos resultados, as conclusões e ilações dos testes realizados, por forma a responder com clareza às hipóteses de investigação previamente formuladas.

Por último, no sexto capítulo, é elaborada a conclusão do trabalho de investigação, onde é feito um compêndio de todo o estudo realizado e se conclui todos os pontos fundamentais que sustentam a dissertação, terminando com as limitações ao estudo e as recomendações futuras.

Capítulo II - Enquadramento teórico-conceitual: Cibersegurança e conceitos conexos

2.1. Ciberespaço

O termo "ciberespaço" surgiu em 1984, pelo escritor William Gibson, numa das suas mais conhecidas obras de ficção científica, o "*Neuromancer*" (Chawki, 2006). Ora, Gibson (1984), afirma que o ciberespaço é uma representação gráfica do conjunto de dados computacionais existentes. Contudo, embora o ficcionismo desta obra, de facto o ciberespaço foi-se desenvolvendo ao longo dos anos, e, atualmente, conquistou relevo no uso quotidiano das pessoas, de forma massiva.

De facto, existem inúmeras definições para este conceito, umas mais centradas naquilo que são as evoluções comunicacionais, outras mais focadas nas tecnologias interligadas entre si, nas redes. Nesta senda, apresentamos neste subcapítulo algumas dessas definições, segundo vários autores.

Aparício (2017), apresenta-nos este conceito no âmbito da evolução da comunicação, e, por conseguinte, a transmissão de informação, realçando que, o ciberespaço contemporâneo, representa uma progressão notável no modo como a comunicação ocorre e como a informação é transmitida. Atualmente, a documentação é preservada em ambientes virtuais, oferecendo amplas capacidades de armazenamento e facilitando, essencialmente, o acesso a esses recursos, o que leva, Aparício (2017), a concluir que esta transformação reflete uma mudança significativa na maneira como lidamos e interagimos com a informação.

Fernandes (2012), realça que o ciberespaço é, nos dias de hoje, um domínio, fundamentalmente associado à Internet, contudo, define-o como uma "rede global de infraestruturas de tecnologias de informação interligados entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores" (p. 12).

Numa vertente mais física, Freire e Caldas (2013), aludem este conceito, tendo em conta as componentes tecnológicas de *hardware*[2], explicando, portanto, o ciberespaço como um conjunto de "computadores interconectados, servidores, *routers*, *switches* e

[2] Diz respeito a toda a componente física de um computador ou dispositivo (*e.g.*, processador, teclado, rato e placa gráfica) (Filho, 2008).

cabos," e conclui que "é este emaranhado tecnológico que serve de suporte, tecnologicamente, às infraestruturas críticas" (p. 90).

Por outro lado, Libicki (2009), acrescenta à definição dois níveis, para além do nível físico, isto é, propõe uma visão do ciberespaço fundamentada num modelo de três níveis: físico, sintático e semântico. Sendo que, o primeiro nível se refere ao nível físico, ou seja, ao *hardware* das Tecnologias de Informação e Comunicação (TIC), visto como a base do ciberespaço (Freire & Caldas, 2013). O nível sintático aborda o *software*[3]e tudo aquilo que que sustenta o funcionamento dos sistemas de redes e computadores. Já o nível semântico, trata das informações partilhadas, armazenadas e processadas pelos utilizadores do ciberespaço, nos sistemas de redes e computadores. É assim que, com esta estrutura tríade, Libicki (2009), oferece uma compreensão abrangente da complexidade do ambiente digital.

Este conceito pode, também, ser interpretado como um domínio que abriga estruturas formadas por redes dinâmicas de interações, de organização e de gestão, entre sistemas. Estas estruturas utilizam a conectividade do espaço para conduzir as suas atividades (McLuhan, 1962), destacando a importância do ciberespaço como um ambiente onde os sistemas interagem e organizam-se para operar as suas funções.

Ademais, o ciberespaço pode ser descrito como um ambiente dinâmico, evoluindo de dia para dia, onde as reformas e mudanças são frequentes e, por vezes, inesperadas. Assim, é um domínio disponível e acessível para a grande maioria da população mundial. Além disso, uma das suas características distintivas é o anonimato, tornando cada vez mais complexa a determinação da identidade dos utilizadores deste espaço (Domingues, 2015). Combinando estas características, define-se um espaço em que a fluidez, a acessibilidade e a relativa dissociação da identidade, são traços proeminentes.

Numa outra conceção, McLuhan (2000), afirma que um meio de comunicação antigo se adapta, assim que um meio de comunicação recente surge, de maneira a coexistir com o novo. Ora, a Internet é, hoje, responsável por provocar mudanças na forma como a informação é transacionada, de e para outros meios de comunicação. Por outro lado, Castells (2004), acrescenta que a função de integrar numa comunidade o acesso à informação e comunicação através da Internet, cabe a essa mesma comunidade, tornando-

[3] Diz respeito aos meios não físicos da tecnologia, que se destinam ao tratamento automático da informação (Rezende, 2006).

se, assim, um elemento constitutivo da própria sociedade e indispensável para os processos formativos, informativos e comunicacionais, que permite o desenvolvimento individual e coletivo.

O Ciberespaço é um domínio onde a vida real transcende para o virtual, contendo características muito próprias, resultando, também, em novas maneiras de comunicação e relacionamento (Elias, 2019), com o auxílio, evidentemente, da Internet.

A disseminação das tecnologias de informação e comunicação, tem levado a um cenário em que, atualmente, um número extremamente significativo de pessoas (cerca de 5.16 mil milhões) possui acesso à Internet, representando, aproximadamente, 64.4% da população global, segundo dados do "*DataReportal*", em 2023. Segundo as estimativas do *website* "*Internet World Stats*" (2023), a Ásia é o continente com maior utilização da Internet (cerca 54% de toda a Internet mundial), seguida da Europa (com, aproximadamente, 14%). Contudo, a América do Norte é a região do globo onde a taxa de penetração da Internet é maior, com cerca de 93% da sua população, encontrando-se, a Europa, novamente em segundo lugar, com 89% de penetração de Internet.

Este amplo acesso à Internet desempenhou um papel crucial no aumento das ameaças e desafios, relacionados à cibersegurança. Consequentemente, temos observado uma constante evolução e aprimoramento das estratégias utilizadas para realizar ataques online, ciberataques. É desta forma que, Poiares (2019a), afirma que:

> Na verdade, a segurança cibernética passou a constituir um dos principais desafios para os Estados, desde logo porque a criminalidade informática tem vindo a aumentar, sendo possível extrapolar que, dentro de cerca de uma década, possa atingir mais de 10% da totalidade dos crimes cometidos em Portugal (Poiares, 2019a).

Nesta senda, Silva (2019), conclui que a navegação pelo ciberespaço pressupõe e obriga a normas que, de forma sustentada, reduzem o risco social e, consequentemente, protegem as instituições, invariavelmente de cariz público ou privado, requerendo, assim, o desenvolvimento de uma estratégia mobilizadora e integradora num plano nacional.

2.2. Cibersegurança

O Instituto da Defesa Nacional, na cooperação IDN-CESEDEN (com o *Centro Superior de Estudios de Defensa Nacional*, em Espanha), afirma que o ciberespaço já foi aceite e considerado como o "quinto domínio operacional", dado o seu crescimento, espaço onde os sujeitos encarregues da sua segurança levam a cabo ações especializadas de segurança e defesa, tendo em conta as características deste determinado domínio/espaço.

Assim, considerando tudo aquilo que foi mencionado anteriormente, relativamente ao ciberespaço, cabe-nos, então, conceitualizar aquilo que é a segurança desse "quinto domínio operacional", uma vez que, (Poiares, 2019b), conclui que o "ciberespaço apresenta oportunidades mas encerra em si mesmo ameaças e riscos" (p. 118). Nesta senda, é necessário enquadrar e integrar um conceito securitário que dê, ou tente dar, resposta às ameaças e aos ataques naquilo que é o ciberespaço. Surgindo, portanto, o conceito de cibersegurança, que, se fragmentando, se obtém: ciber, vinculado ao conceito de ciberespaço, e segurança (Craigen et al., 2014).

Na *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*, é definido o conceito de segurança no ciberespaço, isto é, a cibersegurança. Ora, este termo é conceitualizado como o conjunto de procedimentos e atividades de prevenção, deteção e reação, que veem o seu fim na manutenção do estado de segurança pretendido, garantindo a integridade e confidencialidade das informações, seja das pessoas que "circulam" pelo ciberespaço, seja do próprio domínio em si (Resolução do Conselho de Ministros, 2019).

Concomitantemente, a Cibersegurança é, para Militão (2014), o conjunto de medidas e diligências que procuram garantir o bem-estar e o normal funcionamento de um Estado e dos seus habitantes, tanto no ciberespaço como fora dele, sempre que diretamente lhe estejam associadas ações acometidas. Pelo que, Silva (2019), entende que a Cibersegurança deve ser vista como prioridade a nível nacional, naquilo que é o combate às ciberameaças e a resposta aos ciberataques.

No estudo de Cavelty (2010), é possível sustentar que, tanto a cibersegurança, como a segurança nacional, enfrentam desafios semelhantes, abrangendo desde ameaças de grupos terroristas, até Estados opositores. Contudo, as distinções entre ambas são significativas quando se trata dos agentes envolvidos e do objetivo central de proteção. A diferença fundamental reside na implementação de recursos, pois a segurança nacional

abarca um espectro diversificado de recursos, sejam estes humanos ou financeiros. Além disso, os agentes envolvidos em cada área também divergem, uns sendo especialistas em informática e os outros sendo profissionais em segurança (ou falta dela). É desta maneira que se correlacionam as duas seguranças, pois, hodiernamente, a segurança nacional ampliou a sua preocupação para a construção de resiliência nas infraestruturas nacionais, implementando medidas de cibersegurança. Simultaneamente, a cibersegurança emergiu como um fator prioritário em matérias de segurança nacional (Cavelty, 2010).

De forma breve, Vieira (2016), define este conceito como o garante de vigilância do domínio digital, que tenha a capacidade de dar uma resposta preventiva e reativa, eficientemente, aos incidentes criminosos nesse mesmo domínio. Ao passo que Fischer (2010), contribui para a definição de cibersegurança, incrementando novas noções, ao nível da proteção. Assim, afirma que existem três aspetos a ter em consideração, sendo estes: as normas de proteção do meio digital; o grau de proteção, originado pela efetivação dessas normas e, por último, o peso do empenho humano.

Adicionalmente, destaca-se, também, a visão de Silva (2012), de que a cibersegurança avança sempre de mãos dadas com a supervisão da informação, dado que a informação representa o ativo mais valioso de qualquer organização, é crucial abordar esse fenómeno com a devida seriedade.

Portanto, no seguimento do parágrafo anterior, afigura-se crucial distinguir, desde logo, este conceito dos demais conceitos de segurança que a ele estão interligados, como é o caso do conceito de segurança da informação. Assim, como referem Whitman e Herbert (2017), a "segurança da informação visa proteger a confidencialidade, a integridade e a disponibilidade dos ativos de informação, quer em armazenamento, processamento ou transmissão." (p. 8). A efetivação desta segurança depende, a todo o momento, de vários fatores da organização, como a aplicação de políticas, a formação e sensibilização, a educação e a própria tecnologia existente.

Por último, Moita (2024), apresenta várias subdivisões da cibersegurança, para além da segurança da informação, tais como: a segurança de rede, que visa proteger uma determinada rede de computadores de possíveis intrusos (*bots*[4], pessoas); a segurança de aplicativos, que mantém o *software* e os dispositivos robustos contra ameaças; a segurança

[4] *Bots* são um tipo de software criado para simular ações humanas, de forma repetitiva e padronizada (Adamopoulou & Moussiades, 2020).

operacional, que executa a gestão das permissões de acesso dos utilizadores de uma determinada rede; a recuperação de desastres, que se consubstancia na maneira de como uma organização é capaz de responder a um incidente que cause perda de dados, retomando o normal funcionamento da mesma; e a educação do próprio utilizador, sendo este o fator mais imprevisível da cibersegurança.

2.2.1. Centro Nacional de Cibersegurança

A estratégia definida, em matérias de cibersegurança, no panorama nacional, enquadra-se, essencialmente, na coordenação das entidades competentes com o Centro Nacional de Cibersegurança (Poiares, 2019a).

É, deste modo, que introduzimos ao enquadramento do tema, aquilo que é a Autoridade Nacional de Cibersegurança, o Centro Nacional de Cibersegurança, doravante designado por CNCS.

O CNCS, com a designação que conhecemos hoje, surge através do Decreto-Lei n.º 136/2017, de 6 de novembro. Contudo, é um ano mais tarde, através da publicação da Lei n.º 46/2018, de 13 de agosto – diploma que estabelece o Regime Jurídico da Segurança do Ciberespaço – que lhe é atribuída, de facto, a competência de Autoridade Nacional de Cibersegurança.

Ora, o conceito de cibersegurança é alvo das mais variadas definições e interpretações, como temos vindo a constatar. Pelo que, para o CNCS, este termo é definido na mesma visão que a da *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*, incrementando, apenas, a ótica do "sentimento de segurança percecionado pelas pessoas quando usam a Internet e as tecnologias digitais."[5]

Assim, a sua missão/objetivo, de acordo com o CNCS (2021), passa, precisamente, por:

> […] contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional.
>
> Atuando como coordenador operacional e autoridade nacional em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços

[5] Retirado do *website* do Centro Nacional de Cibersegurança (https://www.cncs.gov.pt/pt/sobre-nos/)

digitais, o CNCS transporta também a sua ação para a sociedade em geral (CNCS, 2021).

É, de igual modo, relevante, referir o serviço que controla e coordena as respostas a incidentes no ciberespaço em Portugal, o CERT.PT. Ora, o CERT.PT tem como primordial objetivo e missão contribuir para o esforço de cibersegurança nacional, nomeadamente no tratamento e coordenação da resposta a incidentes (acontecimento que conta com um efeito adverso naquilo que é a segurança das redes e sistemas de informação e nos respetivos dados e informações neles armazenados), na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança a nível nacional. Em Portugal, o CERT.PT, tem vindo a promover a criação de novas CSIRT (serviços de resposta a incidentes de segurança informática), mediante os protocolos de cooperação com as operadoras de telecomunicações e outras entidades igualmente relevantes, com o objetivo da criação de uma rede nacional e cooperação nas áreas da segurança informática.

2.2.2. Estratégia Nacional de Segurança do Ciberespaço

A Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, aprovou a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, doravante designada por ENSC, revogando a Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, que aprovava a ENSC desde 2015.

Com efeito, a ENSC, coordenada pelo susodito Centro Nacional de Cibersegurança e com o apoio da iniciativa "INCoDe.2030" (programa do Governo que visa a promoção e capacitação das competências digitais de toda a sociedade portuguesa em toda a sua diversidade), tem como objetivos estratégicos três importantes pontos: maximizar a resiliência; promover a inovação; e gerar e garantir recursos. Assim, tendo em conta estes três objetivos estratégicos, desenvolveram-se seis eixos de intervenção, de modo a apresentar as ações que se pretendem executar na ENSC, no âmbito do seu Plano de Ação, sendo eles: Eixo 1 – Estrutura de segurança do ciberespaço; Eixo 2 – Prevenção, educação e sensibilização; Eixo 3 – Proteção do ciberespaço e das infraestruturas; Eixo 4 – Resposta às ameaças e combate ao cibercrime; Eixo 5 – Investigação, desenvolvimento e inovação; Eixo 6 – Cooperação nacional e internacional.

No âmbito do presente trabalho de investigação, destes seis eixos de intervenção, destacamos o Eixo 2 – Prevenção, educação e sensibilização - que indica a importância de

se conhecer os indicadores que estão associados às potenciais ameaças no ciberespaço, traduzindo-se, fundamentalmente, numa medida preventiva. Isto, porque é mencionado na ENSC, que "o conhecimento homogéneo e criterioso de indicadores de ameaça permitirá assim a todo o ecossistema nacional da segurança do ciberespaço o conhecimento prévio adequado à produção de medidas de antecipação da ameaça e de segurança contra impactos não desejados."

Segundo a própria Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, a ENSC tem, como visão, um Portugal mais seguro, mediante ações inovadoras que deem resposta à célere evolução digital da sociedade hodierna, preservando, desta forma, os valores do Estado de Direito Democrático, garantindo o normal e regular funcionamento das instituições portuguesas.

2.3. Cibercrime

Uma das primeiras definições de crime informático foi delineada em 1989, pelo Departamento de Justiça dos Estados Unidos da América, ao definir que qualquer transgressão das leis que recorresse ao conhecimento em tecnologias de computação e redes para sua realização, poderia ser considerada como crime informático (Keyser, 2009). As origens iniciais do cibercrime, surgiram com comunidades de programadores envolvidos em práticas de *hacking*[6], evoluindo, ao longo do tempo, até à variedade de cibercrimes contemporâneos (Williams, 2010).

Atualmente, há uma indicação clara de que as atividades criminosas alcançaram uma dimensão global e informacional, no qual esta dimensão permitiu esta tipologia criminal, oferecendo meios para fomentar a intensificação do pensamento acelerado e a procura por desejos ilícitos (Castells, 2007). Um fator facilitador desse fenómeno é, de facto, a Internet e as redes sociais, que representam um novo cenário para a atividade da criminalidade organizada, muito por conta do fácil acesso à informação, seja ela relativa à radicalização, ao recrutamento e aliciamento político, abarcando, então, um amplo conjunto de causas e orientações ideológicas (Elias, 2019).

[6] O *hacking* refere-se às atividades levadas a cabo por indivíduos dotados de vasto conhecimento informático, que têm como objetivo principal comprometer dispositivos digitais, como computadores e *smartphones*, ou até mesmo, a intrusão em redes inteiras (Jordan, 2017).

Na conceção de Silva (2012), e para melhor clarificar os diferentes vocábulos existentes que caracterizam o cibercrime, também nós, decidimos considerar que:

> […] o termo "criminalidade informática" corresponde à Cibercriminalidade e consequentemente o "crime informático" corresponde ao Cibercrime. Do mesmo modo consideramos que os termos: "crime relacionado com computadores", "crime relacionado com informática", "crime de alta tecnologia", "crime tecnológico", "crime de computação", "crimes informáticos", "crimes virtuais", "crimes digitais", "crimes informático-digitais" se referem a Cibercrime […] (Silva, 2012, p. 22-23).

É, do mesmo modo, que, a APAV (2024), considera e distingue crimes ciberdependentes de crimes possibilitados pela Internet e pelas TIC. Os crimes ciberdependentes dizem respeito às maneiras atuais de criminalidade, onde fica evidente que houve dependência do uso ou da existência de computadores, dispositivos eletrónicos, ou de qualquer uma outra TIC. Ao passo que os crimes possibilitados pela Internet e pelas TIC, traduzem-se naqueles crimes perpetuados pelas formas tradicionais, mas que, ao mesmo tempo, de alguma maneira, as TIC incorporam um papel na sua concretização, podendo ser crimes de motivação financeira como as burlas informáticas, ou até mesmo crimes sexuais, como o *revenge porn*[7].

Nesta senda, Clough (2011), expressa que estes termos realçam o papel preponderante da tecnologia naquilo que é o crime. Uma vez que a dinâmica específica da cibercriminalidade evolui conforme a tecnologia avança, o autor, apresenta três tipos de ilícitos nesta matéria.

Primeiramente, engloba os crimes em que o principal alvo do ilícito é o dispositivo ou a rede informática (*e.g.*, propagação de *malware*[8], toda a pirataria informática e ataques DDoS [9]). De seguida, apresenta os ilícitos onde os dipositivos são o meio para consumar, realmente, o crime (*e.g.*, fraudes, violações de direitos de autor, pornografia infantil,

[7] *Revenge porn*, ou pornografia de vingança, em português, segundo a APAV (2019), é a partilha de fotografias ou vídeos de conteúdo íntimo de alguém, sem o seu consentimento, visando prejudicar a pessoa em questão.

[8] *Malware*, é um tipo de *software* malicioso, isto é, qualquer programa ou código malicioso que faça perigar os sistemas informáticos (Aslan & Samet, 2020).

[9] DDoS - *Distributed Denial-of-Service*, é um ataque de negação de serviço, ou seja, é uma tentativa maliciosa de afetar o tráfego normal de um servidor, serviço ou rede. Estes ataques, sobrecarregam o alvo ou a sua infraestrutura circundante, como a rede a que ele está conectado, com um enorme fluxo de tráfego de Internet, que acabam, muitas das vezes, por interromper o serviço ou alvo que visam (Kumari & Jain, 2023).

ciberbullying). Por último, destaca os crimes em que o uso dos dispositivos como o computador é, meramente, secundário, mas que pode servir como prova criminal (*e.g*., SMS, emails, fotografias e vídeos que comprometam o suspeito do crime).

Na ótica de Elias (2018), o cibercrime abarca os crimes cometidos recorrendo a tecnologias ou meios digitais. Ao mesmo tempo que Bell et al. (2004), argumentam que o cibercrime é traduzido nos atos que incorporam o uso ilegal da tecnologia informática e da Internet. Ao passo que Brown (2015), acrescenta que este conceito pode, ainda, ser dividido em duas partes: o uso da tecnologia informática e o uso da Internet para levar a cabo uma conduta criminosa.

De acordo com Alexandrou (2021), são várias as razões e motivações para o cibercrime, desde motivações financeiras (fraudes, descodificação e leituras óticas de cartões bancários, roubos de identidade, através de diversas ferramentas como o *phishing*[10] e o *ransomware*[11]), espionagem, nomeadamente, a ciberespionagem (acesso a dados de entidades e serviços críticos), motivação ideológica (*hacktivismo*[12]), ou até mesmo motivações geradas através de questões de emoção pessoal, como a vingança, a procura pela fama, reconhecimento, intimidação, entre muitas outras.

O mesmo autor afirma que os alvos do cibercrime podem ser organizados em três categorias, sendo elas: o cibercrime cometido contra o governo; o cibercrime cometido contra indivíduos; o cibercrime cometido contra instituições e/ou organizações.

Por outro lado, Elias (2019), afirma que a principal motivação para o cibercrime é, de facto, o lucro conseguido através das práticas ilícitas perpetuadas no ciberespaço, uma vez que, segundo o mesmo:

> As organizações de cibercriminalidade recrutam jovens universitários, engenheiros informáticos e outros peritos em sistemas de informação, procuram como alvo as instituições financeiras, estabelecem alianças com organizações criminosas de tráfico de droga, tráfico de armas, tráfico de seres humanos, ou

[10] O *phishing* ocorre quando alguém, para conseguir obter informação pessoal de outrem, utiliza formas dissimuladas e enganadoras, como mensagens no correio eletrónico, com a finalidade de levar a pessoa a partilhar os seus dados, muitas das vezes, clicando apenas num *link*. (Dhamija et al., 2006).

[11] O *ransomware* é um *malware*, que ameaça uma vítima, podendo esta ser um indivíduo ou uma organização, ao destruir ou interditar o acesso às informações ou aos sistemas críticos, até que um resgate seja pago, tendo, portanto, na maior parte das vezes, uma motivação financeira (O'Kane et al., 2018).

[12] O *hacktivismo*, segundo Arruda (2021), é "uma forma de ação, individual ou coletiva, dependente da utilização de capacidades de *hacking*, que têm o propósito político-ideológico de enfraquecer, limitar ou destruir o poder coercivo de instituições ou Estados" (p. 35).

> transformam-se em organizações que exploram a criminalidade sexual, a pedofilia, as burlas e os tráficos de diversa ordem, visando sobretudo o lucro (Elias, 2019).

Contudo, para além da motivação económica, consumada através de cibercrimes como o *phishing* (uma ferramenta com formato simples e fácil de perpetuação do cibercrime, dado que aquilo que é explorado são as vulnerabilidades do utilizador, e não as vulnerabilidades técnicas da rede ou computadores) e "ciberburlas" – uma preocupação crescente no panorama nacional - de acordo com Poiares (2019b), surge também, mais uma vez, o fenómeno do *hacktivismo* (movimento *anonymous*, entre outros análogos) como motivador de ilícitos neste domínio.

Em suma, podemos argumentar que não existe uma definição precisa e universalmente aceite de cibercrime, mas antes diversas abordagens e terminologias associadas a atividades criminosas no ciberespaço (Maia, 2019).

2.3.1. Cibercrime – Legislação Portuguesa

No âmbito legislativo, a nível nacional, a tipificação criminal, nestes assuntos, é contemplada em inúmeros diplomas legais. Ora, no Código Penal Português, concretamente no seu artigo n.º 193.º, com a tipificação "Devassa através de meio de comunicação social, da Internet ou de outros meios de difusão pública generalizada", e, também, no seu artigo n.º 221.º, com a tipificação "Burla informática e nas comunicações".

A Lei da Organização e Investigação Criminal (Lei n.º 49/2008, de 27 de agosto), é mais um diploma de se realçar, diploma este que estipula a competência reservada da PJ a investigação dos crimes informáticos e praticados com o recurso a tecnologia informática.

Maia (2019), refere, entre muitos outros diplomas legais, a Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de outubro que:

> […] transpôs para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Maia, 2019, p. 9-10).

Por último, a Lei n.º 109/2009, de 15 de setembro, é um dos diplomas legais com maior importância, em matéria de cibercriminalidade, visto que o cibercrime em Portugal se encontra regulamentado pela Assembleia da República, nos termos desta mesma Lei[13].

2.4. Evolução da Cibercriminalidade em Portugal

O fenómeno da cibercriminalidade já não é novidade, e, o seu crescimento é, cada vez mais, uma realidade, pelo que urge a necessidade de, progressivamente, se consciencializar dos perigos a que nos expomos diariamente no uso do ciberespaço. Nesta senda, no presente subcapítulo será feita uma súmula daquilo que tem sido a evolução deste fenómeno em Portugal, nos últimos anos, mais concretamente no ano de 2022.

Primeiramente, segundo o *Relatório Riscos e Conflitos 2020* (CNCS, 2020), na década passada, concretamente, entre os anos de 2009 e 2020, os crimes informáticos e crimes relacionados com a informática, bem como a burla informática, assistiram a um incremento considerável de ocorrências.

Segundo o *Relatório Cibersegurança em Portugal: Riscos & Conflitos*, produzido pelo CNCS (2023a), no decorrer de 2022, no ciberespaço nacional, os cibercriminosos foram os atores com maior destaque, atuando com a principal intenção de lucrar economicamente, através de diversos crimes cibernéticos, como o *smishing*[14], o *phishing*, o *vishing* [15]e o *ransomware*[16].

Neste mesmo ano, assinala-se, ainda, o aumento do resultado e aperfeiçoamento de determinados acidentes, sendo o *ransomware* um dos que mais se destaca, redundando na divulgação de dados que, de 2021 para 2022, aumentou quase para o dobro em número de

[13] "A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa." (Artigo 1.º - Lei n.º 109/2009, de 15 de setembro).

[14] É um tipo de *phishing* e consiste em um sistema de engenharia social, com a finalidade de cometer fraudes através das mensagens de texto (SMS) Os criminosos fazem-se passar por entidades oficiais, organizações e empresas, enviando um *link* com *malware*, ou então pedindo informações pessoais da vítima (Yeboah-Boateng & Amanor, 2014).

[15] *Vishing* é uma técnica de VoIP (*Voice over Internet Protocol*), que faz uso de telefonemas para aceder a informações pessoais das vítimas. Os criminosos fazem-se passar por entidades legítimas e utilizam atendedores automáticos para que as vítimas forneçam dados pessoais para, supostos, efeitos de segurança (Yeboah-Boateng & Amanor, 2014).

[16] Conforme o "Quadro de Ameaças: Ciberameaças/agentes de ameaça críticos em Portugal, 2022/2023" do *Relatório Cibersegurança em Portugal: Riscos & Conflitos* (CNCS, 2023a).

acidentes (CNCS, 2023a). Este tipo de ataques encontra-se previsto, assim como a sua punição, na Lei 109/09, de 15 de setembro, a Lei do Cibercrime (crimes informáticos), e, verificou-se um significativo incremento destes registos pelas autoridades policiais.

Portanto, segundo o citado relatório, é-nos possível destacar alguns incidentes relacionados com o cibercrime, em Portugal, nos últimos tempos. Assim, de forma primária, destacamos o número de incidentes registados pelo CERT.PT, onde existiu um aumento de 14%, de 1781 para 2023 incidentes, nos anos de 2021 para 2022, respetivamente. Destes números, cerca de um terço ocorreram em entidades públicas. Relativamente aos tipos de incidentes mais registados pelo CERT.PT, no ano de 2022, o *phishing/smishing* surge em primeiro, com 37% do total, menos 3% que no ano anterior, de acordo com o CNCS (2023a).

Do mesmo modo, a Rede Nacional CSIRT (serviços de resposta a incidentes de segurança informática), registou a tentativa de *login* e o sistema infetado, isto é, o *malware*, 14% e 13% do total, respetivamente, como os tipos de incidentes mais detetados.

Adicionalmente, em relação às violações de dados pessoais, o mesmo relatório destaca que a Comissão Nacional de Proteção de Dados (CNPD), registou um incremento de 15%, relativamente ao ano anterior, sendo que 20% das entidades que informaram a CNPD das violações de dados pessoais, foram entidades públicas. Efetivamente, os casos de violação de dados pessoais aumentaram significativamente de 2021 para 2022, sendo que, o princípio da informação mais "violado" foi, de facto, a confidencialidade, com 58% do total. Complementando, as origens dos incidentes de violações de dados pessoais registados pela CNPD foram várias, sendo o *ransomware* (30% do total) aquela que mais se destaca, à frente da falha humana e das falhas aplicacionais (CNCS, 2023a).

Tendo em conta os crimes informáticos, tipificados na Lei do Cibercrime, as autoridades policiais obtiveram um aumento de 48% de registos em 2022, sendo, o acesso/interceção ilegítimos, aquele que mais obteve registos, ao passo que, estes números, tendem a aumentar de ano para ano, conforme o que se tem previsto, segundo os dados da Direção-Geral da Política de Justiça (DGPJ). Deste modo, a DGPJ, apresenta a burla informática como o crime relacionado com a informática (não registada entre os crimes informáticos) o mais comum, e, ao mesmo tempo, houve um incremento de 14% na totalidade dos crimes registados pelas autoridades policiais, quer estes sejam informáticos, quer sejam relacionados com a informática (CNCS, 2023a).

Ademais, segundo o CNCS (2023a), a UNC3T (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica) da Polícia Judiciária "abriu mais 6,7% de inquéritos em 2022 do que em 2021" (p. 19). Como tal, o Gabinete de Cibercrime da Procuradoria-Geral da República "registou 2125 denúncias, mais 83% do que no ano anterior", sendo que o "*phishing* e diversos tipos de burlas *online* são os tipos de criminalidade mais denunciados ao Gabinete Cibercrime da PGR em 2022" (p. 19).

De modo a findar aquilo que são os destaques do anual relatório de cibersegurança do CNCS (2023a), enfatizamos as principais tendências e desafios para o presente e futuro próximo no ciberespaço de interesse nacional. Desta forma, como tendências presentes e futuras, é de realçar: o aumento abrupto da ameaça, resultante da profissionalização do cibercrime; a "relevância de ameaças como o *ransomware* e outros tipos de extorsões, DDoS, *malware* de furto de credenciais, *simishing/vishing/spoofing*" (p.21); numerosos tipos de intrusões, entre muitos outros. Por último, como desafios estratégicos, destacamos "a cibersegurança nas tecnologias IoT" e "a falta de literacia digital e de recursos humanos especializados em cibersegurança" (p.21).

No panorama mundial, de forma breve, o cibercrime tem assistido, também, a aumentos significativos dos seus números. Segundo o Check Point Research (2023), de 2021 para 2022 a média de ataques informáticos semanais a organizações aumentou 38%, sendo que organizações estatais e a educação, foram aquelas que mais sofreram com estes ataques. Destes fenómenos criminais, é possível apresentar, conforme o Check Point Research (2023), as origens e os alvos mais frequentes, sendo que, os EUA, lideram as tabelas, seguidas da Áustria e da Dinamarca, como origem dos ataques, e o Reino Unido e a Índia como principais alvos. Por último, a intrusão em redes e computadores e o *malware*, foram os ataques que mais se verificarem nesse ano de 2022.

Frisa-se, ainda, que todos estes dados são contabilizados a partir das denúncias efetuadas às autoridades competentes, portanto, todos os incidentes que não são apresentados a estas, não são registados, denominando-se, então, por cifras negras.

De facto, existem inúmeros fatores para este fenómeno ser tão recorrente, como cibercrimes não reportados, indetetáveis, não investigados e não concluídos, de acordo com Koops (2010), devendo-se ao facto de serem crimes "invisíveis" e de complexa investigação.

Conforme refere Elias (2019), as cifras negras estão ligadas a diversos fatores, sendo, a hesitação das entidades em apresentar queixa da ocorrência, às autoridades competentes, uma delas. De facto, muitas organizações, quando veem os seus sistemas informáticos corrompidos, têm o receio de que tal possa tornar-se público, denegrindo a sua imagem e, consequentemente, afete a sua presença no mercado. O mesmo se passa com os cidadãos quando não reportam as ocorrências de que foram vítimas no ciberespaço, evidenciando a sua reticência perante a denúncia às autoridades policiais ou judiciárias. É desta forma que se conclui que, o número de ocorrências e incidentes criminais, no âmbito do cibercrime, são inferiores à realidade dos factos.

Em jeito de conclusão, é possível perceber, através deste subcapítulo, que, nunca o cibercrime esteve tão sofisticado quanto à sua estrutura tecnológica, como atualmente. Gabrosky (2017), refere que o cibercrime é, hoje, bastante diferente daquilo que era há uma década, embora a sua distinção não esteja na natureza substantiva dos ilícitos, mas na mencionada sofisticação dos recursos e meios com os quais são perpetrados.

2.5. Ciberameaças e Ciberataques

Hodiernamente, são inúmeros os milhões de pessoas que, no seu quotidiano, sistematicamente dependem deste espaço virtual. Ora, este, por intermédio da sua estruturação baseada numa rede de redes, serve de auxílio, na medida em que sustenta os mais diversos serviços críticos e infraestruturas. Não obstante, a notável e crescente dependência face ao ciberespaço, potencia a emergência de diversas vulnerabilidades que, consequentemente, expande aquilo que se define como risco social.

É neste sentido que, atores seduzidos a debilitar o normal funcionamento dos sistemas de comunicação, bem como das redes, têm conseguido, por intermédio de ataques, credibilizar ainda mais as ameaças. Ora, ao aumentarem consideravelmente o número dos ataques, também as ameaças se têm tornado, cada vez mais, persistentes, e, consequentemente, mais preocupantes. Assim, face ao poder disruptivo que os ciberataques detêm, urge, como prioridade global o estabelecimento duma estratégia neste âmbito (Nunes, 2012).

Cabe-nos agora, então, caracterizar aquilo que se denomina por ciberameaça, assim como as consequências dessas ações no ciberespaço, quer sejam estas direcionadas para indivíduos, quer para instituições ou organizações.

Elias (2019), refere que as ciberameaças:

> […] são aquelas que exercem a sua atividade e se difundem na rede fruto da utilização massiva das tecnologias de informação, podendo afetar infraestruturas críticas, o equilíbrio funcional da sociedade – sistemas informáticos dos Governos, das empresas, dos cidadãos em geral -, assim como os sistemas políticos e financeiros internacionais (Elias, 2019).

Tendo em conta a quantidade de informação disponível nas redes e a sua falta de censurabilidade e sensação de impunidade, além do rápido e fácil acesso a potenciais alvos, conjugado com dinâmicas de oportunidade adjacentes, o próprio ciberespaço, acaba, por si só, a motivar a prática de ilicitudes. Face ao exposto, denota-se que o policiamento deste mesmo espaço é dificultado, viabilizando-se, assim, o aumento exponencial das ameaças ao mesmo (Silva, 2012).

Atualmente, as ciberameaças subjugam os limites das indústrias e de outros setores específicos, impactando numa ampla gama de áreas, sendo, portanto, o reflexo da natureza ubíqua da interconectividade do ciberespaço, no contemporâneo (ENISA, 2023).

O cibercrime, mencionado e exposto num anterior capítulo, é, entre muitos outros exemplos, uma ciberameaça. Elias (2019), enumera algumas das ciberameaças mais expressivas no panorama atual, designadamente: "o ciberterrorismo, a ciberespionagem, a cibercriminalidade, o hacking e o hacktivismo".

Kumar et al. (2005), dividem as ciberameaças em dois campos. Por um lado, enumeram as ciberameaças de cariz mais genérico, sendo estas: as violações de autenticação (i.e., *passwords* descodificadas), "cavalos de troia"[17] e vírus, sabotagem (*hackers* que conseguem corromper a segurança de *websites*, sejam estes de organizações, ou até mesmo do governo, destruindo informações), fraude e ataques a serviços de comunicação. Por outro lado, são enumeradas as ciberameaças às bases de dados da *web*, tais como: violações aos controlos de acesso a bases de dados, bem como a violações de confidencialidade, integridade, autenticidade e privacidade dessas bases de dados.

Para que se tenha uma noção do panorama nacional, em 2022, o CNCS (2023a) expôs, no *Relatório Cibersegurança Em Portugal: Riscos & Conflitos*:

[17] "Cavalos de troia" são um tipo de vírus/*malware*, que aparentemente se passam por programas ou sistemas inofensivos, de maneira que o utilizador os instale na máquina, contaminando, assim, o sistema/*software* (Agrawal et al., 2014).

> As ciberameaças a afetar o ciberespaço de interesse nacional em 2022 de modo mais relevante foram o ransomware, a cibersabotagem/indisponibilidade o phishing/smishing/vishing, a burla online, outras formas de engenharia social e o comprometimento de contas/tentativa de login. (CNCS, 2023a, p. 7)

Os ciberataques são imprevisíveis e a identificação da sua origem é desafiadora, representando uma ameaça sem uma identidade clara, e, nos tempos atuais, a consumação desse fenómeno é algo menos complexo do que aquilo que se pensa (Aparício, 2017).

É, cada vez mais, recorrente a propensão para ataques progressivamente mais danosos aos sistemas de informação cruciais para os Estados, bem como a funções específicas dos setores público e privado, tendo em conta o desenvolvimento de instrumentos paulatinamente mais sofisticados a que os criminosos têm acesso, podendo, assim, realizar ataques de vários tipos (Silva, 2012).

Fernandes (2012), destaca que, além da digitalização da economia, a própria difusão da Internet viabiliza diversas vulnerabilidades, dependências e riscos. Isto é notório, uma vez que, até mesmo a organismos públicos e a empresas privadas são possíveis alvos de ciberataques, ou ainda, uma ciberguerra que envolva atores estaduais.

Destarte, o ciberataque define-se, de um modo geral, como um ataque iniciado geralmente através de um computador, fazendo recurso a ferramentas de intrusão. Este, tem como finalidade aceder a informação presente noutros computadores ou redes dos mesmos, ou a qualquer sistema ou equipamento eletrónico ligado a outro. De acordo com a natureza dos alvos, divergem, portanto, os efeitos do ciberataque, podendo ser mais ou menos gravosos consoante o referido. Isto é, caso o alvo constitua uma infraestrutura crítica de um Estado, logicamente os efeitos do referido ciberataque assumirão consequências mais gravosas do que se atacasse uma infraestrutura mais simples. Neste sentido, um ciberataque em grande escala e amplitude, assume consequências em diversos níveis, entre eles, o civil, político e militar, suportando, por isso, efeitos estratégicos (Moreira, 2012).

Até mesmo no que respeita às organizações mais resistentes, os ciberataques implicar-lhes-ão, invariavelmente, danos financeiros e reputacionais. Ora, ao sofrer um ciberataque, uma organização sujeita-se à perda de ativos, além dos custos referentes à reparação a que o ataque consequentemente demandou (Seemma et al., 2018).

De acordo com Elias (2019), a *Estratégia Nacional de Segurança do Ciberespaço*[18], postula seis eixos de intervenção, eixos estes que se afiguram em medidas específicas e respetivas linhas de ação, com o objetivo de substanciar a potencialidade estratégica nacional neste domínio. Face à presente investigação, importa destacar o Eixo 3, referente à Proteção do Ciberespaço e das Infraestruturas, que se afigura mediante "avaliação da maturidade e a capacidade das entidades públicas e privadas, que administrem infraestruturas críticas ou serviços vitais de informação" (p. 75).

Além disso, este eixo efetua-se através da melhoria e adaptação incessante da proteção dos sistemas de informação das entidades públicas, bem como dos profissionais que operam nas infraestruturas críticas e nos serviços de informação, a fim de garantir a resiliência nacional, designadamente naquilo que diz respeito à adaptação face às vulnerabilidades hodiernas dentro do ciberespaço. Da mesma maneira, por forma a antecipar e prevenir possíveis ataques, bem como intervir corretamente na tomada de decisão a que estes compelem, releva-se a análise ao ambiente de informação e o acompanhamento das constantes novidades tecnológicas. Por fim, Elias (2019), reforça a "inclusão de medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais" (p. 76).

[18] ENSC anterior à atual Estratégia (Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho)

Capítulo III – A Cibersegurança na PSP e a Problemática do Fator Humano

3.1. A PSP e as TIC

As tecnologias de informação e comunicação alteraram a interpretação sobre a distância, acessibilidade e disponibilidade de todas as pessoas, tornando-se, então, em plataformas que influenciam, significativamente, a opinião pública, uma vez que se encontram à disponibilidade de todos. Ainda sim, devido à sua influência no campo político e social, é cada vez mais recorrente a existência de debates sobre a utilização destes instrumentos e plataformas (Militão, 2014).

Nesta senda, e, de forma sucinta, cabe-nos conceptualizar aquilo que são as TIC, sendo que existem várias abordagens a este conceito. As tecnologias de informação e comunicação, para Agoga (2001), caracterizam-se como todos os dispositivos eletrónicos que formam, agrupam, "recuperam e transmitem a informação, a 'grandes' velocidades e em 'grandes' quantidades" (p.24). Por outro lado, Ferreira (2017), entende as TIC como o software que agrupa todos os sistemas de comunicação e processamento de dados.

Numa vertente policial, Engelbrecht et al. (2019), indicam que as TIC são utilizadas tendo em conta a necessidade de se obter dados e informações adequadas para cada situação policial, considerando a própria atividade policial como incerta e mutável.

De facto, a PSP faz uso das TIC há vários anos e, no seguimento, Gomes (2013), afirma que esta utilização pode ser vista em duas vertentes, "a vertente operacional e a vertente de apoio à atividade operacional, onde se inclui toda a atividade de gestão e funcionamento quotidiano da PSP" (p.2).

Com efeito, apraz-nos, então, referir alguns dos Sistemas e Tecnologias de Informação e Comunicação (STIC) mais utilizados pela PSP, nomeadamente pelos seus polícias. Efetivamente, no respeitante aos STIC, a PSP é uma instituição que opera interna e externamente para dar resposta a todas as situações que assim o exijam na sua atividade diária. Ora, a PSP opera nos seus sistemas e *softwares* internos, mas também em sistemas externos por força legal, processual e administrativa a que o seu serviço/função exige.

Portanto, é fundamental para a presente investigação, ter-se uma noção daquilo que são algumas das STIC usadas pelos polícias e perceber, posteriormente, se fazem um uso seguro das mesmas.

A atividade operacional da polícia requere um recurso a informações e a dados específicos que podem ser encontrados agrupados em diversas STIC de várias áreas policiais, "nomeadamente em áreas como fiscalizações, gestão de meios e recursos, informações policiais, trânsito, investigação criminal, segurança privada, armas e explosivos, grandes eventos, entre outras valências" (Azevedo, 2023, p. 12).

Assim, podem enumerar-se alguns destes STIC da atividade operacional, tais como: o Sistema Estratégico de Informação (SEI), o Sistema Integrado de Gestão de Segurança Privada (SIGESP), o Sistema de Contraordenações de Trânsito (SCoT), o Sistema de Informação e Gestão de Armas e Explosivos (SIGAE) e a Plataforma para o Intercâmbio de Informação Criminal (PIIC) (Azevedo, 2023).

Do mesmo modo, é-nos possível identificar uma outra tecnologia de comunicação, também interna, utilizada pelos profissionais da PSP, a Intranet do Ministério da Administração Interna. Esta plataforma conta com diversos domínios operacionais e administrativos, de diversas entidades estatais, como é o caso da PSP, da Guarda Nacional Republicana (GNR), da Inspeção-Geral da Administração Interna (IGAI), da Autoridade Nacional de Segurança Rodoviária (ANSR), do Sistema de Segurança Interna (SSI) e outros.

Jerónimo (2017), entende a intranet como "uma rede de comunicação privada usada internamente nas organizações, tendo como objetivo ser um meio de comunicação digital direcionado para o público interno da empresa" (p. 33). Esta plataforma é acessível apenas aos profissionais de cada domínio, no caso em concreto, o da PSP, e, só pode ser feito a partir do *browser* de um computador da instituição, garantindo que o seu uso não seja feito por nenhuma máquina alheia à instituição, conferindo-lhe um acrescido grau de segurança.

O objetivo da implementação de uma Intranet numa organização é construir um sistema comunicacional e de partilha de informação, possibilitando, aos utilizadores, o acesso a elevados volumes de informação interna (Jerónimo, 2017), eficaz e eficientemente.

Esta ferramenta digital é de elevada importância para o comportamento organizacional, visto que auxilia no aumento do "*empowerment*" dos profissionais da organização, mediante o fácil acesso e partilha de informação (Maurício, 2006).

3.1.1. RNSI

A Rede Nacional de Segurança Interna (RNSI) é uma rede cedida aos Serviços e Forças de Segurança e a todos os organismos do MAI. Traduz-se numa rede de comunicações que oferece um serviço de IP seguro de partilha de serviços e cooperação, é uma rede "integrada e de alto débito" que suporta, ainda, grandes volumes de informação, imagem e voz (SGMAI, 2018).

Esta Rede, de acordo com o SGMAI (2018), é um serviço fulcral para garantir o cumprimento dos deveres do Estado e para a proteção dos cidadãos, bem como para garantir a manutenção da ordem e tranquilidade públicas, sendo, portanto, essencial evitar a difusão da localização física da mesma.

Deste modo, o CSIRT.MAI[19] é um organismo que está encarregue de fornecer a devida segurança a esta rede, seja preventivamente, ou de forma reativa. Ora, este organismo é importante para adequar os sistemas de segurança, assim como operar os serviços de resposta a incidentes de segurança no ciberespaço, tendo em consideração os riscos a que estão sujeitos os "clientes" da RNSI, como é o caso da PSP. Em 2012, nasce o Centro de Operações de Segurança Informática (COSI), um centro de apoio à equipa de CSIRT do MAI, de maneira a reforçar o serviço de resposta a incidentes de segurança, realizando, deste modo, um serviço contínuo "com foco na prevenção, monitorização, controlo e reação a este tipo de fenómeno de segurança no ciberespaço" (CSIRT.MAI, 2024a).

O MAI, desde o momento da criação da equipa COSI, tem tido uma participação cada vez mais presente e ativa na Rede Nacional CSIRT, que, por sua vez, também conta com a SGMAI/RNSI como membro, desde 16 de maio de 2012, de acordo com a RNCSIRT (2024), sendo, portanto, essencial na identificação e proteção de possíveis ciberataques.

[19] Os *Computer Security Incident Response Team* (CSIRT), isto é, os serviços de resposta a incidentes de segurança informática, são descritos como fulcrais preventivamente e, também de forma reativa aos ciberataques e fenómenos análogos (SGMAI, 2018).

Nesta senda, a Secretaria Geral do Ministério da Administração Interna entende que, no âmbito da segurança e gestão de redes, devem ser aplicados três grandes princípios, sendo eles a disponibilidade (que possibilita garantir que, quando necessário, os dados/informação estão disponíveis), a integridade (permitindo assegurar que os dados/informação não são corrompidos nem alterados) e, por último, a confidencialidade (garantindo que os dados/informação são acessíveis apenas a indivíduos autorizados) (SGMAI, 2018).

3.2. Formação, Educação e Sensibilização

Atualmente, e com as mutações que o mundo digital apresenta, torna-se fundamental que os polícias possuam conhecimento necessário para, no mínimo, operar de forma segura no ciberespaço, aquando do exercício das suas funções e fora dele, visto que "estas mudanças obrigam os polícias a atualizarem-se em termos de conhecimentos, procedimentos e técnicas" (Felgueiras, 2011). É neste sentido que a formação, nomeadamente, a formação contínua, entra em "cena" e afigura-se como uma ferramenta essencial para a modernização e para a segurança de organizações como a PSP. Desta forma, van Beek et al. (2005), afirmam que, com a célere evolução da sociedade hodierna, onde se incluem os polícias, estes veem-se forçados a atualizar as suas competências de forma contínua, visando uma polícia mais competente e com capacidade em realizar todas as suas atividades essenciais adequadamente.

É sob este prisma que, Ferreira e Moreira (2014), apresentam as condições necessárias para que a formação contínua na PSP se destaque pelas competências adquiridas, sendo essas condições: a "adoção de estruturas curriculares e de percursos metodológicos inovadores e dinâmicos"; a "implementação e organização de *workshops*, seminários, debates e palestras com profissionais com experiências e de áreas próximas ou interrelacionadas"; a "motivação dos formandos para a pesquisa, investigação e desenvolvimento de projetos adequados e ligados à realidade profissional"; a atualização tecnológica dos recursos pedagógicos e formativos; e a gestão e a organização da formação, "estimulando ainda a formação de formadores nas áreas técnico-policiais e a sua consequente integração na bolsa de formadores" (p. 53).

Silva (2012), dá um elevado foco à importância da formação dos polícias na área da cibersegurança, tendo em conta a especificidade e sensibilidade dos dados que a própria

Polícia gere, isto porque, para os polícias, estarem devidamente formados nestas matérias "é vital dado que todos trabalhamos inevitavelmente com TIC, respeitando o sentimento de *awareness* temos de ter incutidos valores de Cibersegurança para não fazer perigar os sistemas e redes, pessoais, das Organizações e até do próprio Estado" (p. 53). Mouradian (2017), partilhando a mesma ideia, afirma que a formação e a sensibilização, no que concerne a matérias de segurança, devem ter como objetivo fundamental melhorar a ciber-higiene em todas as organizações.

No seguimento, e, quanto à educação dos Polícias nesta área, Elias (2019), indica a Estratégia Nacional de Segurança do Ciberespaço, nomeadamente num dos seus eixos de intervenção, referente à educação, sensibilização e prevenção, como um guia para a PSP, na ótica de melhor sensibilizar os polícias, referindo que "é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço" (p. 75). No mesmo sentido, Zwilling et al. (2022), afirmam que qualificar os profissionais é benéfico, visto que, quanto mais conhecimento em cibersegurança um colaborador tiver, mais elevada é a sua sensibilização para a mesma.

Ora, a própria ENSC 2019-2023 realça a importância da sensibilização, nomeadamente num dos seus eixos de intervenção, implementando uma das suas medidas do Plano de Ação a concretizar, traduzindo-se com a questão de sensibilizar as entidades públicas para as vulnerabilidades a que estão expostas diariamente, no domínio do ciberespaço.

Nesta senda, é importante referir que a educação, nestas matérias, procura conjugar a generalidade das competências num só estudo, traduzindo-se, portanto, num modo de ensino dessas mesmas competências, que permitem aos profissionais utilizarem ferramentas básicas e adequadas em prol da segurança da organização (Peltier, 2005; Wilson & Hash, 2003). A educação pode ser utilizada para alterar a sensibilização para a segurança, dotando os profissionais de uma organização do *know-how* certo, e esta sensibilização promove a "ciberconsciencialização", à medida que esta evolui do conhecimento para a aceitação, convicção e comportamento do colaborador (Alfawaz et al., 2010; Eminağaoğlu et al., 2009).

Na ENSC 2019-2023, é apresentada, entre muitas outras linhas de ação, uma medida de prevenção, educação e sensibilização para a segurança do ciberespaço, onde refere que:

> Tirar proveito das estruturas de ensino e formação militares e policiais nacionais e internacionais, aproveitando em particular a oportunidade da edificação em Portugal de estruturas específicas de ensino da Organização do Tratado do Atlântico Norte e da União Europeia e iniciativas associadas, para o aprofundamento do conhecimento relacionado com o ciberespaço e contribuindo para a sensibilização e prevenção na sua utilização.[20] (Resolução do Conselho de Ministros, 2019).

Por último, segundo Ferreira e Moreira (2014), é de salientar a importância que os cursos de formação têm em identificar e selecionar as competências pretendidas, para que, posteriormente, mediante essa identificação, se "selecionem os saberes básicos inerentes a cada área de conhecimento assim como estruturem o projeto pedagógico a implementar" (p. 52).

3.2.1. Núcleo de Cibercriminalidade - PSP

Não obstante, o Núcleo de Cibercriminalidade no Departamento de Investigação Criminal da Direção Nacional da Polícia de Segurança Pública, foi originado a partir do Despacho n.º 6158/2017, e, esta valência policial, foi criada no final de 2020, contudo, só em janeiro de 2021 é que viu, efetivamente, as suas funções iniciarem. Ora, este Núcleo, tem como finalidade apoiar a Investigação Criminal no que diz respeito aos crimes informáticos e com recurso a meios informáticos, no âmbito das competências da PSP. A criação do Núcleo de Cibercriminalidade foi um marco de elevada importância a nível da segurança do ciberespaço na PSP, contudo, Pereira (2022), afirma que, no que diz respeito à formação dos seus polícias, nomeadamente, na vertente de prevenção, "a PSP carece de investimento na especialização dos seus elementos" (p.20).

Portanto, esta valência da PSP auxilia a Investigação Criminal (IC) de várias formas, sendo a formação nos cursos de IC da Polícia de Segurança Pública uma delas. Neste sentido, são ministradas aulas, onde o conteúdo versa a cibersegurança, em concreto a "Segurança da Informação e Comportamentos Seguros", abrangendo temas de ciber-higiene relevantes, particularmente: as regras de *backups*; a gestão das redes sociais (seja para efeitos profissionais, como pessoais); *links* desconhecidos via *email*; o *spam*; o *pshishing*; as plataformas de compras *online*; a gestão das *passwords*; e a gestão dos computadores de serviço.

[20] Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho.

O Núcleo de Cibercriminalidade, para além da sua vertente reativa e preventiva, no apoio à Investigação Criminal, tem vindo a desenvolver ações de cariz preventivo junto da sociedade e, também, dos seus polícias. Com efeito, este núcleo, conjuntamente com uma entidade parceira, o ".PT" (entidade nacional responsável pelo registo de domínios .pt), promoveram *workshops* de cibersegurança, no contexto do "Roteiro INCoDe.2030 – Capacitação Digital", tendo realizado 3 *workshops*, em 2022, e 9 *workshops*, em 2023, dedicados aos desafios e às boas práticas de cibersegurança. Estas ações de prevenção eram abertas e gratuitas a toda a população, mediante inscrição prévia, e, aquando dos eventos, era difundida pelo Comando Distrital de Polícia da área da realização do *workshop*, visando todos os polícias que manifestassem interesse, para que pudessem inscrever-se nas mesmas. O seu conteúdo era diversificado e relevante, não só para a vida profissional do polícia, mas também para a pessoal, abordando tópicos como: a gestão de *passwords*; a importância dos *backups*; a gestão das redes sociais e a privacidade; normas de proteção de *software* malicioso; e as formas mais comuns de incidentes de cibersegurança (engenharia social e *phishing*) e como preveni-las.

Complementarmente, o núcleo encarrega-se de difundir alertas operacionais ao efetivo policial, sempre que se afigure necessário, como é o caso de *links* desconhecidos disseminados por mensagens de correio eletrónico, de remetente alheio à instituição, que se constituem como situações de *phishing*, tentando, muitas das vezes, a obtenção dos dados de autenticação dos profissionais de polícia.

Por último, para além dos alertas de conteúdo malicioso, emitido pelo núcleo, este também prepara e forma polícias a responderem aos ataques no ciberespaço. Efetivamente, a PSP, através do Núcleo de Cibercriminalidade, e em estreita colaboração com o ECTEG (*European Cybercrime Training and Education Group*), está a desenvolver um curso de formação de cibercriminalidade para *first responders* (eFIRST). É um curso elaborado por peritos e especialistas de cibercriminalidade e cibersegurança, de várias Polícias europeias, onde se prevê a sua conclusão para o final do ano de 2024. No que diz respeito à Polícia de Segurança Pública, este curso de *first responders*, será implementado e ministrado nos respetivos cursos de formação de polícias, isto é, no Curso de Formação de Agentes (CFA), no Curso de Formação de Chefes (CFC) e no Curso de Formação de Oficiais de Polícia (CFOP).

3.3. A Problemática da Natureza Humana na Cibersegurança

Barrinha (2020), foca no fator tecnológico em detrimento do humano, referindo que operar através de organizações com arquiteturas de segurança fortes, é a maneira mais eficaz para nos salvaguardarmos de incidentes e ataques cibernéticos.

Contudo, existem relatórios, segundo a Proofpoint (2019), que apontam que menos de 1% dos ciberataques são realizados por via das vulnerabilidades dos sistemas informáticos, o que significa que a maior parte destes ataques exploram o fator humano, "os instintos de curiosidade e de confiança que levam pessoas bem intencionadas a clicar, descarregar, instalar, abrir, e a enviar dinheiro ou dados." (p. 2).

De facto, existem inúmeros incidentes que advém dos comportamentos dos utilizadores do ciberespaço numa determinada organização, pelo que se torna crucial tê-los em consideração, no que diz respeito à cibersegurança da mesma (Baptista, 2017; CERT, 2013). Portanto, CERT (2013), enumera os incidentes mais comuns: a divulgação acidental (partilha de informações confidenciais); o código malicioso (*e. g.* vírus e *spywares*) e perda, furto/roubo de dispositivos eletrónicos (*e. g.* computadores, *pens* USB e discos rígido externos), sendo todos estes tipos de incidentes originários de fatores humanos, comprometendo, desta forma a cibersegurança das organizações.

Deste modo, de referir que estes incidentes, segundo CERT (2014), devem-se a vários comportamentos e características individuais, como a falta de atenção por parte do colaborador da organização; colaboradores com uma aceitação ao risco demasiado elevada; ansiedade e *stress* por parte de quem opera as tecnologias; e por último, o pouco ou nenhum conhecimento em segurança neste domínio. Daí que seja imperativo um conhecimento primário de cibersegurança, visto que quanto menor o conhecimento nesta área por parte dos trabalhadores, maior é a probabilidade de a organização/instituição vir a sofrer um ciberataque (CERT, 2014).

3.4. Medidas de Mitigação de Incidentes de Cibersegurança

Existem inúmeras medidas que, de uma forma ou outra, direta ou indiretamente, auxiliam na redução do número de incidentes de cibersegurança, de origem humana, nas organizações e na vida privada.

3.4.1. Cultura de Cibersegurança

Uma das medidas fulcrais que facilita essa mesma mitigação, é uma cultura de cibersegurança forte, que, de acordo com a ENISA (2017), pode ser entendida como o conjunto de:

> (…) conhecimentos, crenças, perceções, atitudes, normas e valores das pessoas relativamente à cibersegurança e o modo como se manifestam no comportamento das mesmas com as tecnologias da informação (…), traduz-se em tornar as considerações de segurança da informação parte integrante do trabalho, dos hábitos e da conduta de um colaborador, integrando-as nas suas ações quotidianas (ENISA, 2017, p. 7)[21].

Na ENSC, nomeadamente no seu Eixo 2 "*Prevenção, educação e sensibilização*", é apresentada esta mesma ideia, indicando que a segurança deste domínio está dependente de uma cultura de segurança eticamente integrada, proporcionando, aos cidadãos, toda a consciência e conhecimento necessários para um melhor uso do mesmo, salvaguardando a sua segurança e mitigando as possíveis exposições ao risco (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho).

Não obstante, em Portugal já se faz sentir cada vez mais esta cultura de cibersegurança, como indicam os dados do último "*Relatório Cibersegurança em Portugal*", publicado pelo CNCS, em dezembro de 2023, referindo que em Portugal existiam mais organizações, em 2022, com políticas de segurança das TIC, comparativamente à média da EU, 43% e 32%, respetivamente (CNCS, 2023b). Segundo o mesmo relatório, a área metropolitana de Lisboa, foi aquela que mostrou mais resultados no que diz respeito à quantidade de Câmaras Municipais com estratégias de segurança de informação definidas.

3.4.2. Ciber-Higiene

O conceito de ciber-higiene, é um conceito que não encontra, ainda, uma definição que reúna um consenso dos especialistas (Vishwanath et al., 2020). Ao passo que o relatório "*Review of Cyber Hygiene practices*" de 2016, da ENISA, a Agência Europeia para a Segurança das Redes e da Informação, sublinha a necessidade do estudo da ciber-

[21] Traduzido.

higiene, mas também fornece algumas orientações adicionais para o desenvolvimento do conceito.

Nesta senda, a ENISA (2016) refere que:

> (…) a ciber-higiene deve ser encarada da mesma forma que a higiene pessoal e, uma vez devidamente integrada numa organização, passam a simples rotinas diárias, bons comportamentos e exames ocasionais, para garantir que a saúde *online* da organização encontra-se em ótimas condições[22] (ENISA, 2016, p. 6).

De modo complementar, é um princípio essencial, respeitante à segurança da informação, e, de maneira metafórica com a higiene pessoal, também este tipo de higiene, se relaciona com normas rotineiras simples, que, bem empregues, reduzem o risco de ciberameaças (ENISA, 2016).

Adicionalmente, na versão 6.1 do "*The CIS Critical Security Controls for Effective Cyber Defense*", a ciber-higiene pode ser vista como um meio de manter e proteger, de forma adequada, os dispositivos e sistemas informáticos, implementando as melhores práticas de cibersegurança. Isto é, são práticas e medidas que os utilizadores de computadores e outros dispositivos tomam, diariamente, de forma a assegurar o bom funcionamento do sistema e melhorar a segurança *online*. Estas práticas garantem a segurança da identidade e de outros dados que possam ser corrompidos (CIS Controls, 2015). Assim, tal como a higiene diária e pessoal de cada um, também a ciber-higiene é efetuada, frequentemente, para evitar a deterioração natural e as ameaças comuns.

Por outras palavras, a ciber-higiene refere-se ao conjunto de práticas e regras de cibersegurança que os utilizadores *online* devem seguir, de forma a proteger a segurança e a integridade das suas informações pessoais nos dispositivos conectados à Internet, prevenindo, assim, a possibilidade de comprometimento em caso de ciberataque. Para profissionais que atuam em organizações, a ciber-higiene abarcaria a proteção das informações e dispositivos, que se encontram sob a sua responsabilidade, com o intuito de evitar os tais comprometimentos ou violações de segurança (Vishwanath et al., 2020). Ora, de acordo com este autor, esta definição não se prende a um dispositivo específico, sistema ou ambiente digital do utilizador, o que a torna escalável e aplicável a um amplo conjunto de dispositivos tecnológicos e vários cenários de utilização. Desta forma, esta

[22] Traduzido.

definição, acomoda diversos tipos de consumidores, práticas e tecnologias, adaptando-se às mudanças com o passar do tempo.

Por outro lado, Maybury (2015), classifica a promoção da ciber-higiene como parte daquilo que é o princípio da assimetria no âmbito das operações de manutenção de uma determinada organização. Este autor introduz, ainda, uma nova visão deste conceito, concluindo que muito do esforço e enfoque da temática, é versado para o elemento humano, de modo que, no futuro, segundo a sua previsão, o *focus* será e terá de ser dado à conceção e à arquitetura tecnológica de cada instituição/organização.

A falta de higiene é, realmente, um fator de risco. Ao passo que uma adoção e consequente adaptação de uma melhor ciber-higiene é fundamental para que muitos dos incidentes, como o phishing, não tenham o desfecho pretendido. (Chaudhry & Rittenhouse, 2015).

Por último, Maennel et al. (2018), concluem, apresentando uma proposta deste conceito, onde a "ciber-higiene é um conjunto de práticas destinadas a proteger os ativos e a vida humana do impacto negativo dos riscos relacionados com a cibersegurança" (p. 299).[23]

3.4.3. Boas Práticas de Ciber-Higiene

Tendo por base aquilo que foi mencionado acerca do conceito de ciber-higiene, cabe-nos, agora, caracterizar e apresentar algumas das mais básicas e fundamentais boas práticas de ciber-higiene. Ora, a ENISA (2016), uma das entidades internacionais que mais se destaca naquilo que é a cibersegurança a nível europeu, afirma que o pressuposto subjacente é que, inevitavelmente, fazer uso de boas práticas de ciber-higiene continuamente, conduz, efetivamente, ao incremento de imunidade na generalidade das organizações/instituições.

Com efeito, o ponto de partida passará por se adotar uma postura de maior consciencialização, daí, Şcheau & Pop (2018) afirmarem que um aumento desta atitude de consciência por parte da população, traduzir-se-á, no suporte fundamental dos esforços da luta contra a criminalidade.

A mudança de atitude é algo fulcral quando se trata de assuntos como a cibersegurança, numa vertente de cariz individual. Ora, a Internet não é algo que a

[23] Traduzido.

sociedade em geral deva ter receio ao fazer utilização da mesma, no entanto, também não é um domínio inócuo. De facto, Singer e Friedman (2014), afirmam que um estudo conclui que cerca de dois terços das vítimas de crimes cibernéticos, não tinham, simplesmente, conhecimento dos riscos existentes nestas matérias.

Na ótica de Singer e Friedman (2014), fazemos todos parte de um ecossistema em que as responsabilidades que possuímos, não são unicamente para com os outros, mas, também, para connosco próprios. Isto é, a generalidade da população não está a lidar com problemas graves de segurança nacional, contudo, a falta de bom senso começa a querer fazer "ruído", no qual, aqueles que desejam incorrer no crime, podem ver facilitada a sua oportunidade de o consumarem. É desta forma que, estes autores, concluem que existem diversas medidas (simples) que podem ser tomadas:

> A *Australian Defence Signals Directorate* (equivalente à *National Security Agency* dos Estados Unidos da América), descobriu num estudo que, com apenas algumas ações primárias – "whitelisting", uma correção muito rápida de aplicações e de vulnerabilidades do sistema operativo que restringe o número de pessoas com o acesso de administrador a um sistema – impediram que 85% dos ataques direcionados fossem bem sucedidos.[24] (Singer & Friedman, 2014, p. 241).

De acordo com o CNCS (2022), a ciber-higiene é tão importante quanto a higiene pessoal, ao mesmo tempo que afirma que a responsabilidade pela cibersegurança é, de facto, dos cidadãos e não da tecnologia em si. Nesta senda, apresenta diversas normas básicas e boas práticas que cada pessoa deve ter, aquando da utilização do ciberespaço, sendo elas relativas a: *passwords, email, hardware* e navegação.

Destarte, no respeitante às *passwords*, o CNCS (2022), afirma que o objetivo fulcral de cada indivíduo passaria por "complicar" e, desta forma evitar que estas sejam descodificadas manualmente, ou então, com recurso a um *software* de tentativa-erro. As chamadas *passwords* fortes, contemplam diversas características que, efetivamente, as tornam menos propícias ao seu comprometimento, sendo exemplos dessas mesmas características: a alteração da *password* frequentemente; a sua complexidade (i.e., conter mais que 12 caracteres, letras maiúsculas e minúsculas, algarismos e caracteres especiais);

[24] Traduzido.

a utilização de uma *password* por plataforma ou dispositivo; bem como, se se verificar possível, a utilização da função da autenticação de duplo fator.

No que concerne aos cuidados com o *email*, aquilo que refere o supracitado CNCS, é que, este sistema de comunicação, é, muitas das vezes, a porta de entrada de inúmeros ataques a indivíduos ou organizações, pelo que, conhecer a origem dos *emails* é de extrema relevância. Ora, como referido anteriormente, o *ransomware* é disseminado por esta via, através do já conhecido *phishing*, consequentemente, há várias precauções a serem tomadas que o previnem, que de acordo com o CNCS (2022), passam pela atenção aos *links* e anexos recebidos; a veracidade dos *emails*; a identificação do *spam*, de forma que o sistema selecione, previamente, o que realmente é importante, do que não é.

O *hardware* é um outro fator a ter em consideração nesta matéria, sendo o bloqueio o comportamento mais frequente a se adotar. Neste caso, o CNCS (2022), apresenta algumas boas normas, tendo sempre presente o bloqueio de acessos, seja ele a *pen drives* desconhecidas, ou a disco rígidos alheios, que de uma forma ou outra, possam danificar o dispositivo.

Por último, afirma o CNCS (2022), que a navegação pelo ciberespaço é um fator primordial, no que toca a boas práticas cibernéticas. Neste sentido, começa por enaltecer a importância do cuidado ao aceder a redes *Wi-Fi*, nomeadamente àquelas que são públicas, pois estas permitem o acesso mais facilitado aos dados dos dispositivos ligados. É referido ainda os *downloads* desnecessários, tendo em consideração a sua origem. Ademais, uma atitude fundamental a tomar é o uso da *firewall*[25], que controla o tráfego da rede e bloqueia aquilo que é indesejável para o dispositivo, tal como manter o sistema e o antivírus atualizados. Finalmente, considerar como medida securitária os endereços/URL com "https", pois são indicadores de segurança adicional, visto que "permite cifrar as comunicações entre dois pontos, de forma a garantir a Confidencialidade e a Integridade dos dados em trânsito e Não Repúdio da origem ou do destino das comunicações" (CSIRT.MAI, 2024b).

De forma sucinta, Dobbins et al. (2015), afirmam que os cibercriminosos exploram, acima de tudo, a deficitária ciber-higiene dos utilizadores do ciberespaço. Pelo que enumeram algumas das boas práticas securitárias, fundamentalmente *softwares* de

[25] Uma *firewall* é uma ferramenta de segurança da rede que controla o tráfego de rede, quer de entrada ou saída, e faz a gestão dos bloqueios e permissões de tráfegos. Pode, ainda, assumir a forma de um *hardware*, *software* ou ambos (Wack et al., 2002).

segurança que podem ser instalados, tais como: a utilização de *scanners* antivírus, antivírus e *antispyware*[26]; a atualização das aplicações, *software* e sistemas operativos nas primeiras horas após a disponibilização dos *patches* de atualização, entre muitas outras medidas técnicas e comportamentais.

De uma perspetiva internacional, segundo a ENISA (2023), a Bélgica é um dos países da UE que mais se preocupa com as matérias da cibersegurança, e, consequentemente, com a ciber-higiene, focalizando-se, maioritariamente, com instituições nacionais, bem como em pequenas e médias empresas. Portanto, através de um manual de cibersegurança, produzido pela *Microsoft* e por diversas organizações belgas, é-nos possível retirar algumas práticas securitárias de valor acrescido.

Não obstante, no manual do ICC Belgium et al. (2014), são apresentadas muitas das práticas de segurança cibernética supramencionadas, assim como muitas outras medidas. Assim, apraz-nos dizer que se constituem, também, boas práticas de ciber-higiene para as organizações a encriptação dos dados/informação, isto porque, atualmente, a estratégia de segurança da informação não se deve centrar tanto na tecnologia de segurança, mas sim nos dados e na sua encriptação, dado que o controlo de acesso tradicional já não é suficiente, essencialmente quando os dados da organização são armazenados em ambientes de pouca fiabilidade, como a Internet.

No que diz respeito aos dispositivos móveis, constatamos no guia do ICC Belgium et al. (2014), que estes criam desafios significativos de segurança e gestão, nomeadamente, quando são dotados de informações sensíveis da organização. Deste modo, este guia sugere que exista, por parte da organização, a "adoção de uma posição clara acerca dos dispositivos que podem aceder à rede e/ou às informações da mesma e adapte a política e os procedimentos de segurança adequados" (p.27).

A navegação no ciberespaço é uma das maiores preocupações em assuntos de ciber-higiene, daí que, este manual de cibersegurança, reforce essa questão, afirmando que a rede interna da organização só deve ter a possibilidade de aceder aos serviços e recursos *online* que sejam essenciais para esta, bem como para as necessidades profissionais dos elementos

[26] *Antispyware* é um sistema/*software* de segurança de deteção e remoção de *Spyware*. Por sua vez, um *spyware* é um *software* malicioso que se infiltra nos sistemas de computadores e dispositivos, com o intuito de aceder a informações pessoais do utilizador, para que, mais tarde, essa informação possa ser utilizada ou partilhada para fins financeiros ou outros fins mais perversos (Agrawal et al., 2014).

(ICC Belgium et al., 2014). Contudo, o manual prevê, também, que o uso da Internet, se limite aos serviços estritamente necessários.

Efetivamente, estes riscos não se restringem só a vírus e *spywares*, mas torna, também, a organização mais vulnerável ao fenómeno do *phishing*, o que aumenta o risco de os dados/informações pessoais dos profissionais serem comprometidos. É desta forma que, o manual do ICC Belgium et al. (2014), sugere que todos os dispositivos que navegam *online*, devem executar sempre a versão mais recente dos *browsers* que utiliza, pois a maior parte dos *browsers* têm a capacidade de identificar os *websites* de maior risco.

Em suma, a adoção de boas práticas de ciber-higiene, é algo preponderante para qualquer organização que preze a sua segurança informática, assim como a dos seus trabalhadores. Portanto, combinar a utilização de filtragem daquilo que é procurado na *Web*, "proteção antivírus, *firewalls* de proteção proativa contra *malware*, políticas de segurança sólidas" (ICC Belgium et al., 2014, p. 32) e, sobretudo, apostar na formação dos profissionais da organização, reduz, significativamente, o risco de incidentes cibernéticos.

3.4.4. Consciencialização para a Cibersegurança – "Ciberconsciencialização"

Este conceito estende-se a muitas áreas da sociedade, pelo que importa referir aquelas que melhor se enquadram no presente estudo. Neste sentido, abordaremos este conceito à luz daquilo que é realizado em organizações onde, além de uma cadeia hierárquica, existe um envolvimento de todo o efetivo em ambientes tecnológicos, tal como na Polícia de Segurança Pública.

Posto isto, este conceito pode ser definido como um processo de aprendizagem contínua, que é significativo para os colaboradores e que traz benefícios mensuráveis para uma determinada organização, através de mudanças comportamentais que perduram no tempo (ENISA, 2017),

Não obstante, Zook (2019), assemelha o conceito de cidadania digital a este conceito de "ciberconsciencialização", referindo-se ao uso responsável de tecnologia por um indivíduo que utilize a Internet, computadores e dispositivos digitais com o objetivo de se imiscuir com a sociedade. Acima de tudo, é a adoção de um comportamento preventivo para todas as ações desenvolvidas no ambiente digital, indo ao encontro do aspeto principal do conceito de ciber-higiene, mencionado anteriormente.

Portanto, a "ciberconsciencialização" é abordada por Kim (2017), como um procedimento, no qual, tendo por base uma organização, o objetivo é despertar e alertar os respetivos profissionais para a importância da segurança dos sistemas de informação que a mesma requer. Assim, esta abordagem contribui para a conceção de uma consciência coletiva, referente à segurança como uma problemática, com o objetivo de desenvolver motivação por parte dos profissionais a atender às práticas de ciber-higiene, potenciando a proteção de dados e de informações relevantes para a organização. Isto é, por si só, as proteções e sistemas tecnológicos não conseguem tornar uma organização 100% segura, contudo, profissionais bem informados podem ajudar a reduzir os riscos (HIMSS, 2020). Por outro lado, Gleitman et al. (2011), concluem que é a entidade competente que determina as práticas mais adequadas face à segurança da informação, sendo impreterível o empenho e envolvimento do profissional que as desempenha, para a sua efetiva concretização.

Na ENSC 2019-2023, é apresentada esta ideia no seu segundo eixo de intervenção (Eixo 2 – Prevenção, educação e sensibilização), referindo que, a sensibilização, informação e a consciencialização são fatores fundamentais, não só na ótica das entidades públicas ou privadas, mas para toda a sociedade civil.

Concomitantemente, quanto à prevenção do cibercrime, Jahankhani et al. (2014), mostram que é essencial, para este fenómeno, a educação e a consciencialização, chegando a identificar estes elementos como críticos para a redução deste tipo de crimes. Da mesma forma que Baptista (2017), conclui que dar a devida formação e educação, e, consciencializar os profissionais para comportamentos corretos e apropriados para a cultura de cibersegurança, é o sustento para fortalecer as organizações.

Contudo, esta formação, para ter um impacto efetivo na "ciberconsciencialização" numa determinada organização, é necessário que seja desenvolvida tendo em conta dois aspetos: compreender as responsabilidades associadas às diferentes funções de cada profissional; e atingir um nível mínimo de sensibilização/consciencialização em toda a organização (PCI SSC, 2014). Pelo que, todas as pessoas de uma organização deveriam receber um determinado nível mínimo de formação nesta matéria, de modo a estarem preparados e conscientes dos riscos e competências especificamente relacionados com as suas próprias funções dentro da organização (Furnell & Clarke, 2005; Thomson et al., 2006; van Niekerk, 2005).

Segundo Siponen (2000), esta consciência sobre a cibersegurança, proporcionará aos profissionais de uma organização a redução de ações e comportamentos que ameacem a segurança da mesma, pelo que se pode concluir que a atenção dos colaboradores terá que recair sobre a cibersegurança e a segurança da informação, de modo a intensificar a sua sensibilização e cuidado com estes assuntos (Wilson & Hash, 2003).

No seguimento, e em termos práticos, destacam-se alguns dados e estatísticas dos últimos dois anos, em Portugal, respeitantes a esta questão da sensibilização e consciência securitária a nível digital.

Assim, através do "*Relatório Cibersegurança em Portugal*", é-nos possível referir que, em 2022, foram realizadas cerca de 13.600 ações de sensibilização para a cibersegurança em todo o país, que contaram com a participação de mais de 1 milhão de pessoas. Estas ações foram efetivadas tanto *online* como presencialmente, mas, maioritariamente, através de cursos *online*, com cerca de 92%. O conteúdo das ações de sensibilização versava os temas das boas práticas de ciber-higine, a privacidade, o *cyberbullying* e a proteção de dados (CNCS, 2023b).

O ensino superior é um outro fator de propagação desta "ciberconsciencialização", na medida em que, cada vez mais, surgem novos cursos superiores dedicados à cibersegurança e à segurança da informação em Portugal e, até 2023, existiam 28 cursos no total, sendo que 79% são oferta do setor público. O número de alunos e de diplomados cresceu, consideravelmente, no último ano – (24%) - o que se traduz numa maior sensibilização do mercado de trabalho em relação a estas matérias (CNCS, 2023b).

Por fim, Parsons et al. (2017), elaboram um modelo de consciencialização onde conjugam as atitudes, os comportamentos e os conhecimentos, de modo a efetivar essa consciência para a segurança da informação. Ora, é defendido que, quanto mais conhecimentos de cibersegurança e de segurança da informação um determinado profissional possuir, mais adequados serão os seus comportamentos, estando, portanto, mais envolvido e empenhado na segurança da organização a que pertence. Em suma, os comportamentos securitários estão em dependência direta dos conhecimentos de segurança que cada indivíduo de determinada entidade possui, sendo crucial que essa entidade forneça o devido conhecimento, através da educação e formação (Parsons et al., 2017).

Capítulo IV - Método

Segundo Fortin (2000), a produção de conhecimento é o cerne da investigação científica. Como tal, por forma a conceber determinado conhecimento como conhecimento científico, é impreterível o reconhecimento de "operações mentais", bem como de "técnicas", de modo a assegurar a sua verificação. Isto é, precisar o método que viabilizou atingir determinado conhecimento (Gil, 2008, p. 8).

Marconi e Lakatos (2017), determinam que, o método, assenta no agrupamento de "atividades sistemáticas e racionais" que viabilizam que o investigador atinja determinado objetivo, nomeadamente, "conhecimentos válidos" (p. 96). Para tal, o investigador determina uma direção restrita, pertinente e adequada, que providenciar-lhe-á a identificação de imprecisões que coadjuvarão as suas decisões.

Para que uma investigação se desencadeie, é lhe antecedida a definição de um método. Como tal, isto implica cumprir com o estabelecido para as respetivas etapas do procedimento, contudo, pretende-se a valorização da adaptação e flexibilidade, em detrimento da rigidez (Campenhoudt et al., 2019).

Deste modo, imediatamente se estabelece uma estruturação criteriosa das práticas em questão, seguindo, ordenadamente, um caminho que se inicia com a conceptualização, até chegar à conclusão, clara e fidedigna, alinhada com os objetivos previamente determinados para a investigação em causa (Reis, 2010).

Portanto, definida a pergunta de partida, a pertinência e relevância do tema em questão, e a identificação dos objetivos da presente investigação, nomeadamente determinar, no âmbito da cibersegurança e ciber-higiene, o atual nível atitudinal e comportamental dos polícias do COMETLIS, perceber a importância que os polícias do COMETLIS atribuem a este assunto e a viabilidade da implementação de um *Quick reference guide* de cibersegurança na PSP. Cabe-nos, neste momento, dar a conhecer as nossas opções metodológicas, bem como o trabalho realizado para atingir os susoditos objetivos e hipóteses de investigação.

Na etapa inicial da presente investigação, foi priorizada uma abordagem essencialmente teórica, fundamentada através da consulta de documentos, mediante pesquisa e análise de literatura especializada, pertinente à temática em evidência (Marconi & Lakatos, 2017). Assim, através da revisão de fontes bibliográficas inerentes à

cibersegurança e ciber-higiene, fomentou-se a apreensão face ao problema de investigação, o que contribuiu para a formulação de hipóteses (Quivy & Campenhoudt, 1998).

Numa segunda fase, a investigação recorreu-se da utilização de um método quantitativo, que, na ótica de Santos et al. (2016), consubstancia-se, essencialmente, num processo metódico "de recolha de dados observáveis e quantificáveis baseados na observação de factos, acontecimentos e fenómenos objetivos que existem independentemente do investigador" (p. 27), com o objetivo de validar ou refutar as hipóteses formuladas, na etapa precedente da investigação. (Quivy & Campenhoudt, 1998).

Destarte, por forma a efetivar o presente estudo de forma objetiva, íntegra e fidedigna, optou-se pelo emprego de um inquérito por questionário. Assim, no capítulo em evidência, descreveu-se a caracterização dos respetivos participantes, além de se ter procedido à explanação relativa aos instrumentos de recolha de dados priorizados, bem como dos seus procedimentos e técnicas de análise, invariavelmente, de acordo com as hipóteses e objetivos previamente estabelecidos, para, numa última fase, se proceder à apresentação e discussão dos resultados obtidos.

4.1. Caracterização dos Participantes

A caracterização dos participantes do presente trabalho de investigação é feita, primeiramente, identificando o público-alvo utilizado e as razões pelas quais foi escolhido.

Neste sentido, o Comando Metropolitano de Lisboa, doravante designado por COMETLIS, uma unidade de polícia, conforme o artigo 17.º e 19.º n.º 2, al. b), da Lei Orgânica da Polícia de Segurança Pública (LOPSP), foi o comando selecionado para a investigação, apresentando-se como o universo do estudo em questão. Ora, a razão pela qual o COMETLIS foi o comando escolhido para a presente investigação, prende-se com o facto de ser o comando com maior número de efetivo no território nacional, com 7268 polícias[27], sendo também o comando mais jovem, no que diz respeito ao seu efetivo, pelo que, o pretendido, era um maior número de respostas, bem como respostas das várias faixas etárias existentes.

Adicionalmente, no respeitante à caracterização da população, é de realçar que a presente investigação não foi direcionada a um público-alvo específico, dentro do universo

[27] Conforme os dados apresentados no Balanço Social da Polícia de Segurança Pública de 2022 (Anexo II).

de estudo em questão, pelo que se optou por direcionar a investigação a todo o efetivo do COMETLIS, independentemente da sua carreira policial atual (agente, chefe e oficial), assim como as suas funções, sexo e faixa etária. Deste modo, a população do presente trabalho, caracteriza-se tendo por base todos os polícias do comando, tendo, estes, funções administrativas ou operacionais, constituindo-se na sua totalidade por: 175 da carreira de oficial de polícia, 668 da carreira de chefe de polícia e, por último, 6425 da carreira de agente de polícia, conforme o Anexo II.

No mesmo sentido, a partir da população-alvo em estudo, é necessário identificar e apresentar uma amostra, que, segundo Neto (2002), traduz-se numa parte finita da população, a partir da qual será realizada a investigação, de maneira a compreender as suas características. É desta forma que, Sarmento (2013), apresenta uma proposta de equação para calcular a dimensão da amostra aleatória simples (n), que se segue:

Equação 1

Dimensão da amostra aleatória simples

$$n = \frac{p \times (1 - p)}{\frac{\varepsilon^2}{z_{\propto}/2^2} + \frac{p \times (1 - p)}{N}}$$

Assim, importa referir que, para identificar a dimensão da amostra, (N) diz respeito à população finita da presente investigação, (λ) corresponde ao nível de confiança, o erro é representado por (Ɛ) e a proporção da população por (p). Da mesma forma, para o trabalho de investigação, optou-se por um grau de confiança de 95% (λ = 0,95%) e uma margem de erro de 5% (Ɛ = 0,05%), o que corresponde a uma distribuição normal de 1,96.

Portanto, depois de calculada a fórmula da dimensão da amostra aleatória simples, tendo em conta os valores atribuídos, chegou-se a uma dimensão de n=365. Ora, sendo que os inquéritos por questionário foram difundidos a todo o COMETLIS, obteve-se um total de 405 respostas ao mesmo.

Tabela 1

Caracterização sociodemográfica da amostra (N = 405)

	N	%
Género		
Feminino	84	20,7
Masculino	321	79,3
Idade		
18 -25 anos	75	18,5
26 - 35 anos	86	21,2
36 - 45 anos	121	29,9
46 - 55 anos	102	25,2
> 55 anos	21	5,2
Habilitações Literárias		
Ensino Básico	4	1,0
Ensino Secundário	310	76,5
Ensino Superior	91	22,5
Carreira Atual		
Agente de Polícia	249	61,5
Chefe de Polícia	100	24,7
Oficial de Polícia	56	13,8

Relativamente à caracterização sociodemográfica dos participantes do presente estudo, realça-se que, dos 405 polícias do COMETLIS inquiridos, a maioria é do sexo masculino, em concreto 79,3% (n=321), sendo os outros 21% (n=84) dos polícias, do sexo feminino (Figura 3, Apêndice A). No que diz respeito às faixas etárias da amostra, aquela que foi mais representada foi a dos 36 aos 45 anos, com 29,9% (n=121). Tendo em conta a faixa etária dos polícias mais novos (entre 18 e 25 anos), o número de inquiridos foi de 75, correspondendo a 18,5%, comparativamente aos 5,2% (n=21) que se obteve por parte dos polícias da faixa etária mais elevada (mais de 55 anos) (Figura 4, Apêndice A).

Relativamente às habilitações literárias dos inquiridos, a maioria deles está habilitada ao nível do ensino secundário, com 76,5% (n=310), e 22,5% (n=91) ao nível do ensino superior (Figura 5, Apêndice A). No respeitante à carreira atual dos inquiridos, 61,5% (n=249) são Agentes de Polícia, 24,7% (n=100) são Chefes de Polícia e 13,8% (n=56) Oficiais de Polícia (Figura 6, Apêndice A).

4.2. Instrumento de Recolha de Dados

Primeiramente, antes de partir para a apresentação daquilo que foi o instrumento de recolha de dados da presente investigação, é importante clarificar a diferença entre atitude e comportamento. Deste modo, segundo Gleitman et al. (2011), as atitudes consubstanciam-se numa dimensão psicológica de um determinado comportamento, sendo, portanto, uma expectativa, uma perceção, ou até um conhecimento, que, quando interligados, permitem influenciar a análise/juízo de alguém ou de alguma coisa. Isto é, refere-se à avaliação, seja ela positiva ou negativa, que um determinado indivíduo tem relativamente a algo ou alguém.

Por outro lado, os comportamentos são as ações que podem ser observáveis, praticadas por alguém. Ou seja, as atitudes são uma predisposição interna, influenciando a maneira como um indivíduo pensa face a uma determinada situação, ao passo que os comportamentos são a ação efetiva que esse indivíduo concretiza face à mesma situação (Gleitman et al., 2011), pelo que os comportamentos podem, ou não, estar alinhados com as atitudes.

Assim, para analisar aquilo que são os comportamentos e as atitudes, optou-se por realizar a aplicação de um inquérito por questionário, como instrumento de recolha de dados (Sarmento, 2013). Pelo que o recurso a esta ferramenta de recolha de dados não só possibilita a análise estatística de um determinado fenómeno, mas permite, também, examinar e relacionar variáveis que se afigurem relevantes e pertinentes Stockemer (2019), e, para além disso, admite a generalização e comparação, posteriormente, dos resultados obtidos, consequentes da sua utilização (Santo, 2015).

Complementarmente, um inquérito por questionário é, de acordo com Marconi e Lakatos (2017), um conjunto de perguntas que são respondidas individualmente, "sem a presença do entrevistador" (p. 235), e são estas respostas que, mais tarde, possibilita que se verifique todas as hipóteses do estudo, previamente formuladas, tendo em consideração as correlações existentes (Quivy & Campenhoudt, 2005), descrevendo, desta forma, uma determinada população (Reis, 2018).

O instrumento de recolha de dados escolhido foi o inquérito por questionário, uma vez que, para avaliar os comportamentos e as atitudes dos participantes, em relação à cibersegurança e ciber-higiene, afigurou-se necessário recorrer a uma série de

questões/afirmações curtas e diretas, por forma a identificar o nível de consciencialização dos mesmos, e, fazê-lo através da plataforma *online* "Microsoft Forms" demonstrou ser a melhor opção para a boa prossecução do trabalho de investigação em causa. Este instrumento de recolha de dados, conforme Sousa e Baptista (2014), é vantajoso pela sua precisa e direta aplicação e, como apresenta Marconi e Lakatos (2017), fornece ao inquirido um conforto no que respeita a confidencialidade e, a liberdade de determinar onde e quando responder ao mesmo.

Posto isto, importa agora elucidar e apresentar as escalas que dão corpo ao inquérito por questionário. Assim, numa fase inicial, recorrendo a um levantamento da literatura, nomeadamente a escalas que determinem um nível atitudinal e comportamental em cibersegurança existentes e publicadas, elegeram-se as escalas já validadas de Hadlington (2017). Este autor, no seu estudo relativamente à análise dos fatores humanos que levam ou podem levar a que um determinado indivíduo, de maneira não propositada, se transforme numa ameaça no ciberespaço de uma organização, desenvolveu duas escalas: uma, referente aos comportamentos arriscados em cibersegurança (RScB – *Risky Cyber Security Behaviours*) e outra, referente às atitudes em relação à cibersegurança num ambiente empresarial (ATC-IB – *Attitudes Towards Cybersecurity in Business*).

É neste sentido que foi requerida a autorização ao autor das duas escalas para a sua utilização na presente investigação, à qual se obteve resposta positiva (Apêndice B). Dada a autorização do autor (Anexo III), optou-se por utilizar a versão traduzida e validada das escalas para português, apresentadas na investigação de Nunes (2019), conforme se apresenta no Anexo IV, e posteriormente adaptadas para o contexto policial e aplicadas aos polícias do COMETLIS (Apêndice C). Estas adaptações foram feitas, uma vez que as escalas continham algumas questões de contexto empresarial, não se enquadrando com o presente estudo. As adaptações realizadas foram orientadas pelo Professor Especialista Pedro Moita, perito e especialista na área.

A escala de comportamentos arriscados em cibersegurança é uma escala de vinte perguntas, adaptada da escala RScB do estudo de Hadlington (2017). A nova escala RScB é do tipo *Likert*, isto, porque uma *Escala de Likert*, segundo Jebb et al. (2021), fornece uma maneira adequada e apropriada de "medir construtos não observáveis" (p. 1), sendo que a pontuação varia dos 0 aos 120 pontos, considerando que valores mais elevados indicam comportamentos mais arriscados, o que se traduz, consequentemente, em níveis

mais reduzidos de consciencialização securitária. De forma a proceder à sua pontuação e avaliação, a *Escala de Likert* tem os seus valores a variar de 0 a 6, onde (0) corresponde a "Nunca", (1) corresponde a "1 a 2 vezes por semestre", (2) corresponde a "1 a 2 vezes por trimestre", (3) corresponde a "1 a 2 vezes por mês", (4) corresponde a "1 a 2 vezes por quinzena", (5) corresponde a "1 a 2 vezes por semana" e (6) corresponde a "Diariamente", tendo em conta a frequência com que os inquiridos do estudo praticaram determinados comportamentos, durante os seis meses imediatamente anteriores à data da submissão do questionário.

No seguimento, a escala de atitudes em relação à cibersegurança, é composta por vinte e cinco perguntas referentes às atitudes que conduzem as organizações a serem alvos de ataques no ciberespaço, resultantes das práticas deficitárias. É uma adaptação da escala "ATC-IB – *Attitudes Towards Cibersecurity in* Business" de Hadlington (2017), pelo que, esta nova escala adaptada e renomeada de "ATC-P - *Attitudes Towards Cibersecurity in Police*", foi concebida no sentido de apurar a perceção dos polícias do COMETLIS face às ameaças do cibercrime presentes no seu quotidiano, e, da consciencialização da cibersegurança na sua própria instituição, sofrendo, desta forma, alterações linguísticas, face à realidade do presente estudo. Assim, é pontuada segundo uma *Escala de Likert* de apenas quatro pontos, sendo que, (1) corresponde a "Concordo totalmente", (2) corresponde a "Concordo", (3) corresponde a "Discordo" e (4) corresponde a "Discordo totalmente". A sua pontuação global varia entre os 25 e os 100 pontos, onde pontuações mais reduzidas indicam um fraco envolvimento na cibersegurança, e pontuações mais altas traduzem-se num fator positivo na consciencialização securitária do domínio do ciberespaço.

Portanto, urge agora apresentar a estrutura do inquérito por questionário (Apêndice D), que se dividiu em quatro partes. Nesta senda, depois da apresentação introdutória do questionário, onde se contextualizou o assunto do estudo e se esclareceu os procedimentos necessários para responder e submeter o inquérito, foi gerada uma primeira questão relativa ao consentimento dos participantes. Neste, denotou-se uma ressalva, ora, caso o inquirido não consentisse com a participação na investigação, seria conduzido à parte final do questionário, os agradecimentos.

Assim, a primeira parte do questionário diz respeito à caracterização sociodemográfica, composto por quatro variáveis, onde se apuram o sexo, as faixas etárias, as habilitações literárias e a carreira atual dos inquiridos.

A segunda parte consiste em vinte (20) afirmações, relativamente aos comportamentos arriscados em cibersegurança, correspondendo à escala RScB, adaptada ao atual contexto, onde as questões 13, 16 e 23 do questionário são itens com pontuação inversa, para posteriores efeitos estatísticos.

A terceira parte do inquérito por questionário em questão, que conta com vinte e cinco (25) afirmações e corresponde à escala ATC-P, onde os inquiridos respondiam de acordo com o seu nível de concordância, tendo em conta a *Escala de Likert* utilizada. Nesta terceira parte, as questões 27, 28, 39, 40, 44, 45 e 46 apresentam pontuação inversa.

Por último, e, por forma a ir ao encontro da última hipótese de investigação (H3), foi incluído e introduzido o tema no questionário, nomeadamente, nas últimas duas questões, do *Quick Reference Guide* de cibersegurança para o contexto policial. Isto é, foi elaborado um exemplo de um breve manual sobre ciber-higiene, através da pesquisa da literatura do assunto, pelo que a última parte do inquérito consiste no apuramento da perceção policial perante esta ferramenta de auxílio secuitário.

Com efeito, os *Quick Reference Guide* são breves resumos de materiais de formação e de sensibilização, que permitem aos utilizadores e funcionários aprender e assimilar de forma simples os conceitos e regras básicas de um determinado produto ou serviço (Goodwin, 1994). Portanto, este tipo de documentos não excede, por norma, duas páginas, sendo intensamente pormenorizados e bastante simples de interpretação, contendo o estritamente necessário ao utilizador. A sua utilidade serve o profissional, ao cobrir a falta de conhecimentos prévios, permitindo a obtenção de competências genéricas e básicas.

Segundo o CNCS (2022), manuais simples, focados em cibersegurança, nomeadamente nas boas práticas a adotar continuamente, é uma mais valia para as organizações.

É, nesta senda, que nos propusemos a construir um exemplo de *Quick Reference Guide* de boas práticas de ciber-higiene direcionado para os profissionais da Polícia de Segurança Pública. Contudo, a ciber-higiene compreende várias subdimensões, determinadas tendo em conta a função desempenhada por cada profissional, pelo tipo de

departamento/divisão em que opera e, num plano mais genérico, pela organização em si (Vishwanath et al., 2020). Tudo isto, acaba por influenciar as ações e práticas de ciber-higiene que se espera que o profissional, o polícia, tenha.

Assim, tendo em apreço a pesquisa bibliográfica realizada acerca das principais normas básicas de ciber-higiene, bem como a atividade dos polícias no uso do ciberespaço, nomeadamente, os sistemas/*softwares* que utilizam diariamente, foi elaborado uma proposta/exemplo de *Quick Reference Guide* de cibersegurança (Apêndice E).

4.3. Procedimentos

Selecionado o inquérito por questionário como o instrumento de recolha de dados destinado a ser aplicado ao universo do presente estudo, urge explanar os procedimentos necessários e efetuados ao longo da investigação:

1. No que concerne à escolha do inquérito por questionário, após a revisão da literatura e do *feedback* positivo do orientador do presente estudo, mostrou-se evidente que as escalas do estudo de Hadlington (2017), relativas aos comportamentos arriscados e às atitudes em cibersegurança, eram as mais apropriadas para se ter uma perceção do estado atual da consciencialização dos inquiridos, nesta matéria.
2. Definidas as escalas a utilizar no questionário, foi elaborado um pedido de autorização de utilização ao autor das mesmas. Posteriormente, depois de autorizado, recorreu-se às escalas traduzidas do estudo de Nunes (2019). Assim, procedeu-se a uma ligeira adaptação das mesmas ao contexto policial, orientada pelo Professor Especialista Pedro Moita, perito na área. Foi, ainda, elaborado um exemplo de *Quick Reference Guide* em cibersegurança, e adicionadas duas questões relativas à viabilidade do mesmo na Polícia de Segurança Pública.
3. Concluída a elaboração do questionário, foi enviado um requerimento dirigido à Exma. Sra. Diretora Nacional Adjunta, para a Unidade Orgânica dos Recursos Humanos, Superintendente-chefe Paula Cristina da Graça Peneda, solicitando autorização para aplicação do inquérito por questionário aos polícias do COMETLIS (Apêndice F).
4. Após o deferimento do requerido (Anexo V), foi solicitado ao Núcleo de Formação do COMETLIS, o envio do questionário a todo o efetivo policial do

comando (Apêndice G) e, posteriormente, foi solicitado um novo envio dos questionários ao efetivo, por forma a atingir a taxa de resposta pretendida (Apêndice H).

5. O questionário foi suportado através da ferramenta *Microsoft Forms*, ao longo do mês de março.
6. Após a obtenção das respostas pretendidas da amostra, todas as submissões do questionário foram transferidas para uma folha Excel, da qual foram inseridas, mais tarde, no programa *Statistical Package for the Social Sciences* (SPSS), versão 28 para *Windows* (IBM® SPSS® V.28), de modo a serem trabalhadas estatisticamente.

4.4. Instrumento de Análise de Dados

Para Quivy e Campenhoudt (1998), é necessário, após a recolha dos dados alcançados, efetuar uma análise quantitativa dos mesmos, de modo a permitir comparações das respostas obtidas e, consequentemente, analisar as variáveis e as possíveis correlações entre as mesmas.

Efetivamente, como referem Creswell e Creswell (2018), as relações entre as demais variáveis de um determinado estudo de abordagem quantitativo, para serem avaliadas da melhor forma possível, devem sofrer uma análise mediante métodos estatísticos.

Deste modo, na análise dos dados, foi realizada, numa primeira fase, uma abordagem descritiva, através da estatística descritiva dos dados, mediante a construção de tabelas de frequências. Posteriormente, de modo a dar continuidade e melhor concluir a análise dos dados obtidos, optou-se por uma análise inferencial, através da estatística inferencial, onde se testou as hipóteses de investigação do presente estudo, através das variáveis existentes (Marôco, 2021).

Assim sendo, executou-se a análise da primeira hipótese de investigação, onde se assumiu uma distribuição normal tendo em consideração os pressupostos do Teorema do Limite Central, uma vez que n>30 (405 participantes). Posteriormente, nas hipóteses subsequentes, de modo a analisar a normalidade de distribuição de variáveis da amostra, optou-se por recorrer aos testes *Kolmogorov-Smirnov* e *Shapiro-Wilk*. Assim, analisadas todas as variáveis, constatou-se que apresentavam um $p \leq 0{,}05$, (Tabela 17 e 18, Apêndice

I), o que nos leva a concluir que nenhuma apresentou uma distribuição normal, logo, de acordo com Fávero e Belfiore (2017), rejeita-se, desta forma, a H0 (hipótese nula – amostra com distribuição normal).

No seguimento, para a análise estatística dos dados, envolvemos medidas de estatística descritiva (frequências absolutas e relativas, médias e respetivos desvios-padrão) e estatística inferencial. Nesta, utilizou-se o coeficiente de consistência interna *Alpha de Cronbach* (α), de modo a verificar a consistência interna das variáveis do estudo que, de acordo com Hill e Hill (2008), um valor de (α) superior a 0,8, traduz-se em uma boa consistência interna. Contudo, segundo os mesmos autores, são aceitáveis valores acima de 0,6, sempre que o número de itens das escalas seja relativamente baixo.

Foi calculado o coeficiente de correlação de Pearson, de modo a identificar se a correlação entre os comportamentos arriscados em cibersegurança e as atitudes de cibersegurança é estatisticamente significativa e se a sua direção é positiva ou negativa. Ora, segundo Sousa (2019), o valor zero deste coeficiente indica "uma inexistência de uma relação linear entre as duas variáveis", e, "quanto mais próximo de 1 for o valor absoluto deste coeficiente mais forte é a relação linear entre as duas variáveis" (p. 1). Uma direção positiva, indica que as variáveis variam no mesmo sentido, ao passo que uma direção negativa indica o contrário, isto é, variam em sentido inverso.

Optou-se por utilizar o teste T de *Student* para uma amostra e o teste não paramétrico de *Kruskal-Wallis*, que analisa a "distribuição de variáveis", sendo estas observáveis em "duas ou mais amostras independentes" (Marôco, 2021, p. 316). Recorreu-se, por fim, ao teste Binomial, de modo a dar resposta à última hipótese de investigação.

Capítulo V – Apresentação e Discussão de Resultados

Findada a explanação das opções metodológicas para a presente investigação, urge, neste momento, apresentar e discutir os resultados obtidos ao longo da mesma, de modo a dar resposta à pergunta de investigação, a qual serviu de base para o desenvolvimento do estudo em questão, aos objetivos preconcebidos e às hipóteses de investigação.

5.1. Análise Estatística Descritiva

Primeiramente, importa apresentar aquilo que se apurou das respostas dos inquiridos, relativamente às duas escalas (RScB e ATC-P).

Ora, as respostas às questões relacionadas com os "Comportamentos Arriscados em Cibersegurança" podem ser apreciadas na Tabela 2, em percentagem. Em cinza-claro, evidenciamos as respostas mais frequentes, isto é, a "Moda" das respostas. Assim, os comportamentos arriscados realizados com mais frequência ("Diariamente"), são: "Usar a mesma password para diferentes websites." (44.9%), "Guardar informações/dados da instituição no dispositivo eletrónico pessoal." (36.3%) e "Guardar automaticamente as credenciais de acesso ao email/websites." (36.5%).

Tabela 2

Comportamentos Arriscados em Cibersegurança (%)

	0	1	2	3	4	5	6
Partilhar passwords com amigos e colegas.	63,5	26,2	10,1	0,2	0,0	0,0	0,0
Usar ou criar passwords demasiado simples.	54,3	9,9	21,5	11,6	0,2	0,2	2,2
Usar a mesma password para diferentes websites.	6,7	8,4	5,9	4,4	2,7	26,9	44,9
Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível.	24,2	31,4	3,5	2,2	1,5	21,2	16,0
Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita.	61,5	24,4	10,1	1,2	1,2	0,5	1,0
Usar redes de Wi-Fi de acesso livre (públicas), no acesso ao email institucional.	28,9	32,6	2,2	3,2	20,5	11,4	1,2
Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online.	13,8	35,1	6,4	6,2	21,7	11,9	4,9
Identificar devidamente o spam *****	18,3	28,4	4,2	3,5	3,2	6,9	35,6
Guardar automaticamente as credenciais de acesso ao email/websites.	19,5	7,7	4,7	25,7	2,2	3,7	36,5
Utilizar a pen drive pessoal com a finalidade de transferir informação institucional para ela.	19,8	7,7	25,4	23,2	2,5	12,8	8,6
Verificar as atualizações de software do smartphone /tablet /portátil /PC. *****	12,3	6,7	27,2	7,7	26,2	15,8	4,2
Descarregar conteúdos digitais de fontes não fidedignas.	26,9	36,0	21,5	11,4	1,0	1,7	1,5
Navegar em websites que não contenham "https://" no seu URL.	26,9	10,4	2,7	25,7	1,5	30,6	2,2
Utilizar uma pen drive desconhecida no computador, para aceder aos seus conteúdos.	37,5	57,8	0,7	1,0	1,2	0,2	1,5
Clicar em links de emails recebidos de uma fonte desconhecida.	63,7	3,7	29,9	0,7	1,2	0,5	0,2
Enviar informação pessoal a estranhos pela Internet.	88,6	10,9	0,2	0,2	0,0	0,0	0,0
Clicar em links de email enviados por amigos próximos ou por colegas de trabalho.	13,6	13,6	6,4	27,9	22,2	13,6	2,7
Terminar a sessão, sempre que não faça uso do email. *****	25,6	25,4	2,7	5,2	2,5	23,2	15,6
Descarregar informação e material de websites para o computador sem verificação da veracidade.	30,6	29,9	3,5	21,5	12,1	1,5	1,0
Guardar informações/dados da instituição no dispositivo eletrónico pessoal.	18,8	7,4	26,4	5,2	2,7	3,2	36,3

Legenda: 0 – Nunca 1 - 1 a 2 vezes por semestre 2 - 1 a 2 vezes por trimestre 3 - 1 a 2 vezes por mês 4 - 1 a 2 vezes por quinzena 5 - 1 a 2 vezes por semana 6 – Diariamente

* questões com cotação inversa

Neste sentido, constata-se que cerca de 45% dos participantes, afirmaram que, diariamente, utilizam a mesma *password* para vários *websites*, além de 36,5% guardarem, de forma automática, os dados de acesso ao *email* e *websites*, demonstrando um nível de consciencialização precário, neste aspeto de segurança da própria informação.

Adicionalmente, 30,6% dos polícias afirmam que, 1 a 2 vezes por semana, acedem a *websites* que não possuem a certificação de segurança "https://" no seu URL, bem como,

15,6% admitem nunca terminar a sessão do *email*, logo após a sua utilização. Ora, estes comportamentos, podem levar a uma maior exposição a ameaças indesejadas, e, consequentemente, a um maior risco de virem a ser alvos de um ciberataque. Ademais, essa situação tem um peso acrescido e afigura-se alarmante, uma vez que 36,3% dos polícias declaram que guardam, diariamente, informações e dados da instituição nos dispositivos pessoais.

No que diz respeito às repostas das questões relacionadas com a escala "Atitudes em relação à Cibersegurança", podem ser apreciadas na Tabela 3. Assim, as Atitudes que geram mais preocupação e com níveis de concordância mais elevados, são: "A Polícia não tem meios para combater o cibercrime de forma eficaz." (65,2%), "Não tenho as competências necessárias para proteger a instituição do cibercrime." (62,7%) e "Não sei quem é responsável por proteger a instituição do cibercrime." (61,7%).

Tabela 3

Atitudes em relação à Cibersegurança (%)

	1	2	3	4
Penso que a instituição tem a responsabilidade de assegurar que esta esteja protegida de cibercrime.	56,8	42,0	1,2	0,0
Estou ciente do meu papel em manter a instituição protegida de potenciais cibercriminosos.*	0,0	11,6	35,1	53,3
Penso que todos na instituição têm um papel a desempenhar na proteção contra ameaças de cibercriminosos.*	0,0	10,1	31,9	58,0
É difícil saber como posso proteger a instituição do cibercrime.	15,3	39,8	41,5	3,5
Não tenho as competências necessárias para proteger a instituição do cibercrime.	17,0	62,7	16,5	3,7
Não creio que a segurança informática seja uma prioridade na minha instituição.	12,3	27,2	42,0	18,5
Os sistemas informáticos oferecem toda a proteção que uma instituição precisa.	1,2	37,3	52,6	8,9
Creio que denunciar o cibercrime é uma perda de tempo.	0,2	10,9	37,0	51,9
A Polícia não tem meios para combater o cibercrime de forma eficaz.	16,3	65,2	15,3	3,2
Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.	42,2	46,7	9,6	1,5
Penso que a informação do Governo e da Polícia em relação ao cibercrime não tem importância para as organizações.	0,7	18,8	47,2	33,3
Penso que a Polícia está demasiado ocupada para se preocupar com o cibercrime.	1,2	39,8	50,6	8,4
Receio que, se denunciar um ciberataque à Polícia, isso vá prejudicar a reputação da própria instituição.	0,5	15,3	46,9	37,3
Penso que deve ser feito mais para comunicar os riscos do cibercrime às pessoas na instituição.*	0,2	1,5	55,3	43,0
Estou a par da política de uso informático da instituição, e tento segui-la.*	1,0	41,5	51,4	6,2
Se ocorrer um ciberataque, não saberei como denunciá-lo.	1,7	22,0	68,9	7,4
Não acho que é da minha responsabilidade denunciar um ciberataque contra a instituição.	0,7	0,5	51,1	47,7
Não presto atenção à informação disponibilizada pela instituição sobre as ameaças de cibercrime.	1,0	15,1	48,9	35,1
Confio na minha capacidade de reconhecer sinais de um ciberataque.*	11,6	35,6	48,9	4,0
Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da instituição.*	14,3	61,5	20,7	3,5
Sinto que qualquer pessoa na instituição está em risco de manipulação por ciber "vigaristas e burlões".*	0,7	12,3	81,7	5,2
Penso que os cibercriminosos apenas atingem uma instituição quando têm muito a ganhar do ponto de vista financeiro.	2,0	40,5	49,9	7,7
Penso que apenas as grandes empresas e organizações são atingidas por hackers e cibercriminosos.	0,5	13,8	44,7	41,0
Penso que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque.	1,0	15,1	44,2	39,8
Não sei quem é responsável por proteger a instituição do cibercrime.	15,6	61,7	18,3	4,4

Legenda: 1 - Concordo totalmente 2 - Concordo – 3 – Discordo 4 - Discordo totalmente
* questões com cotação inversa

Assim, tendo em conta aquilo que são os resultados da Tabela 3, é nos possível constatar que, cerca de 81,5% (somatório das respostas "Concordo" e "Concordo totalmente") dos polícias, acreditam que a Polícia, enquanto instituição, não tem meios de combate ao cibercrime. Assim, revela-se um certo desconhecimento, quer em relação às funções do Núcleo de Cibercriminalidade, quer às entidades que auxiliam na segurança das TIC institucionais, como é o caso da rede de segurança RNSI. No seguimento, cerca de 16% dos polícias, revelam falta de atenção perante informação institucional de sensibilização para a cibersegurança. Estes números tornam-se ainda mais alarmantes quando comparados com o facto de que, no somatório, 47,2% responderam "Discordo" e "Discordo totalmente" à questão "Confio na minha capacidade de reconhecer sinais de um ciberataque.", para além de que, no somatório, 55,1% dos polícias sentem dificuldade em perceber como proteger a instituição, revelando um conhecimento precário nestas matérias.

Ao mesmo tempo, 75,8% dos inquiridos acredita que as maiores ameaças ao ciberespaço da Polícia vêm do exterior da própria instituição, sendo que, através do relatório *Human Factor Report* (Proofpoint, 2019), é-nos possível constatar que a maior parte dos cibercrimes a nível mundial, acontecem por descuido ou falta de conhecimento, evidenciando o fator humano para a efetivação da ameaça.

Ademais, através da supramencionada tabela descritiva, constata-se que, grande parte dos polícias, atribuem um senso de responsabilidade, no âmbito da cibersegurança, à própria instituição, uma vez que, no somatório, 98,8% concordou ou concordou totalmente, que a responsabilidade de proteção contra cibercrimes é da organização. Estes dados alinham-se com as conclusões de Tischer et al. (2016) e Hadlington (2017), onde referem que os profissionais de uma organização, uma vez que chegam ao serviço, "transferem" a responsabilidade de cibersegurança à administração da determinada instituição. Para Hadlington e Parsons (2017), esta atitude pode provocar ainda mais preocupação, dado que esses profissionais, acreditando estarem protegidos pela organização, podem envolver-se em mais comportamentos de risco, neste contexto.

Com efeito, a última afirmação da escala "Atitudes em relação à Cibersegurança" vem, fundamentalmente, ao encontro desta matéria das responsabilidades de proteção da instituição. Deste modo, 77,3% dos polícias desconhece em quem recai a responsabilidade da proteção da instituição face ao cibercrime. Assim, configura-se um panorama alarmante para a prevenção destes crimes, visto ser da responsabilidade de cada um, possuir o

mínimo de conhecimento securitário nesta área, uma vez que o CNCS (2022) explana que a responsabilidade pela cibersegurança não recai na tecnologia, mas sim nas pessoas.

Posto isto, as estatísticas descritivas dos valores obtidos nas escalas "Comportamentos Arriscados em Cibersegurança" e "Atitudes em relação à Cibersegurança" podem ser apreciadas na tabela seguinte. Nela, indicamos os valores mínimos e máximos, média e respetivos desvios padrão.

Tabela 4

Estatísticas descritivas

	Mínimo	Máximo	Média	Desvio padrão
Comportamentos Arriscados em Cibersegurança	0	96	41,41	24,231
Atitudes em relação à Cibersegurança	47	96	73,30	11,131

Recorreu-se à análise do coeficiente de consistência interna *Alfa de Cronbach* (α), por forma a analisar a consistência interna das escalas "Comportamentos Arriscados em Cibersegurança" e "Atitudes em relação à Cibersegurança", verificando-se 0,941 e 0,936, respetivamente. Estes valores do *Alfa de Cronbach* demonstram uma excelente consistência interna (Hill & Hill, 2008; Pestana & Gageiro, 2014).

Tabela 5

Consistência interna (Alpha de Cronbach)

	Alpha Cronbach	N.º de itens
Comportamentos Arriscados em Cibersegurança	.941	20
Atitudes em relação à Cibersegurança	.936	25

5.2. Análise Estatística Inferencial

A correlação entre os "Comportamentos Arriscados em Cibersegurança" e as "Atitudes em relação à Cibersegurança" é, como se apresenta na Tabela 6, estatisticamente significativa, negativa e elevada ($r = -.793$, $p < .001$). Ora, sendo o coeficiente negativo, então, à medida que diminuem as "Atitudes em relação à Cibersegurança", os "Comportamentos Arriscados em Cibersegurança" aumentam, reduzindo, assim, a

consciencialização em segurança no ciberespaço. Isto é, pode concluir-se que, uma pontuação elevada de cada indivíduo, na escala das "Atitudes em relação à Cibersegurança", traduzir-se-á numa pontuação reduzida na escala "Comportamentos Arriscados em Cibersegurança", significando, portanto, que quanto mais adequadas forem as atitudes nesta área, menos riscos estarão associados aos seus comportamentos (Hadlington, 2018).

Tabela 6

Coeficiente de Correlação de Pearson

	Atitudes em relação à Cibersegurança
Comportamentos Arriscados em Cibersegurança	-.793***

* $p \leq .05$ ** $p \leq .01$ *** $p \leq .001$

Relembrando, a primeira hipótese de investigação da presente dissertação consubstanciou-se no seguinte:

H1: As atitudes dos polícias do COMETLIS em relação à cibersegurança são corretas e adequadas no âmbito das suas funções.

Efetivamente, analisando os resultados da escala "Atitudes em relação à Cibersegurança" (questões 26 a 50 do Questionário, Apêndice D), e tendo em conta o ponto médio da mesma, de 62,5 pontos, uma vez que esta escala pode variar a sua pontuação entre os 25 e os 100 pontos, obteve-se a média dos valores obtidos pelos polícias do COMETLIS de 73,29 pontos (*Cfr*. Tabela 7). Portanto, tendo em consideração o Teorema do Limite Central, que indica que nas amostras com dimensão superior a 30 (n>30), podemos pressupor a normalidade de distribuição das variáveis dependentes quantitativas, foi aplicado o teste T de *Student* para a amostra em questão.

Comparando com o ponto médio da escala (62,5 pontos), constamos que a diferença é estatisticamente significativa, uma vez que t (404) = 19,523, $p < 0{,}001$, tendo os polícias do COMETLIS obtido cerca de 10,79 pontos a mais que o ponto médio da escala (*Cfr*. Tabela 8).

Deste modo, segundo Hadlington (2018), "uma pontuação elevada na escala (…) indica um envolvimento e uma sensibilização positiva para a cibersegurança, enquanto

uma pontuação mais baixa indica um envolvimento mais fraco e uma consciência mais limitada[28]" (p. 273). Assim, tendo em consideração a pontuação média obtida, podemos considerar que as atitudes dos polícias do COMETLIS em relação à cibersegurança são, tendencialmente, corretas/adequadas, corroborando, desta forma, a **H1**, $p<0{,}001$.

Tabela 7

Atitudes em relação à cibersegurança – Estatística da amostra

	Média	Desvio padrão
Atitudes em relação à Cibersegurança	73,29	11,13

Tabela 8

Teste T de Student para uma amostra

	Valor do Teste = 62,5			
	t	df	Sig.	Diferença da Média
Atitudes	19,523	404	0,000***	10,79877

* $p \leq .05$ ** $p \leq .01$ *** $p \leq .001$

Não obstante a média das respostas obtidas ser positiva num ponto de vista macro, é necessário, também, atentar alguns fatores menos positivos, que possam ser indicadores de uma má conduta atitudinal securitária dentro da organização, como versado anteriormente na análise da estatística descritiva, da Tabela 3.

De seguida, recorda-se a segunda hipótese de investigação:

H2a: Existem diferenças significativas de comportamentos de cibersegurança e ciber-higiene entre as faixas etárias dos polícias do COMETLIS.

Posto isto, são comparados os valores obtidos das questões da escala "Comportamentos Arriscados em Cibersegurança" (Questões 6 à 25 do Questionário, Apêndice D), em função das faixas etárias dos polícias do COMETLIS, por forma a encontrar-se diferenças estatisticamente significativas, ou não.

Neste sentido, recorreu-se ao teste *Kruskal-Wallis*, uma vez que, para esta hipótese, foi verificada a distribuição, tendo esta diferido da normal. Foram realizados os testes de

[28] Traduzido.

normalidade *Kolmogorov-Smirnov* e *Shapiro-Wilk*, dada a existência de uma variável com menos de 50 participantes (n<50), especificamente, a variável da faixa etária "Mais de 55 anos" (Tabela 17 e 18, Apêndice I).

Foi possível, então, obter χ^2_{KW} (4) = 30,851, p < 0,001 (*Cfr*. Tabela 9). Verificando-se, desta forma, que os polícias do COMETLIS com mais de 55 anos, obtiveram valores significativamente mais baixos do que as restantes faixas etárias, corroborando, então, a veracidade da **H2a**, significando, ainda, que esta faixa etária tem comportamentos menos arriscados que as restantes.

Tabela 9

Teste Kruskal-Wallis – Faixas Étarias (RScB)

	Comportamentos
Kruskal-Wallis	30,851
df	4
Sig.	0,000***

* $p \leq .05$ ** $p \leq .01$ *** $p \leq .001$

Hadlington (2018), esclarece que quanto menor a pontuação obtida na escala RScB, correspondente aos comportamentos arriscados, por parte dos polícias, menor o risco que estes correm no ciberespaço. Ora, tendo isto em apreço e considerando a Tabela 10 que se segue, é de realçar a faixa etária mais elevada (Mais de 55 anos) como aquela que menor risco corre, comparando com as restantes. Por outro lado, a que mais se expõe ao risco é a faixa etária dos polícias entre os 36 e 45 anos (Figura 7, Apêndice J). A faixa etária mais jovem (Entre 18 e 25 anos), obteve um valor de 40,16 pontos, traduzindo-se em maiores riscos associados aos seus comportamentos no ciberespaço, quando comparado com a faixa etária mais antiga (Mais 55 anos). Ora, note-se que, a partir destes resultados, pode existir uma relação linear entre a faixa etária e a consciencialização para a cibersegurança, com a faixa etária mais velha a demonstrar mais consciência neste âmbito (McCormac et al., 2017 as cited in Hadlington, 2018).

Tal, de acordo com Reyna e Farley (2006), pode ser explicado por inúmeras razões, sendo, a razão fundamental, relacionada com os aspetos de aversão ao risco. Portanto, segundo os mencionados autores, indivíduos mais jovens, são, geralmente, menos adversos

ao risco, o que, consequentemente, faz com que esses indivíduos se envolvam em comportamentos de risco com mais frequência.

Tabela 10

Médias e DP – RScB e ATC-P – Faixas Etárias

	18-25		26-35		36-45		46-55		> 55		
	M	DP	M	DP	M	DP	M	DP	M	DP	Sig.
Comp. Arriscados em Cibersegurança	40,16	21,59	37,06	19,37	46,98	24,94	43,77	26,94	20,05	19,01	.001***
Atitudes em relação à Cibersegurança	76,71	10,40	76,20	9,39	70,76	11,82	70,86	11,28	75,71	9,58	.001***

Legenda: M – Média DP – Desvio padrão * $p \leq .05$ ** $p \leq .01$ *** $p \leq .001$

Findada esta análise, a investigação segue com a aceitação ou rejeição da hipótese subsequente:

H2b: Existem diferenças significativas de comportamentos de cibersegurança e ciber-higiene nas diferentes carreiras dos polícias do COMETLIS.

Realizado novamente o teste *Kolmogorov*-Smirnov para aferir a distribuição, chegou-se à conclusão de que o teste a utilizar seria o *Kruskal-Wallis*, em razão da distribuição diferir da normal. No que diz respeito às diferenças nos valores obtidos para a mesma escala de comportamentos (RScB), não se verificaram diferenças estatisticamente significativas ($p > 0,05$), em função das carreiras dos polícias do COMETLIS inquiridos, como se apresenta na Tabela 11.

Tabela 11

Teste Kruskal-Wallis – Carreiras Policiais (RScB)

	Comportamentos
Kruskal-Wallis	0,696
df	2
Sig.	0,706

Tendo em conta que $p > 0,05$, possibilita a rejeição da **H2b**, uma vez que as carreiras policiais dos inquiridos não encontram diferenças significativas nas suas respostas, como se apresenta na tabela 12. Desta forma, não se constata a existência de carreiras mais ou menos preparadas, no que diz respeito aos seus comportamentos de ciber-higiene na instituição.

Tabela 12

Médias e DP – RScB e ATC-P – Faixas Etárias – Carreiras policiais

	Agente de Polícia		Chefe de Polícia		Oficial de Polícia		
	M	DP	M	DP	M	DP	Sig.
Comportamentos Arriscados em Cibersegurança	42,11	25,43	39,93	22,65	40,93	21,59	.706
Atitudes em relação à Cibersegurança	73,11	11,62	73,89	10,60	73,09	9,89	.762

M – Média DP – Desvio padrão

Importa ainda realçar que, tendo-se obtido uma média de 41,41 pontos nas respostas dos polícias inquiridos para a escala "Comportamentos Arriscados em Cibersegurança", e o ponto médio da escala ser 60 pontos, é possível afirmar que os comportamentos arriscados dos polícias do COMETLIS, ficaram abaixo desse valor. Indicando um fator positivo, uma vez que, quanto maior a pontuação, maior o envolvimento em comportamentos arriscados em cibersegurança.

Contudo, a Tabela 2 apresenta alguns itens que revelam fatores de preocupação, respeitantes aos comportamentos preventivos de cibersegurança e ciber-higiene dos polícias inquiridos, como explicitado na análise da estatística descritiva realizada anteriormente.

Por fim, como última hipótese de investigação segue-se a seguinte afirmação:

H3: Os polícias do COMETLIS consideram útil um *Quick reference guide* de cibersegurança implementado na PSP.

Para tal, analisaram-se as duas últimas questões do questionário (Questão 52 e 53 do Questionário, Apêndice D), recorrendo ao teste Binomial. Este teste contemplou dois

grupos, um referente às respostas “Concordo totalmente” e “Concordo”, e o outro referente às respostas “Discordo totalmente” e “Discordo”.

Ora, relativamente à utilidade de um *Quick Reference Guide* de cibersegurança implementado na PSP, denotou-se que a proporção de polícias do COMETLIS que o consideram útil (99%), é significativamente superior à proporção de polícias do COMETLIS que consideram o oposto, tendo-se efetuado o teste Binomial, onde $p < 0{,}001$, representado na seguinte tabela.

Tabela 13

Teste Binomial – Viabilidade de um Quick Reference Guide na PSP

		Categoria	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
Q52	Grupo 1	Concordo	401	0,99	0,01	0,000
	Grupo 2	Discordo	4	0,01		
	Total		405	1,00		

Ao mesmo tempo que a proporção de polícias do COMETLIS que utilizaria um *Quick Reference Guide* na sua área de trabalho (95%) é significativamente superior à proporção de polícias do COMETLIS que não utilizariam (5%), pelo que, ao abrigo do teste Binomial, foi possível chegar, mais uma vez, a um *p-value* significativo, $p < .001$, comprovando a veracidade da **H3** (Tabela 14).

Tabela 14

Teste Binomial – Utilidade de um Quick Reference Guide na PSP

		Categoria	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
Q53	Grupo 1	Concordo	385	0,951	0,049	0,000
	Grupo 2	Discordo	20	0,049		
	Total		405	1,00		

Capítulo VI - Conclusão

É irrefutável que, diariamente, o mundo digital é alvo de ameaças constantes. Pelo que, o presente estudo propõe uma análise das hipóteses de investigação e dos objetivos concebidos, enquanto resposta primeira do trabalho em evidência.

Portanto, o segundo capítulo da presente dissertação, possibilitou uma abrangência conceitual daquilo que é a cibersegurança e dos seus conceitos análogos, bem como do atual panorama nacional e internacional do cibercrime e os seus principais dados estatísticos.

No terceiro capítulo, apurou-se o envolvimento da Polícia de Segurança Pública em matérias de cibersegurança, tendo-se constatado que esta polícia tem vindo a crescer nesta matéria, fundamentalmente, com a criação de um núcleo especializado no cibercrime. Contudo, no que diz respeito à prevenção do seu próprio efetivo no ciberespaço, carece ainda de ferramentas capazes de adequar os mesmos às ameaças e incidentes a que estão sujeitos no seu quotidiano. No mesmo sentido, neste capítulo abordou-se a problemática do fator humano da cibersegurança, tendo-se verificado que este fator é fulcral para uma boa capacidade securitária organizacional. Concluiu-se que, hodiernamente, uma segurança eficaz e que perdura, não se baseia apenas em soluções tecnológicas, mas também no nível de consciencialização para a cibersegurança e dos comportamentos dos indivíduos na utilização dos sistemas.

Seguidamente, recorrendo à utilização de testes estatísticos, foi possível analisar e apresentar os resultados apurados, relativamente às respostas do inquérito por questionário. Com efeito, estas ferramentas estatísticas, possibilitaram a verificação da veracidade ou rejeição das hipóteses formuladas, anteriormente, na investigação.

No mesmo sentido, constatou-se a veracidade da primeira hipótese do presente estudo (**H1**), onde se afirmava que as atitudes dos polícias do COMETLIS eram adequadas e corretas, no âmbito da cibersegurança. Através do recurso aos testes estatísticos, concluiu-se que a pontuação dos inquiridos em relação às atitudes de cibersegurança e ciber-higiene eram, no geral e em média, positivas, uma vez que eram significativamente superiores ao ponto médio da pontuação da escala estabelecida. Não obstante à média positiva de atitudes dos polícias em relação à cibersegurança, apurou-se, através dos resultados obtidos, alguns pontos alarmantes e que colocam em causa o bom funcionamento dos sistemas informáticos e a segurança, tanto da instituição, como

individual. Nesta linha de pensamento, resulta, dos testes realizados, que a maior parte dos inquiridos expressam não saber proteger a instituição nesta matéria, bem como atribuem essa responsabilidade para a própria administração da organização. Ora, com base na revisão da literatura, é possível afirmar que a responsabilidade em manter a instituição segura é de todos, dada a especificidade das funções policiais e o constante recurso à tecnologia.

Posto isto, apraz-nos referir que uma mudança de atitude no respeitante às responsabilidades, é, fundamentalmente, benéfico à segurança de todos no ciberespaço. Ademais, uma mudança de atitude é crucial, não só nos papéis individuais de cada um, mas também nos papéis desempenhados dentro das organizações, enfatizando, desta forma, a especial necessidade de nos educarmos continuamente e de nos protegermos.

No que diz respeito à hipótese seguinte, a **H2a**, note-se que foi possível, também, a sua corroboração. Esta hipótese defendia que os comportamentos arriscados em cibersegurança e ciber-higiene divergiam em função da faixa etária do polícia inquirido. Assim, verificou-se diferenças significativas entre faixas etárias, sendo, a faixa etária dos polícias com mais idade, aquela que menos se envolve em comportamentos arriscados, comparativamente com as restantes. Em média, os polícias com idades compreendidas entre os 18 e 25 anos, ora, os inquiridos mais jovens, obtiveram uma avaliação de 40,16 pontos, mais 20,11 pontos que os anteriores. Estes dados traduzem-se numa consciencialização para a cibersegurança mais ponderada para os mais velhos, ao passo que uma das razões diz respeito à adversidade ao risco que os mais jovens demonstram nestas matérias.

Os resultados inerentes aos comportamentos arriscados em cibersegurança constataram, assim como as atitudes, de acordo com a escala estabelecida, uma média positiva. Contudo, à semelhança dos resultados obtidos relativos às atitudes em cibersegurança, também nestes, existem pontos que requerem a devida atenção, uma vez que são indicadores de má conduta ou negligência informática, podendo comprometer a instituição em que estão inseridos. Assim, denote-se que cerca de 45% dos polícias utilizam a mesma *password* para diversos *websites*, bem como grande parte dos inquiridos guarda automaticamente os dados de acesso ao *email* e a outros *websites* e admitem nunca terminar a sessão do seu *email*, ora, consubstancia-se, isto, em comportamentos arriscados, colocando a segurança da sua própria informação em causa, e, consequentemente a da

instituição. Estes comportamentos, apesar de individualizados, demostram um nível reduzido de consciencialização destes polícias nas questões supramencionadas, uma vez que possibilitam uma maior exposição a ameaças, e, em último caso, a constituírem-se como vítimas de um ciberataque.

Na mesma linha de pensamento da hipótese anterior, para a **H2b**, visou-se constatar se a carreira atual de cada polícia do COMETLIS inquirido influenciava o comportamento que este tinha, em relação à cibersegurança e ciber-higiene. Através dos testes estatísticos realizados foi possível rejeitar a **H2b**, uma vez que as diferentes carreiras policiais não demonstraram diferenças significativas para os seus comportamentos. Conclui-se, portanto, que não se constatam carreiras policiais mais preparadas que outras, no que concerne aos comportamentos que os polícias dessas carreiras adotam relativamente à cibersegurança.

Por fim, corroborou-se a **H3**, que procurava verificar a utilidade, para os polícias, de um *Quick Reference Guide* de cibersegurança na PSP. Ora, com a formulação desta hipótese, visou-se ir mais além da análise dos comportamentos e atitudes dos polícias, sendo elaborado uma proposta de um exemplo de um manual breve de ciber-higiene que propõe auxiliar os polícias com recomendações básicas e cruciais para manter um funcionamento normal e seguro dos sistemas e dispositivos do seu local de trabalho. Atendendo à grande proporção de polícias inquiridos que responderam considerar ser viável e que utilizariam o manual, conclui-se que, apesar das boas atitudes e comportamentos (na generalidade) demonstrados anteriormente, um auxílio de um *Quick Reference Guide* pode vir a minimizar ainda mais os riscos inerentes à utilização do ciberespaço, por parte dos mesmos.

Relativamente ao objetivo específico relacionado com a noção de importância da cibersegurança, bem como o cumprimento das normas básicas de proteção, foi-nos possível, através dos valores obtidos tanto para as questões relativas à escala "Comportamentos arriscados em cibersegurança", assim como para as questões da escala "Atitudes em relação à cibersegurança", avaliar o mesmo. Assim, no caso, podemos concluir que os polícias do COMETLIS, em média, são cumpridores dessas mesmas normas e as suas atitudes adequam-se, tendo, por isso, noção da relevância desta matéria.

No que diz respeito ao objetivo específico referente à utilidade e viabilidade do *Quick Refernce Guide*, como constatado anteriormente, é notória a perceção dos polícias

inquiridos ao afirmarem, quase unanimemente, a utilidade do mesmo na sua área de trabalho, como forma de auxílio adicional de segurança.

O último objetivo específico, relativo ao interesse da incorporação de formação específica de cibersegurança nos cursos de formação da PSP (consciencializando-os das vulnerabilidades a que estão expostos no ciberespaço), é cumprido, uma vez que, como explanado no terceiro capítulo da presente dissertação, a Polícia de Segurança Pública carece deste tipo de formação de cariz preventivo. Ora, através do trabalho realizado ao longo do estudo, foi-nos possível concluir que a capacidade de incutir um senso de bom comportamento e de se exponenciar uma consciencialização em matéria de cibersegurança, deve ser considerada de importância primordial para todas as organizações, através, fundamentalmente, da formação e educação.

É crucial que a educação e formação em matérias de cibersegurança vá além da mera prestação de informações aos profissionais de polícia numa fase embrionária das suas vidas policiais. De modo a contornar esta situação, sugere-se que a informação deva ser direcionada e relevante, e que deve ser fornecida de forma mais frequente, de maneira contínua, uma vez que a evolução da tecnologia não estagna e que novas formas de crime nascem de dia para dia.

Finalmente, mediante todas as conclusões apresentadas, podemos, uma última vez, concluir que tanto o objetivo geral, como a pergunta de investigação, foram cumpridos com sucesso. Deste modo, verificou-se que a consciencialização que os polícias alvo do estudo em apreço apresentam, relativamente à cibersegurança, nomeadamente na sua proteção, é, de facto, positiva. Contudo, é sabido que a tecnologia não vê a sua evolução a abrandar, ao passo que é indispensável focalizar as atenções nesta direção, mantendo o nível de consciência elevado, melhorando-o cada vez mais, por forma a mitigar, ao máximo, os riscos.

6.1. Limitações e Recomendações

Apesar de alcançar e cumprir os objetivos propostos, o presente estudo apresenta como limitação, desde logo, a escassez bibliografia relativamente ao assunto abordado em contexto policial. Efetivamente, não foi possível aferir, quer no panorama nacional, quer no panorama internacional, investigações que estudassem a consciencialização para a

cibersegurança e ciber-higiene dos polícias. Por outro lado, esta limitação valoriza este trabalho, sendo que os respetivos resultados serão uma mais-valia significativa para a PSP.

Para futuras investigações, propõe-se um aprofundamento da potencialidade e respetiva implementação de um *Quick Refernce Guide* de cibersegurança, semelhante àquele que foi concebido neste estudo, de modo a materializar esta ideia e a dotar os quadros da Polícia de Segurança Pública de profissionais mais capazes e mais protegidos no ciberespaço.

"*Deeds will not be less valiant because they are unpraised.*"

- Aragorn *in* "*LOTR*", J.R.R. Tolkien

Referências Bibliográficas

Adamopoulou, E., & Moussiades, L. (2020). An Overview of Chatbot Technology. Em I. Maglogiannis, L. Iliadis, & E. Pimenidis (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 584, pp. 373–383). Springer International Publishing. https://doi.org/10.1007/978-3-030-49186-4_31

Agoga, F. (2001). *As Novas Tecnologias no Instituto Superior de Ciêncieas Policiais e Segurança Interna*. ISCPSI.

Agrawal, M., Singh, H., Gour, N., & Kumar, M. A. (2014). *Evaluation on Malware Analysis*. *5*.

Alexandrou, A. (2021). *Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*. CRC Press.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). *Information security culture: A behaviour compliance conceptual framework*. *105*. https://doi.org/10.5555/1862266.1862275

Aparício, M. (2017). *O Ciberespaço como Dimensão de Segurança* [Dissertação de Mestrado, Academia da Força Aérea]. http://hdl.handle.net/10400.26/23108

APAV. (2019). *Https://apav.pt/apav_v3/index.php/pt/2039-diario-de-noticias-revenge-porn-quando-as-imagens-intimas-acabam-a-vista-de-todos*. Associação Portuguesa de Apoio à Vítima. https://apav.pt/apav_v3/index.php/pt/2039-diario-de-noticias-revenge-porn-quando-as-imagens-intimas-acabam-a-vista-de-todos

APAV. (2024). *Cibercrime*. https://apav.pt/cibercrime/

Arruda, J. P. (2021). Hackers, Hacktivistas e Whistleblowers: O caso português. *Perspectivas em Ciência da Informação*, *26*(2), 15–36. https://doi.org/10.1590/1981-5344/3869

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

Azevedo, M. (2023). *Utilização de Tecnologias Móveis e o Respetivo Potencial Operacional: Perceção dos Polícias das Esquadras Territoriais da Divisão Policiail de Cascais do COMETLIS* [Dissertação de Mestrado, ISCPSI]. http://hdl.handle.net/10400.26/45768

Baptista, I. (2017). *O Fator Humano na Cibersegurança* [Dissertação de Mestrado, Instituto Superior Técnico]. https://fenix.tecnico.ulisboa.pt/cursos/msidc/dissertacao/1409728525632070

Barrinha, A. (2020). Cibersegurança e ciberdefesa em tempos de pandemia. *IDN Brief*, 2–10.

Beck, U. (1992). *Risk Society: Towards a New Modernity* (Vol. 17). SAGE Publications.

Bell, D., Loader, B., Pleace, N., & Schuler, D. (2004). *Cyberculture: The Key Concepts* (1.ª ed.). Routledge.

Brown, C. S. D. (2015). *Investigating And Prosecuting Cyber Crime: Forensic Dependencies And Barriers To Justice*. *9*, 55–119. https://doi.org/10.5281/ZENODO.22387

Campenhoudt, L. V., Marquet, J., & Quivy, R. (2019). *Manual de Investigação em Ciências Sociais*. Gradiva.

Castells, M. (2004). *A Galáxia Internet—Reflexões sobre Internet, Negócios e Sociedade*. Fundação Calouste Gulbenkian.

Castells, M. (2007). *A Era da Informação: Economia, Sociedade e Cultura—A Sociedade em Rede* (Vol. 1). Fundação Calouste Gulbenkian.

Cavelty, M. D. (2010). Cyber-Security. Em *The Routledge Handbook of New Security Studies* (1.ª ed., p. 328). Routledge.

Centro Nacional de Cibersegurança. (2020). *Cibersegurança em Portugal: Riscos e Conflitos* (p. 103). Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2020-observatoriocibersegurancа-cncs.pdf

Centro Nacional de Cibersegurança. (2021). *CNCS - Sobre Nós*. Obtido 22 de novembro de 2023, de https://www.cncs.gov.pt/pt/sobre-nos/#oquee

Centro Nacional de Cibersegurança. (2022). *Ciber-higiene e boas práticas de cibersegurança*. Conteúdo de sensibilização em ciber-higiene. https://www.cncs.gov.pt/docs/2ciberhig.pdf

Centro Nacional de Cibersegurança. (2023a). *Relatório Cibersegurança em Portugal: Riscos & Conflitos*. Observatório de Cibersegurança.

Centro Nacional de Cibersegurança. (2023b). *Relatório Cibersegurança em Portugal* (5; Sociedade 2023). https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

CERT. (2013). Unintentional Insider Threats: A Foundational Study. *Software Engineering Institute*. https://insights.sei.cmu.edu/documents/2255/2013_004_001_58748.pdf

CERT. (2014). Unintentional Insider Threats: Social Engineering. *Software Engineering Institute*. https://apps.dtic.mil/sti/tr/pdf/ADA592507.pdf

Chaudhry, J., & Rittenhouse, R. (2015). *Phishing: Classification and Countermeasures*. 28–31. https://doi.org/10.1109/MulGraB.2015.17

Chawki, M. (2006). *Essai sur la notion de cybercriminalité*. 36.

Check Point Research. (2023). *Cyber Security Report* (p. 108). CPR. https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/2023-cyber-security-report.pdf

CIS Controls. (2015). *Critical Security Controls for Effective Cyber Defense V6*. Center for Internet Security. http:// www.cisecurity.org

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, *37*(4), 671–680. https://doi.org/10.1080/03050718.2011.621277

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*, 13–21. https://doi.org/10.22215/timreview/835

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach* (5.ª ed.). SAGE Publications.

CSIRT.MAI. (2024a). *Missão | CSIRT.MAI*. https://www.csirt.rnsi.mai.gov.pt/

CSIRT.MAI. (2024b). *Boas práticas de Segurança | CSIRT.MAI*. https://www.csirt.rnsi.mai.gov.pt/content/boas-pr%C3%A1ticas-de-seguran%C3%A7a

Decreto-Lei n.º 136/2017, de 6 de novembro. *Diário da República n.º 213/2017, Série I*. 5874-5881.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590. https://doi.org/10.1145/1124772.1124861

Digital 2023: Global Overview Report. (2023, janeiro 26). DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-global-overview-report

Dobbins, J., Solomon, R. H., Chase, M. S., Henry, R., Larrabee, F. S., Lempert, R. J., Liepman, A. M., Martini, J., Ochmanek, D., & Shatz, H. J. (2015). *Choices for America in a Turbulent World: Strategic Rethink*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1114.html.

Domingues, E. J. (2015). *Os Ciberataques como um Novo Desafio para a Segurança: O Hacktivismo* [Dissertação de Mestrado, ISCPSI]. http://hdl.handle.net/10400.26/15403

Elias, L. (2018). *Ciências Policiais e Segurança Interna: Desafios e prospetivas*. ISCPSI.

Elias, L. (2019). *Ciberameaças e (In)Segurança*. *1*(7), 61–95.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, *14*(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002

Engelbrecht, H., Lukosch, S. G., & Datcu, D. (2019). Evaluating the Impact of Technology Assisted Hotspot Policing on Situational Awareness and Task-Load. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *3*(9), 1–18. https://doi.org/10.1145/3314396

European Union Agency for Cybersecurity. (2017). *Cyber security culture in organisations.* Publications Office. https://data.europa.eu/doi/10.2824/10543

European Union Agency for Cybersecurity. (2023). *Awareness Raising* [Topic]. ENISA. https://www.enisa.europa.eu/topics/cybersecurity-education

European Union Agency for Cybersecurity. (2016). *Review of cyber hygiene practices.* Publications Office. https://data.europa.eu/doi/10.2824/352617

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023: July 2022 to June 2023.* Publications Office. https://data.europa.eu/doi/10.2824/782573

European Union Agency for Network and Information Security. (2017). *Cyber security culture in organisations.* Publications Office. https://data.europa.eu/doi/10.2824/10543

Fávero, L., & Belfiore, P. (2017). *Manual de análise de dados: Estatística e modelagem multivariada com excel, spss e stata.* Elsevier Brasil.

Felgueiras, S. (2011). Police Learning Strategies. Em B. Akhgar & S. Yates (Eds.), *Intelligence Management* (pp. 213–223). Springer London. https://doi.org/10.1007/978-1-4471-2140-4_14

Fernandes, J. (2012). Utopia, liberdade e soberania no ciberespaço. *IDN - Revista Nação e Defesa*, *133*, 11–31.

Ferreira, F., & Moreira, A. (2014). *A Formação em eLearning e bLearning na Polícia de Segurança Pública em Portugal: Retrato, Percurso e Perspetivas* (1ª ed.). WhiteBooks.

Ferreira, S. (2017). *Sistemas de Informação em Segurança*. Editora e Distribuidora Educacional.

Filho, A. C. G. (2008). *Importance of Hardware and Software in Organizations Dealing with e-Government*. *6*.

Fischer, E. (2010). *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. BiblioGov.

Fortin, M.-F. (2000). *O Processo de Investigação: Da Concepção à Realização*. Lusodidacta.

Freire, V., & Caldas, A. (2013). O Ciberespaço: Desafios à Segurança e à Estratégia. Em *Atena n.º 30* (pp. 81–150). Instituo da Defesa Nacional.

Furnell, S., & Clarke, N. (2005). *Organisational Security Culture: Embedding Security Awareness, Education and Training*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5aba1d63509984b92dce7be2388ffc0319f851ad

Gabrosky, P. (2017). The Evolution of Cybercrime, 2006-2016. *Cybercrime through an Interdisciplinary Lens*, 15–36.

Gibson, W. (1984). *Neuromancer* (Vol. 1). Ace.

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social* (6.ª ed.). Atlas.

Gleitman, H., Gross, J. J., & Reisberg, D. (2011). *Psychology* (8th ed). W. W. Norton & Co.

Gomes, P. J. V. (2013). *Estratégia para as Tecnologias de Informação e Comunicação na PSP 2013-2016*. https://www.psp.pt/Documentos%20Varios/Estrat%C3%A9gia%20TIC%20PSP%202013-2016.pdf

Goodwin, D. (1994). *Designing a Quick Refernce Guide: A Teaching Case*. *24*(3). https://doi.org/10.2190/JCYC-ELUU-9U9N-Q0KL

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). *Employees Attitude Towards Cyber Security And Risky Online Behaviours: An Empirical Assessment In The United Kingdom*. https://doi.org/10.5281/ZENODO.1467909

Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

Hill, M. M., & Hill, A. (2008). *Investigação por Questionário* (2.ª ed.). Edições Sílabo.

HIMSS. (2020). *HIMSS*. https://www.himss.org/resources/cybersecurity-healthcare

ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE, & ISACA Belgium. (2014). *Belgian Cyber Security Guide* (Protect your information).

IDN-CESEDEN. (2013). *Estratégia da informação e segurança no ciberespaço* (12.ª ed.). Instituto da Defesa Nacional; IDN-Cadernos. http://hdl.handle.net/10400.26/7757

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cyber crime Classification and Characteristics. Em *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149–164). Elsevier Science. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Jebb, A. T., Ng, V., & Tay, L. (2021). A Review of Key Likert Scale Development Advances: 1995–2019. *Frontiers in Psychology*, *12*, 637547. https://doi.org/10.3389/fpsyg.2021.637547

Jerónimo, S. F. G. (2017). *A importância da Intranet enquanto meio de Comunicação Interna—A Intranet na Câmara Municipal de Cascais* [Dissertação de Mestrado, Instituto Superior de Novas Profissões]. http://hdl.handle.net/10400.26/34163

Jordan, T. (2017). A genealogy of hacking. *Convergence*, *23*(5), 528–544. https://doi.org/10.1177/1354856516640710

Keyser, M. (2009). The Council of Europe Convention on Cybercrime. Em *Computer Crime* (1.ª ed., p. 40). Routledge.

Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing*, *47*(6), 65–67. https://doi.org/10.1097/01.NURSE.0000516242.05454.b4

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1738223

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). *Managing Cyber Threats: Issues, Approaches, and Challenges*. Springer Science & Business Media.

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, *127*, 103096. https://doi.org/10.1016/j.cose.2023.103096

Lei n.º 46/2018, de 13 de agosto. *Diário da República n.º 155/2018 - Série I.* Portugal: Assembleia da República.

Lei n.º 49/2008, de 27 de agosto. *Diário da República n.º 165/2008, Série I*. Assembleia da República.

Lei n.º 67/98, de 26 de outubro. *Diário da República n.º 247/1998, Série I*. Assembleia da República.

Lei n.º 109/2009, de 15 de setembro. *Diário da República n.º 179/2009 - Série I.* Portugal: Assembleia da República.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

Maennel, K., Mäses, S., & Maennel, O. (2018). Cyber Hygiene: The Big Picture. Em N. Gruschka (Ed.), *Secure IT Systems* (Vol. 11252, pp. 291–305). Springer International Publishing. https://doi.org/10.1007/978-3-030-03638-6_18

Maia, C. (2019). *Ciberpoliciamento das redes sociais: O contributo das ciências tecnológicas* [Trabalho Individual Final, 3.º Curso de Comando e Direção Policial, ISCPSI]. http://hdl.handle.net/10400.26/34925

Maia, C. M. T. (2019). *Ciberpoliciamento das redes sociais: O contributo das ciências tecnológicas* [Report]. https://comum.rcaap.pt/handle/10400.26/34925

Mansfield-Devine, S. (2016). The death of defence in depth. *Computer Fraud & Security*, *2016*, 16–20. https://doi.org/10.1016/S1361-3723(15)30048-8

Marconi, M. de A., & Lakatos, E. M. (2017). *Fundamentos de Metedologia Científica* (7.ª ed.). Atlas.

Marôco, J. (2021). *Análise Estatística com o SPSS Statistics* (8.ª ed.). ReportNumber.

Maurício, M. (2006). *O Papel da Intranet na Gestão do Conhecimento Organizacional*. ISCTE.

Maybury, M. T. (2015). Toward Principles of Cyberspace Security. Em J.-L. Richet, *Cybersecurity Policies and Strategies for Cyberwarfare Prevention:* IGI Global. https://doi.org/10.4018/978-1-4666-8456-0

McLuhan, M. (1962). *The Gutenberg Galaxy: The Making of Typographic Man* (Vol. 39). University of Toronto Press.

McLuhan, M. (2000). *Os Meios de Comunicação como Extensões do Homem (understanding media)*. Cultrix.

Militão, O. P. (2014). *Guerra da Informação: A cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional* [Dissertação de Mestrado, Universidade Nova de Lisboa]. http://hdl.handle.net/10362/14300

Moita, P. (2024). *Tecnologias de Segurança—Cibersegurança*.

Moreira, J. (2012). *O Impacto do Ciberespaço como nova dimensão nos conflitos* [Curso de Promoção a Oficial Superior, Instituto de Estudos Superiores Militares]. http://hdl.handle.net/10400.26/12369

Mouradian, A. (2017). Employees are lax on cyber fundamentals. *Computer Fraud & Security*, *2017*(8), 17–18. https://doi.org/10.1016/S1361-3723(17)30073-8

Neto, P. L. (2002). *Estatísitca* (2.ª ed.). Edgard Blücher.

Nunes, P. (2019). *Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar* [Dissertação de Mestrado, Instituto Politécnico de Lisboa, Escola Superior de Tecnologia da Saúde de Lisboa]. http://hdl.handle.net/10400.21/12523

Nunes, P. F. V. (2012). *A Definição de uma Estratégia Nacional de Cibersegurança*. *133*, 113–127.

O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209. https://doi.org/10.1093/jcsl/krs017

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

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

PCI SSC. (2014). *Best Practices for Implementing a Security Awareness Program* (1.0).

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Pereira, S. (2022). *Cibersegurança: O Papel da Polícia de Segurança Pública na Prevenção do Cibercrime* [Dissertação de Mestrado, ISCPSI]. http://hdl.handle.net/10400.26/41482

Pestana, M. H., & Gageiro, J. N. (2014). *Análise de dados para ciências sociais: A complementaridade do SPSS* (6.ª ed.). Edições Sílabo.

Poiares, N. (2019a). A cibersegurança à luz da criminologia moderna. *Cyber Law by CIJIC*, *Cyber Law by CIJIC*(7). Faculdade de Direito da Universidade de Lisboa. http://hdl.handle.net/10400.26/34692

Poiares, N. (2019b). Cibersegurança. Literacia e Resiliência Digital dos Idosos. *Janus 2018-2019*, 118–119.

Proofpoint. (2019). *Human Factor Report 2019*. Proofpoint. https://www.proofpoint.com/us/resources/webinars/human-factor-2019

Quivy, R., & Campenhoudt, L. V. (1998). *Manual de Investigação em Ciências Sociais* (2.ª ed.). Gradiva.

Reis, F. L. (2010). *Como Elaborar uma Dissertação de Mestrado Segundo Bolonha*. Pactor.

Reis, F. L. (2018). *Investigação Científica e Trabalhos Académicos: Guia Prático* (2.ª ed.). Edições Sílabo.

Resolução do Conselho de Ministros n.º 92/2019. *Diário da República n.º 108/2019- Série I.* Portugal: Presidência do Conselho de Ministros.

Reyna, V. F., & Farley, F. (2006). Risk and Rationality in Adolescent Decision Making: Implications for Theory, Practice, and Public Policy. *Psychological Science in the Public Interest, 7*(1), 1–44. https://doi.org/10.1111/j.1529-1006.2006.00026.x

Rezende, D. A. (2006). *Engenharia de Software e Sistemas de Informação*. Brasport.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). *Planning for Cyber Security in Schools: The Human Factor*. *27*(2). https://api.semanticscholar.org/CorpusID:226456526

RNCSIRT. (2024). *Rede Nacional CSIRT*. Objetivos. https://www.redecsirt.pt/

Rodrigues, B. (2009). *Direito Penal—PArte Especial—Tomo I: Direito penal informático-digital*. Coimbra.

Sabillón, R., Serra-Ruiz, J., Cavaller, V., & Cano Martinez, J. J. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology, 21*(3), 26–39. https://doi.org/10.4018/JCIT.2019070102

Santo, P. E. (2015). *Introdução à Metodologia das Ciências Sociais: Génese, Fundamentos e Problemas* (2.ª ed.). Edições Sílabo.

Santos, L., Lima, J., Garcia, F., Monteiro, F., Silva, N., Silva, J., Santos, R., Afonso, C., & Piedade, J. (2016). *Orientações Metodológicas para Elaboração de Trabalhos de Investigação*. Instituto de Estudos Superiores Militares.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses*. Universidade Lusíada.

Şcheau, M. C., & Pop, Ş. Z. (2018). Cybercrime Evolution. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *24*(1), 225–229. https://doi.org/10.1515/kbo-2018-0034

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *IJARCCE*, *7*(11), 125–128. https://doi.org/10.17148/IJARCCE.2018.71127

SGMAI. (2018). *Secretaria Geral do MAI*. RNSI. https://www.sg.mai.gov.pt/Tecnologias/RNSI/Paginas/default.aspx

Silva, J. (2019). *Apontamentos sobre Cibersegurança e Cibercrime* [Trabalho Individual Final, 3.º Curso de Comando e Direção Policial, ISCPSI]. http://hdl.handle.net/10400.26/34970

Silva, N. (2012). *Cibersegurança—Um Paradigma Internacional de Eminente Cooperação Policial* [ISCPSI]. http://hdl.handle.net/10400.26/32114

Silva, N. T. C. (2012). *Cibersegurança: Um paradigma internacional de eminente cooperação policial* [Dissertação de Mestrado, ISCPSI]. http://hdl.handle.net/10400.26/32114

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know* (1.ª ed.). Oxford University Press.

Siponen, M. (2000). Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1), 31-41. *Inf. Manag. Comput. Security*, *8*, 31–41. https://doi.org/10.1108/09685220010371394

Sousa, Á. (2019). *Coeficiente de Correlação de Pearson e Coeficiente de correlação de Spearman. O que medem e em que situações devem ser utilizados?* https://repositorio.uac.pt/bitstream/10400.3/5365/1/Sousa_CA_21%20Mar%C3%A7o%202019.pdf

Sousa, M. J., & Baptista, C. S. (2011). *Como Fazer Investigação, Dissertações, Tese e Relatórios* (6.ª ed.). Pactor.

Stockemer, D. (2019). *Quantitative Methods for the Social Sciences: A Practical Introduction with Examples in SPSS and Stata* (1.ª ed.). Springer.

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *2016 IEEE Symposium on Security and Privacy (SP)*, 306–319. https://doi.org/10.1109/SP.2016.26

van Beek, M., ter Huurne, J., van Vierssen, D., & Vinter, E. (2005). *Pallete for teachers, learning methods for use*. Tandem Felix publishers.

van Niekerk, J. (2005). *An Holistic Framework for the Fostering of an Information Security Sub-Culture in Organizations*. https://digifors.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf

Vieira, S. de J. (2016). *Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança* [Dissertação de Mestrado, Escola Naval]. http://hdl.handle.net/10400.26/15073

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*. https://doi.org/10.1016/j.dss.2019.113160

Wack, J., Cutler, K., & Pole, J. (2002). *Guidelines on Firewalls and Firewall Policy*.

Webster, A. L. (2007). *Estatística Aplicada à Administração e Economia* (3.ª ed.). McGrawHill.

Whitman, M., & Herbert, J. M. (2017). *Principles of Information Security* (6.ª ed.). Cengage Learning.

Williams, M. (2010). Cybercrime. Em *Handbook on Crime* (1.ª ed., p. 23). Willan Publishing.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST SP 800-50; 0 ed., p. NIST SP 800-50). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50

World Internet Users Statistics and 2023 World Population Stats. (2023). Obtido 10 de dezembro de 2023, de https://www.internetworldstats.com/stats.htm

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

Zook, C. (2019). *HBR's 10 Must Reads on Managing in a Downturn*. Harvard Business Review.

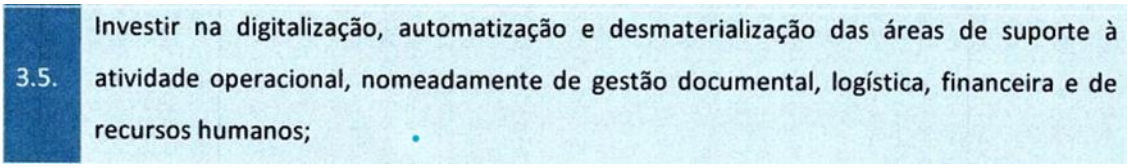
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Anexos

Anexo I - Estratégia PSP 2024-2026 (Eixo Estratégico 3 - Talento, empreendedorismo, inovação e sustentabilidade)

Figura 1

Eixo 3.5



Fonte: Polícia de Segurança Pública. (2023). Estratégia da PSP - 2024-2026.

Nota: Acedido através do seguinte link: https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Documentos%20Estrat%C3%A9gicos/Estrat%C3%A9gia%20da%20PSP%20-%202024-2026.pdf

Anexo II - Balanço Anual Social da PSP 2022

Figura 2

Quadro I – Distribuição do Efetivo Policial

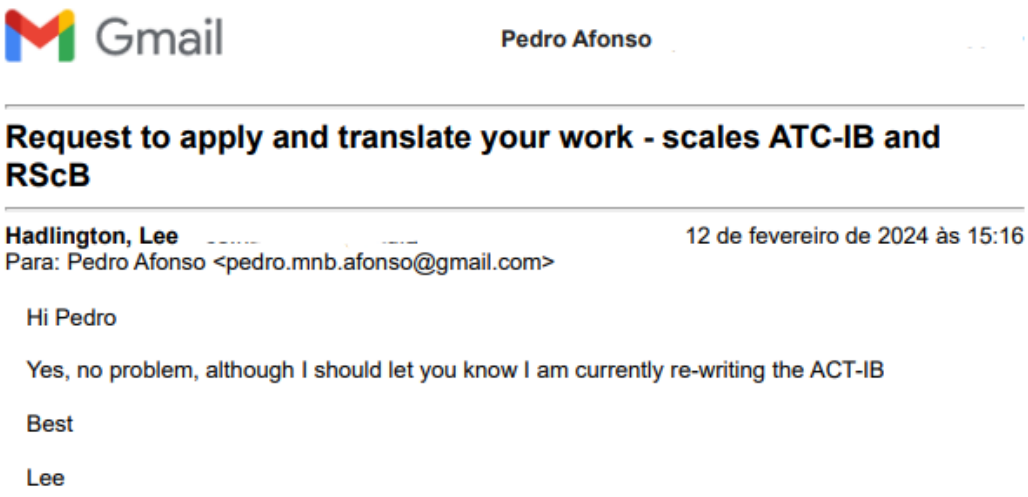
Carreiras e Categorias																															
DN/EE/UP	Superintendente-Chefe	Superintendente	Intendente	Subintendente	Comissário	Subcomissário	Oficial	Chefe Coordenador	Chefe Principal	Chefe	Chefe	Agente Coordenador	Agente Principal	Agente	Agente	Total	Cadetes Não Policiais				Aspirantes Oficiais de Polícia	Alunos EPP	Técnico Superior	Assistente técnico	Assistente operacional	Médico	Inspetor	Docente	Técnico Diag. e Terapêutica	Informático
																	1.º Ano	2.º Ano	3.º Ano	4.º Ano										
TOTAL	13	47	70	103	408	159	800	154	272	1719	2145	280	13484	3553	17317	20262	24	23	20	21	18	651	173	258	89	4	1	19	1	41
DN	6	19	18	21	52	8	124	12	28	169	209	42	443	80	565	898							108	47	5	1	0	0	1	24
ISCPSI	1	2	4	2	7	0	16	4	4	3	11	8	65	27	100	127	24	23	20	21	18		7	1	6	0	0	19	0	2
EPP	1	1	2	4	11	0	19	1	5	18	24	4	107	0	111	154						651	1	12	6	0	0	0	0	2
CD AVEIRO	0	1	2	5	11	3	22	5	9	38	52	10	411	1	422	496							4	8	2	0	0	0	0	0
CD BEJA	0	1	1	1	4	1	8	0	5	14	19	4	151	21	176	203							3	19	3	0	0	0	0	0
CD BRAGA	0	1	2	3	14	3	23	8	6	40	54	2	453	3	458	535							4	10	2	0	0	0	0	0
CD BRAGANÇA	0	1	1	0	5	0	7	4	4	12	20	7	141	2	150	177							1	11	1	0	0	0	0	1
CD C. BRANCO	0	1	1	1	4	3	10	4	8	13	25	9	178	2	189	224							2	2	2	0	0	0	0	1
CD COIMBRA	0	1	2	2	8	2	15	9	7	29	45	6	370	2	378	438							9	11	2	0	0	0	0	1
CD ÉVORA	0	0	1	1	4	1	7	2	5	12	19	2	165	1	168	194							1	6	1	0	0	0	0	0
CD FARO	0	1	1	3	18	6	29	6	6	68	80	4	654	41	699	808							2	13	0	0	0	0	0	2
CD GUARDA	0	1	1	0	5	2	9	2	5	12	19	5	136	0	141	169							1	8	1	0	0	0	0	0
CD LEIRIA	0	1	1	2	12	4	20	5	8	33	46	10	394	1	405	471							6	11	3	0	0	0	0	0
CM LISBOA	1	4	13	18	79	60	175	17	60	591	668	48	3374	3003	6425	7268							2	8	21	0	0	0	0	0
CD PORTALEGRE	0	1	1	1	3	3	9	1	4	12	17	6	139	2	147	173							1	6	0	0	0	0	0	1
CM PORTO	1	1	10	11	59	22	104	24	33	250	307	14	2653	40	2707	3118							6	22	12	2	1	0	0	3
CD SANTARÉM	0	1	0	2	8	2	13	3	11	37	51	5	324	1	330	394							3	13	2	0	0	0	0	1
CD SETÚBAL	0	1	2	4	20	10	37	6	13	89	108	18	908	86	1012	1157							3	12	2	1	0	0	0	1
CD V CASTELO	0	1	1	0	6	1	9	5	5	10	20	8	145	3	156	185							1	2	0	0	0	0	0	0
CD VILA REAL	0	1	1	1	7	1	11	2	4	15	21	4	159	0	163	195							2	10	2	0	0	0	0	0
CD VISEU	0	1	1	2	6	3	13	5	5	15	25	9	204	1	214	252							2	9	2	0	0	0	0	2
CR MADEIRA	1	1	1	5	17	7	32	4	11	58	73	5	610	43	658	763							2	4	5	0	0	0	0	0
CR AÇORES	1	1	1	4	16	14	37	7	10	77	94	15	677	140	832	963							1	13	8	0	0	0	0	0
UEP	1	3	2	10	32	3	51	18	16	104	138	35	623	53	711	900							1	0	1	0	0	0	0	0

Fonte: Polícia de Segurança Pública. (2023). *Balanço Social da PSP 2022*.

Nota: Acedido através do seguinte *link*:

https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Balan%C3%A7o%20Social/Balan%C3%A7o%20Social%20da%20PSP%202022.pdf

Anexo III – Autorização para aplicação das escalas no questionário



Gmail Pedro Afonso

Request to apply and translate your work - scales ATC-IB and RScB

Hadlington, Lee 12 de fevereiro de 2024 às 15:16
Para: Pedro Afonso <pedro.mnb.afonso@gmail.com>

Hi Pedro

Yes, no problem, although I should let you know I am currently re-writing the ACT-IB

Best

Lee

Anexo IV – Escalas RScB e ATC-IB traduzidas e validadas

	Item
1	Partilhar palavras-passe com amigos e colegas.
2	Usar ou criar palavras-passe pouco complicadas (por ex., apelido e data de nascimento).
3	Usar a mesma palavra-passe para sites diferentes.
4	Usar sistemas de armazenagem online para partilhar ou guardar informação pessoal e sensível.
5	Inserir informação de pagamento em sites que não têm informação/certificação de segurança clara
6	Usar Wi-Fi de livre acesso público
7	Confiar num amigo ou colega próximo para conselhos em aspetos de segurança online.
8	Descarregar anti-vírus gratuito de uma fonte desconhecida.
9	Desactivar o anti-vírus no meu computador de trabalho para que possa descarregar informação de sites.
10	Trazer a minha própria pen para o trabalho a fim de transferir informação para ela.
11*	Verificar que o software do meu smartphone/tablet/portátil/PC está actualizado.
12	Descarregar conteúdos digitais (música, filmes, jogos) de fontes não-licenciadas.
13	Partilhar a minha localização actual em redes sociais.
14	Aceitar solicitações de amizade em redes sociais porque reconheço a foto.
15	Carregar em links de emails não solicitados de uma fonte desconhecida.
16	Enviar informação pessoal a estranhos pela Internet.
17	Carregar em links de emails de amigos próximos ou de um colega de trabalho.
18*	Procurar actualizações para qualquer anti-vírus que tenha instalado.
19	Descarregar informação e material de sites para o meu computador de trabalho sem verificar a sua autenticidade.
20	Guardar informação da empresa no meu dispositivo electrónico pessoal (por ex., smartphone/tablet/portátil)

* Indica itens com pontuação inverse.

Fonte: Nunes, P. (2019). *Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar* [Dissertação de Mestrado, Instituto Politécnico de Lisboa, Escola Superior de Tecnologia da Saúde de Lisboa]. http://hdl.handle.net/10400.21/12523

	Item
1	Penso que a administração tem a responsabilidade de assegurar que a empresa esteja protegida de cibercrime
2*	Estou ciente do meu papel em manter a companhia protegida de potenciais cibercriminosos.
3	Penso que todos na empresa têm um papel a desempenhar na protecção contra ameaças de cibercriminosos.
4	É difícil saber como posso proteger a organização do cibercrime.
5	Não tenho as competências necessárias para proteger a organização do cibercrime.
6	Não creio que a segurança informática seja uma prioridade na minha organização.
7	Os sistemas de computador oferecem toda a protecção que uma companhia precisa.
8	Creio que denunciar cibercrimes é uma perda de tempo.
9	A Polícia não tem meios para combater o cibercrime de forma eficaz.
10	Creio que os cibercriminosos são mais avançados do que as pessoas que nos deviam proteger.
11	Penso que a informação do Governo e da Polícia em relação ao cibercrime não tem importância para as empresas.^
12	Penso que a Polícia está demasiado ocupada para se preocupar com o cibercrime.^
13	Receio que, se denunciar um ciberataque à Polícia, isso vá prejudicar a reputação da empresa
14*	Penso que deve ser feito mais para comunicar os riscos de cibercrime às pessoas na organização.
15*	Estou a par da política de uso informático da empresa, e tento segui-la.
16	Se ocorrer um ciberataque, não saberei como denunciá-lo.
17	Não acho que é da minha responsabilidade denunciar um ciberataque contra a empresa.
18	Não presto atenção ao material da empresa sobre ameaças de cibercrime.
19*	Confio na minha capacidade de reconhecer sinais de um ciberataque.
20*	Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da empresa.
21*	Sinto que qualquer pessoa na empresa está em risco de manipulação por vigaristas.
22	Penso que os cibercriminosos apenas atingem uma empresa quando têm muito a ganhar do ponto de vista financeiro.
23	Penso que apenas as grandes empresas são atingidas por hackers e cibercriminosos.
24	Penso que apenas empresas que recebem pagamentos por sistemas online estão em risco de serem vítimas de cibercrime.^
25	Acho que não sei quem é responsável por proteger a companhia do cibercrime.

Fonte: Nunes, P. (2019). *Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar* [Dissertação de Mestrado, Instituto Politécnico de Lisboa, Escola Superior de Tecnologia da Saúde de Lisboa]. http://hdl.handle.net/10400.21/12523

Anexo V - Autorização para aplicação do inquérito por questionário

RE: Pedido de Colaboração em Trabalho de Dissertação de Mestrado Integrado em Ciências Policiais | 158336 – Pedro Afonso

DN DEPFORM

qua 28-02-2024 10:54

Caixa de Entrada

Para:ISCPSI - Direcção Ensino <de.iscpsi@psp.pt>;

Cc:Paulo Jorge Da Silva Onofre <pjonofre@psp.pt>; Paula Alexandra Da Conceição Cunha <pacunha@psp.pt>; Pedro Miguel Nunes Barreiros Afonso <pmafonso@psp.pt>;

Exmo. Senhor Diretor do ISCPSI

Relativamente ao assunto em epígrafe, encarrega-me o Exmo. Sr. Diretor do Departamento de Formação, da Policia de Segurança Pública, Superintendente Paulo Jorge da Silva Onofre, de informar V.ª Ex.ª o deferimento por sua Ex.ª a DNAUORH no pedido infra, cujo despacho se transcreve:

"Autorizo a título voluntário.
28/02/2024
DNAUORH
Paula Peneda
Superintendente Chefe"

Com os melhores cumprimentos,

"Uma Polícia das pessoas e para as pessoas: segurança, igualdade, respeito e confiança." – Estratégia PSP 2024/2026"

Catarina Silva Batista Tomeno
Comissário | *Chief Inspector*
Departamento de Formação
Chefe de Núcleo de Recursos Didáticos

T: +351 21 811 10 00
Ext: 11374
E: casbatista@psp.pt

POLÍCIA
SEGURANÇA PÚBLICA

Direção Nacional da PSP
Largo da Penha de França, n.º 1 | 1199-010 Lisboa

policiasegurancapublica
policiasegurancapublica
www.psp.pt
PT

Apêndices

Apêndice A – Caracterização Sociodemográfica

Figura 3

Sexo dos Inquiridos

Feminino	84
Masculino	321

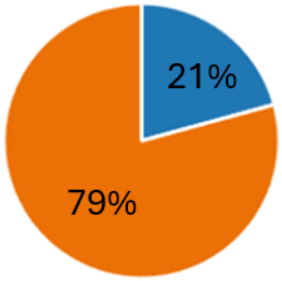


Figura 4

Faixas Etárias

Entre 18 e 25 anos	75
Entre 26 e 35 anos	86
Entre 36 e 45 anos	121
Entre 46 e 55 anos	102
Mais de 55 anos	21

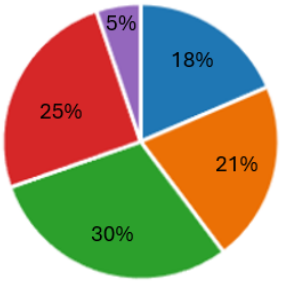


Figura 5

Habilitações Literárias

Ensino Básico	4
Ensino Secundário	310
Ensino Superior	91

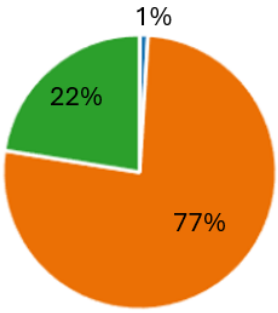
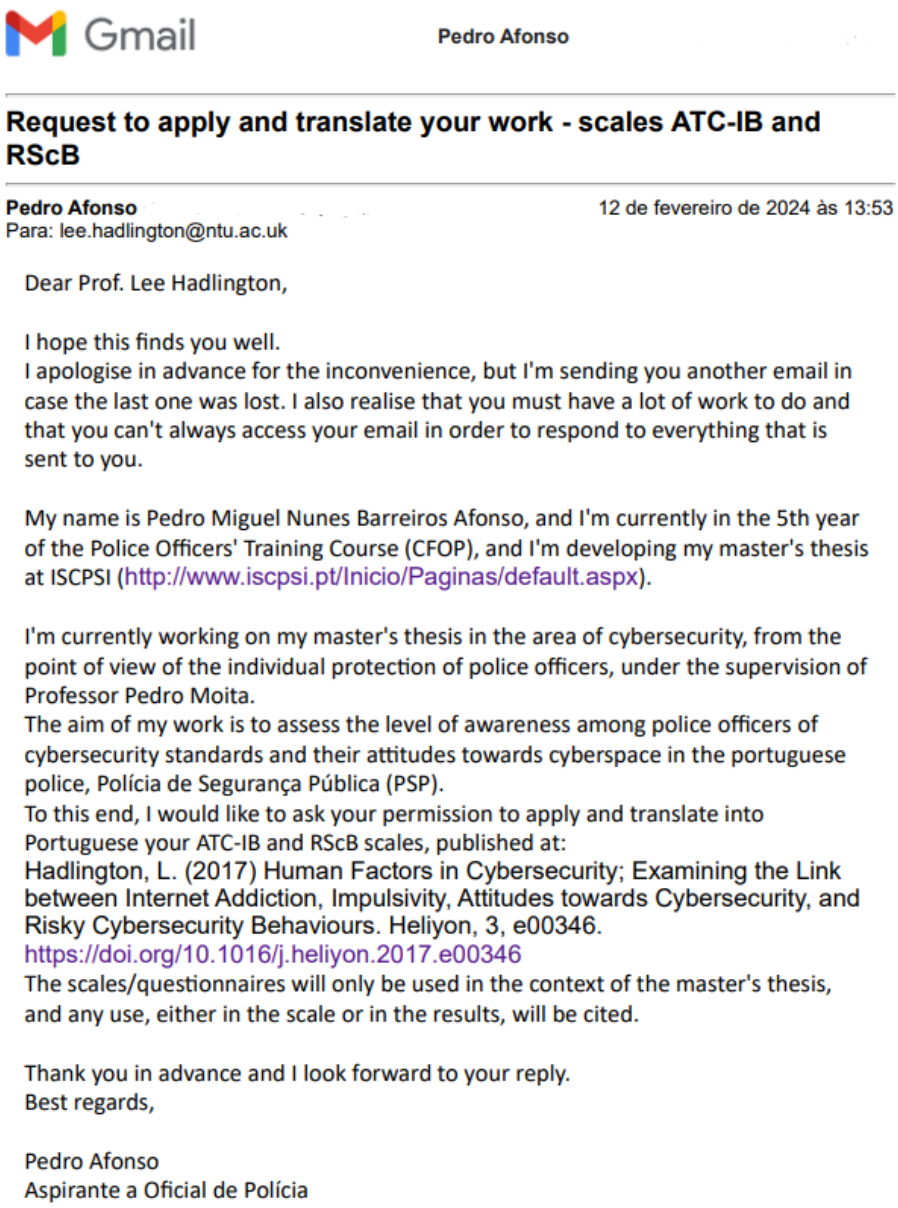


Figura 6

Carreira Atual

Apêndice B – Pedido de autorização para aplicação das escalas no questionário



Gmail Pedro Afonso

Request to apply and translate your work - scales ATC-IB and RScB

Pedro Afonso 12 de fevereiro de 2024 às 13:53
Para: lee.hadlington@ntu.ac.uk

Dear Prof. Lee Hadlington,

I hope this finds you well.
I apologise in advance for the inconvenience, but I'm sending you another email in case the last one was lost. I also realise that you must have a lot of work to do and that you can't always access your email in order to respond to everything that is sent to you.

My name is Pedro Miguel Nunes Barreiros Afonso, and I'm currently in the 5th year of the Police Officers' Training Course (CFOP), and I'm developing my master's thesis at ISCPSI (http://www.iscpsi.pt/Inicio/Paginas/default.aspx).

I'm currently working on my master's thesis in the area of cybersecurity, from the point of view of the individual protection of police officers, under the supervision of Professor Pedro Moita.
The aim of my work is to assess the level of awareness among police officers of cybersecurity standards and their attitudes towards cyberspace in the portuguese police, Polícia de Segurança Pública (PSP).
To this end, I would like to ask your permission to apply and translate into Portuguese your ATC-IB and RScB scales, published at:
Hadlington, L. (2017) Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours. Heliyon, 3, e00346.
https://doi.org/10.1016/j.heliyon.2017.e00346
The scales/questionnaires will only be used in the context of the master's thesis, and any use, either in the scale or in the results, will be cited.

Thank you in advance and I look forward to your reply.
Best regards,

Pedro Afonso
Aspirante a Oficial de Polícia

Apêndice C – Escalas adaptadas ao contexto policial

Escala dos Comportamentos arriscados de Cibersegurança (RScB), adaptada à Polícia: (* Indica itens com pontuação inversa)

1- Partilhar *passwords* com amigos e colegas.
2- Usar ou criar palavras-passe demasiado simples. (por exemplo, nome de familiar, data de nascimento e apelidos)
3- Usar a mesma *password* para diferentes *websites*.
4- Usar sistemas de armazenamento *online* (*cloud*) para partilhar ou guardar informação pessoal e sensível.
5- Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita.
6- Usar redes de Wi-Fi de acesso livre (públicas), no acesso ao email institucional.
7- Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online.
8- *Identificar devidamente o spam (selecionar "marcar como lixo").
9- Guardar automaticamente as credenciais de acesso ao email/websites.
10- Utilizar a *pen drive* pessoal com a finalidade de transferir informação institucional para ela.
11- *Verificar as atualizações de software do smartphone/tablet/portátil/PC.
12- Descarregar conteúdos digitais de fontes não fidedignas.
13- Navegar em websites que não contenham "https://" no seu URL.
14- Utilizar uma *pen drive* desconhecida no computador, para aceder aos seus conteúdos.
15- Clicar em links em emails recebidos de uma fonte desconhecida.
16- Enviar informação pessoal a estranhos pela Internet.
17- Clicar em links de email enviados por amigos próximos ou por colegas de trabalho.
18- *Terminar a sessão, sempre que não faça uso do email.
19- Descarregar informação e material de websites para o computador sem verificação da veracidade.
20- Guardar informações/dados da instituição no dispositivo eletrónico pessoal. (por exemplo, smartphone/tablet/portátil).

Escala das Atitudes em relação à Cibersegurança (ATC-P) adaptada à Polícia:

(* Indica itens com pontuação inversa)

1- Penso que a instituição tem a responsabilidade de assegurar que esta esteja protegida de cibercrime.
2- *Estou ciente do meu papel em manter a instituição protegida de potenciais cibercriminosos
3- *Penso que todos na instituição têm um papel a desempenhar na proteção contra ameaças de cibercriminosos.
4- É difícil saber como posso proteger a instituição do cibercrime.
5- Não tenho as competências necessárias para proteger a instituição do cibercrime.
6- Não creio que a segurança informática seja uma prioridade na minha instituição.
7- Os sistemas informáticos oferecem toda a proteção que uma instituição precisa.
8- Creio que denunciar o cibercrime é uma perda de tempo.
9- A Polícia não tem meios para combater o cibercrime de forma eficaz.
10- Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.
11- Penso que a informação do Governo e da Polícia em relação ao cibercrime não tem importância para as organizações.
12- Penso que a Polícia está demasiado ocupada para se preocupar com o cibercrime.
13- Receio que, se denunciar um ciberataque à Polícia, isso vá prejudicar a reputação da própria instituição.
14- *Penso que deve ser feito mais para comunicar os riscos do cibercrime às pessoas na instituição.
15- *Estou a par da política de uso informático da instituição, e tento segui-la.
16- Se ocorrer um ciberataque, não saberei como denunciá-lo.
17- Não acho que é da minha responsabilidade denunciar um ciberataque contra a instituição.
18- Não presto atenção à informação disponibilizada pela instituição sobre as ameaças de cibercrime.
19- *Confio na minha capacidade de reconhecer sinais de um ciberataque.
20- *Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da instituição.
21- *Sinto que qualquer pessoa na instituição está em risco de manipulação por ciber "vigaristas e burlões".
22- Penso que os cibercriminosos apenas atingem uma instituição quando têm muito a ganhar do ponto de vista financeiro.
23- Penso que apenas as grandes empresas e organizações são atingidas por hackers e cibercriminosos.
24- Penso que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque.
25- Não sei quem é responsável por proteger a instituição do cibercrime.

Apêndice D – Questionário aplicado

Comportamentos e Atitudes de Cibersegurança: Questionário aos Polícias do COMETLIS

O presente questionário é aplicado no âmbito de uma investigação para a Dissertação de Mestrado do Curso de Formação de Oficiais de Polícia, do mestrado em Segurança Pública, subordinada ao tema "Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS".

O questionário tem como finalidade recolher dados sobre aquilo que os polícias pensam e atuam relativamente à Cibersegurança e à sua Ciber-Higiene.
O recurso à tecnologia e ao Ciberespaço por parte da Polícia é inequívoco, daí que seja relevante para a Polícia que os seus profissionais estejam aptos a operar esta tecnologia de forma segura, prevenindo-se de incidentes e ataques cibernéticos que coloquem em causa a integridade e confidencialidade dos dados sensíveis que trabalham.

A título exemplificativo, estas tecnologias inerentes ao serviço policial são os Computadores (fixo ou portátil), *Smartphones* e *Tablets*, utilizados no quotidiano policial, seja em serviço ou fora dele (para aceder o *e-mail*, por exemplo).

Assim, pedimos que responda a este questionário de forma sincera e individual em todas as questões.
Os dados obtidos são anónimos e confidenciais e serão utilizados única e exclusivamente no âmbito da dissertação de mestrado. De referir que a realização deste questionário levará apenas cerca de **5 a 8 minutos** do seu tempo, não existindo respostas certas ou erradas, pelo que se pede que selecione aquela resposta que considera mais válida no seu entender.

Terminado o questionário, submeta-o, selecionando "Submeter".
Alguma dúvida que surja, poderá contactar o autor via email: pmafonso@psp.pt

Agradecemos desde já a sua colaboração!

O Aspirante a Oficial de Polícia,
Pedro Afonso
M/158336

)brigatória

Termo de consentimento informado

«Li e compreendi a informação fornecida relativa ao presente questionário, no âmbito da dissertação de mestrado "Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS" e concordo responder voluntariamente ao mesmo.»

1

Consentimento *

Marcar apenas uma opção.

◯ Concordo

◯ Discordo *(Avançar para a última secção - **Agradecimento**)*

Parte 1 - Caracterização Sociodemográfica

2

Sexo *

Marcar apenas uma opção

- ◯ Feminino
- ◯ Masculino

3

Idade *

Marcar apenas uma opção

- ◯ Entre 18 e 25 anos
- ◯ Entre 26 e 35 anos
- ◯ Entre 36 e 45 anos
- ◯ Entre 46 e 55 anos
- ◯ Mais de 55 anos

4

Habilitações Literárias *

Marcar apenas uma opção

- ◯ Ensino Básico
- ◯ Ensino Secundário
- ◯ Ensino Superior

5

Carreira Atual *

Marcar apenas uma opção

- ◯ Agente de Polícia
- ◯ Chefe de Polícia
- ◯ Oficial de Polícia

Parte 2 - Comportamentos de Cibersegurança

Selecione a opção que melhor se adequa à frequência com que nos últimos 6 meses tem sido o seu comportamento.

6

Partilhar *passwords* com amigos e colegas. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	◯	◯	◯	◯	◯	◯	◯

7

Usar ou criar *passwords* demasiado simples. (por exemplo, nome de familiar, data de nascimento e apelidos) *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	◯	◯	◯	◯	◯	◯	◯

8

Usar a mesma *password* para diferentes *websites*. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	◯	◯	◯	◯	◯	◯	◯

Usar sistemas de armazenamento *online* (*cloud*) para partilhar ou guardar informação pessoal e sensível. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

10

Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

Usar redes de Wi-Fi de acesso livre (públicas), no acesso ao email institucional. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

12

Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

13

Identificar devidamente o spam (selecionar "marcar como lixo"). *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

14

Guardar automaticamente as credenciais de acesso ao email/websites. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

15

Utilizar a *pen drive* pessoal com a finalidade de transferir informação institucional para ela. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

Verificar as atualizações de software do smartphone/tablet/portátil/PC. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

17

Descarregar conteúdos digitais de fontes não fidedignas. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

18

Navegar em websites que não contenham "https://" no seu URL. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

19

Utilizar uma *pen drive* desconhecida no computador, para aceder aos seus conteúdos. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

20

Clicar em links de emails recebidos de uma fonte desconhecida. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

21

Enviar informação pessoal a estranhos pela Internet. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

22

Clicar em links de email enviados por amigos próximos ou por colegas de trabalho. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

23

Terminar a sessão, sempre que não faça uso do email. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

24

Descarregar informação e material de websites para o computador sem verificação da veracidade. *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

25

Guardar informações/dados da instituição no dispositivo eletrónico pessoal. (por exemplo, smartphone/tablet/portátil). *

0- Nunca
1- 1 a 2 vezes por semestre
2- 1 a 2 vezes por trimestre
3- 1 a 2 vezes por mês
4- 1 a 2 vezes por quinzena
5- 1 a 2 vezes por semana
6- Diariamente

	0	1	2	3	4	5	6
Assinale apenas uma opção	○	○	○	○	○	○	○

Parte 3 - Atitudes de Cibersegurança

Selecione a opção que melhor se adapta à sua experiência nos últimos 6 meses.

26

Penso que a instituição tem a responsabilidade de assegurar que esta esteja protegida de cibercrime. *

- ○ Concordo totalmente.
- ○ Concordo.
- ○ Discordo.
- ○ Discordo totalmente.

27

Estou ciente do meu papel em manter a instituição protegida de potenciais cibercriminosos. *

- ○ Concordo totalmente.
- ○ Concordo.
- ○ Discordo.
- ○ Discordo totalmente.

28

Penso que todos na instituição têm um papel a desempenhar na proteção contra ameaças de cibercriminosos. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

29

É difícil saber como posso proteger a instituição do cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

30

Não tenho as competências necessárias para proteger a instituição do cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

31

Não creio que a segurança informática seja uma prioridade na minha instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

32

Os sistemas informáticos oferecem toda a proteção que uma instituição precisa. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

33

Creio que denunciar o cibercrime é uma perda de tempo. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

34

A Polícia não tem meios para combater o cibercrime de forma eficaz. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

35

Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

36

Penso que a informação do Governo e da Polícia em relação ao cibercrime não tem importância para as organizações. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

37

Penso que a Polícia está demasiado ocupada para se preocupar com o cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

38

Receio que, se denunciar um ciberataque à Polícia, isso vá prejudicar a reputação da própria instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

39

Penso que deve ser feito mais para comunicar os riscos do cibercrime às pessoas na instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

40

Estou a par da política de uso informático da instituição, e tento segui-la. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

41

Se ocorrer um ciberataque, não saberei como denunciá-lo. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

42

Não acho que é da minha responsabilidade denunciar um ciberataque contra a instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

43

Não presto atenção à informação disponibilizada pela instituição sobre as ameaças de cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

44

Confio na minha capacidade de reconhecer sinais de um ciberataque. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

45

Penso que a maior ameaça para os sistemas informáticos vem de pessoas de dentro da instituição. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

46

Sinto que qualquer pessoa na instituição está em risco de manipulação por ciber "vigaristas e burlões". *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

47

Penso que os cibercriminosos apenas atingem uma instituição quando têm muito a ganhar do ponto de vista financeiro. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

48

Penso que apenas as grandes empresas e organizações são atingidas por hackers e cibercriminosos. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

49

Penso que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

50

Não sei quem é responsável por proteger a instituição do cibercrime. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Parte 4 - Quick Reference Guide
Cibersegurança na PSP

51

Tendo em conta o seguinte exemplo de Quick Reference Guide, responda às questões:

52

Considera viável um Quick Reference Guide, na área da Cibersegurança, implementado e presente para consulta na PSP. *

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

53

Utilizaria um Quick Reference Guide na sua área de trabalho. *

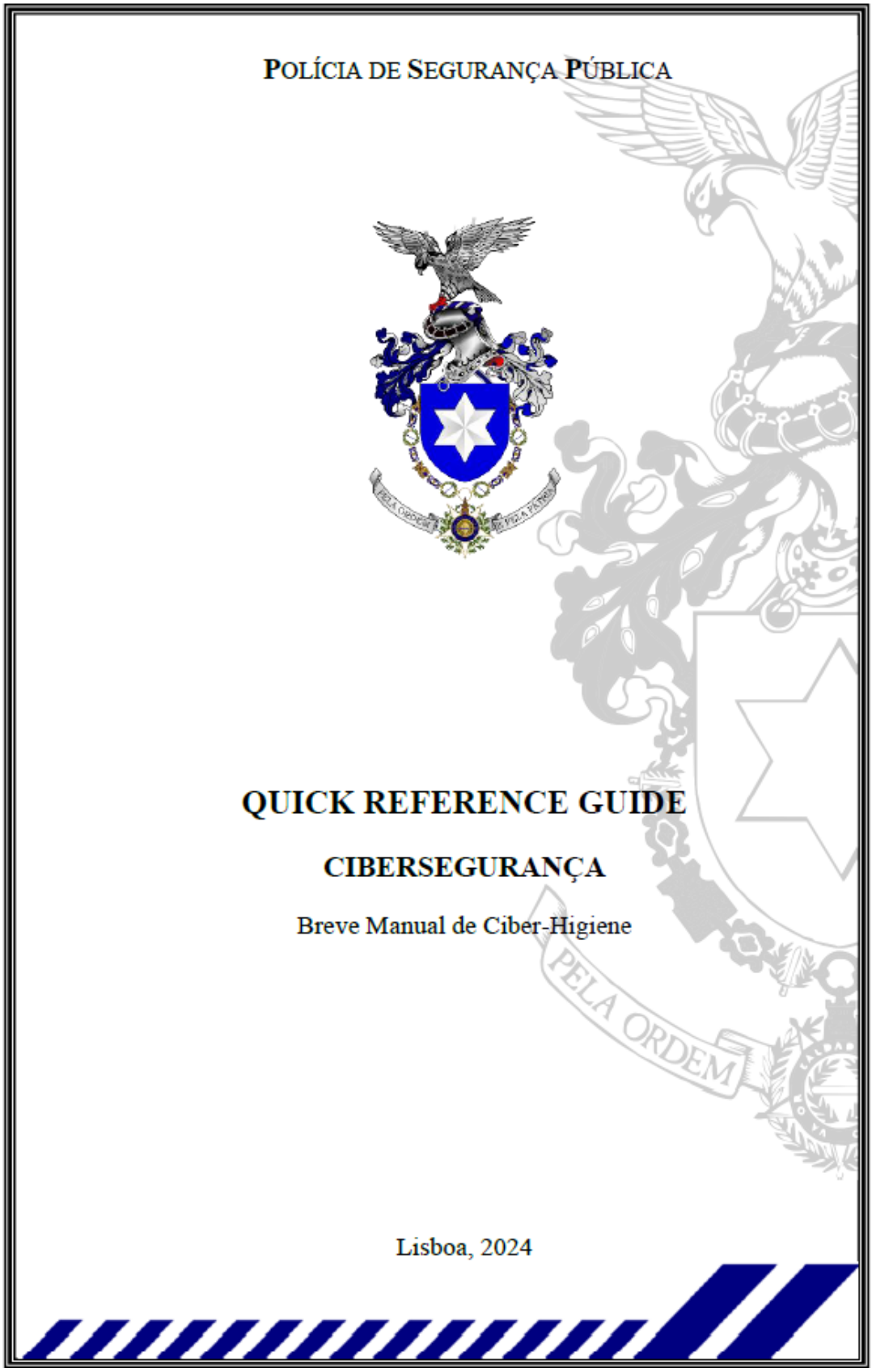
- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Agradecimento

O questionário chegou ao fim.
A sua colaboração será fundamental para o presente estudo, pelo que agradeço o tempo despendido.
Votos de maiores sucessos pessoais e profissionais.
Aspirante Pedro Afonso

Microsoft Forms

Apêndice E – Proposta do Quick Reference Guide – PSP



POLÍCIA DE SEGURANÇA PÚBLICA

QUICK REFERENCE GUIDE – CIBERSEGURANÇA

Este *Quick Reference Guide* consiste num breve manual de **normas básicas** a ter em consideração na utilização do ciberespaço, no desempenho das suas funções.

O uso de tecnologias digitais/virtuais é inerente às funções dos polícias e, dado a sofisticação do cibercrime e de uma panóplia de incidentes informáticos a que os mesmos estão expostos aquando da navegação pelo ciberespaço, este guia, vem **auxiliar** na utilização deste domínio, através das suas **recomendações** de ciber-higiene.

Tendo em conta o seu perfil de utilizador do computador, seja ele perfil de administrador, seja perfil de utilizador comum, recomenda-se, desde já, uma **atitude preventiva** no que diz respeito ao uso do mesmo.

Este *Quick Reference Guide* é direcionado para todos os profissionais da Polícia de Segurança Pública que fazem uso de computadores institucionais, mas também, pode servir de auxílio no uso de computadores e dispositivos pessoais, tendo em conta a especificidade do serviço policial, dado que, muitas das vezes, o *email* institucional é acedido através do computador ou *smartphone* pessoal, por exemplo.

POLÍCIA DE SEGURANÇA PÚBLICA

PERFIL DE UTILIZADOR COMUM

PASSWORD

As *passwords* têm a missão de impedir que um indivíduo aceda a um dispositivo, conta, aplicação, *email*, entre outros domínios que não lhe pertençam, evitando assim o acesso a informações pessoais de outrem.

Assim, a salvaguarda da *password* tem início na sua criação, pelo que o principal objetivo passa por "complicar" a mesma.

Recomendações:

- *Password* complexa, que contemple: >12 caracteres; letras maiúsculas e minúsculas; algarismos e caracteres especiais;
- Evitar o uso do nome do utilizador na *password*;
- Utilização de uma *password* por plataforma, *email*, dispositivo ou outro tipo de conta, evitando a repetição da mesma *password* em domínios diferentes;
- Evitar guardar a *password* em qualquer domínio ou *browser*;
- Se possível, utilizar a função da autenticação de duplo fator.
- Alterar frequentemente a *password*;

EMAIL

Os *emails* são, muitas das vezes, a porta de entrada de inúmeros ciberataques. O *email* institucional tem protocolos de segurança acrescida, devido ao domínio RNSI, contudo, existem algumas recomendações a ter em conta.

Recomendações:

- Ter especial atenção aos *links* e anexos recibos na caixa;
- Verificar a veracidade dos *emails*;
- Identificar devidamente o *spam*, selecionando devidamente "marcar como lixo";
- Terminar a sessão aquando da não utilização do *email*.
- Evitar guardar automaticamente as credenciais de acesso ao.

HARDWARE

A devida atenção dada ao *hardware* é fulcral para a prevenção de ciberataques. Essencialmente, é importante bloquear o acesso a este por parte de dispositivos externos alheios ou estranhos.

Recomendações:

- Evitar introduzir *pen drives*, CDs ou discos externos desconhecidos nos computadores e dispositivos;
- Bloquear dispositivos desnecessários, ou aquando da não utilização dos mesmos;
- Bloquear, sempre que possível o acesso à câmara e ao microfone.

POLÍCIA DE SEGURANÇA PÚBLICA

NAVEGAÇÃO

A navegação pelo ciberespaço, especialmente na *Internet*, é algo que deve ser feito de forma segura e consciente, adotando um comportamento preventivo face a todas as ações que são tomadas no mundo virtual.

Recomendações:

- Evitar aceder a redes *Wi-fi* públicas ou desconhecidas;
- Evitar *downloads* desnecessários;
- Evitar ceder autorização para funcionalidades, para além daquilo que é estritamente necessário;
- Priorizar a navegação em *websites* que contenham a expressão "https" no seu URL (e.g. "**https**://intranet.mai.pt");
- Recusar *cookies*;
- Executar sempre a versão mais recente do *browser*;
- Verificar as políticas de privacidade dos *websites* a que acede.

LOGOUT

Na navegação de uma sessão autenticada, garantir que existe um recurso que permita, no *website*, a função de terminar a sessão.

Recomendações:

- Garantir que termina a sessão de todos os *websites* do browser, de *emails* e outras aplicações instaladas no computador.
- Garantir que todas as janelas do *browser* se encontram fechadas após o *logout*.

PERFIL DE ADMINISTRADOR

FIREWALL

A *firewall* controla o tráfego da rede, bloqueando aquilo que se torna indesejável para o computador.

Recomendações:

- Utilizar um sistema de *firewall*, ou ativá-la, nos computadores com acesso à *Internet*.

UPDATES

Uma grande parte dos ataques no ciberespaço são consumados devido às falhas exploradas nas aplicações e sistemas usados pelos utilizadores. Uma boa prática que auxilia na prevenção desse fenómeno, passa por contar sempre com as versões mais recentes dessas mesmas aplicações e sistemas.

Recomendações:

- Aplicações, *browsers*, sistema operativo e antivírus sempre atualizados na versão mais recente.

ANTIVÍRUS

O antivírus analisa e ajuda a remover ficheiros de *malware* infiltrados nos computadores e dispositivos.

Recomendações:

- Procurar ativar as Proteções contra Vírus e Ameaças do Windows;
- Manter atualizadas as Proteções contra Vírus e Ameaças do Windows.

POLÍCIA
SEGURANÇA PÚBLICA

Apêndice F – Requerimento para aplicação de inquérito por questionário aos polícias do COMETLIS

MINISTÉRIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Exma. Senhora Diretora Nacional Adjunta da UORH,

Superintendente-chefe Paula Cristina da Graça Peneda,

Eu, Pedro Afonso, Aspirante a Oficial de Polícia n.º 3631/158336, do 36.º Curso de Formação de Oficiais de Polícia, do Mestrado em Segurança Pública, no âmbito da realização da Dissertação de Mestrado, subordinada ao tema "Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS", do qual é orientador o Senhor Professor Especialista Pedro Moita, venho mui respeitosamente solicitar a V.ª Ex.ª que se digne autorizar a realização de questionários a polícias pertencentes ao Comando Metropolitano de Lisboa.

A realização destes questionários tem como intuito a recolha de dados relativos à temática em estudo. Pretende-se destes polícias (participantes voluntários quanto à concessão do questionário), identificar qual o nível de consciencialização relativamente à cibersegurança e à sua proteção aquando do uso das tecnologias inerentes ao seu serviço.

O nosso intuito é aplicá-lo ao efetivo do COMETLIS, tendo em conta a nossa amostra de cerca de 365 polícias, solicitando a posteriori o envio do questionário a 700 polícias, na tentativa de salvaguardar a falta de adesão.

Para esta investigação será realizado um questionário, que se encontra em anexo. Para o tratamento de dados recorrer-se-á ao software Statistical Package for Social Sciences (SPSS), que por excelência, é o instrumento de análise nos estudos quantitativos, onde se enquadra metodologicamente o presente estudo.

Comprometo-me a manter a confidencialidade dos dados recolhidos, fora do âmbito da elaboração e discussão da dissertação, bem como a cumprir as demais regras éticas relativas à realização da investigação científica.

Pede deferimento.

Lisboa, ISCPSI, 20 de fevereiro de 2024

Pedro Afonso

Aspirante a Oficial de Polícia n.º 3631/158336

Apêndice G - Pedido de divulgação do inquérito por questionário à população do estudo

Pedro Miguel Nunes Barreiros Afonso

qua 28-02-2024 16:20

Para:COMETLIS - Núcleo de Formação <formacao.lisboa@psp.pt>;

Cc:Tiago Veloso Nabais <tvnabais@psp.pt>; Pedro Francisco Manique Silva Moita <pfmoita@psp.pt>; DN DEPFORM <depform@psp.pt>;

Exmo. Senhor
Chefe do Núcleo de Formação do COMETLIS
MI Comissário João Moura

Relativamente ao assunto em epígrafe, no âmbito da Dissertação de Mestrado intitulada: "Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS", da qual é orientador o Exmo. Sr. Professor Especialista Pedro Francisco Manique Silva Moita, venho por este meio solicitar a difusão do deferido Questionário anexado e disponível para resposta a partir do seguinte Código QR ou do link: https://forms.office.com/e/fUAqtYFca9

Neste sentido, solicito a difusão do susodito link ou Código QR por todo o efetivo policial do COMETLIS (agentes, chefes e oficiais), de modo a salvaguardar um maior número de respostas ao mesmo.
Obrigado pela atenção dispensada.

Com os meus melhores cumprimentos,

AOP Pedro Afonso
M/ 158336

Pedro Miguel N. Barreiros Afonso

Aspirante a Oficial de Polícia

T: +351 938 551 732
E: pmafonso@psp.pt
XXXVI CFOP

policiasegurancapublica

POLÍCIA
SEGURANÇA PÚBLICA

Instituto Superior de Ciências Policiais e Segurança Interna

Rua 1º de Maio, nº 3, 1349-040 Lisboa
www.psp.pt

PT

Apêndice H - Pedido de reforço de divulgação do inquérito por questionário à população do estudo

Pedro Miguel Nunes Barreiros Afonso

seg 11-03-2024 13:17

Para:COMETLIS - Núcleo de Formação <formacao.lisboa@psp.pt>;

Cc:Tiago Veloso Nabais <tvnabais@psp.pt>; Pedro Francisco Manique Silva Moita <pfmoita@psp.pt>;

Exmo. Senhor
Chefe do Núcleo de Formação do COMETLIS
MI Comissário João Moura

Relativamente ao assunto em epígrafe, no âmbito da Dissertação de Mestrado intitulada: "Cibersegurança na PSP: Uma Análise do Nível de Consciencialização dos Polícias do COMETLIS", da qual é orientador o Exmo. Sr. Professor Especialista Pedro Francisco Manique Silva Moita, venho por este meio solicitar uma **insistência** de difusão de Questionário, devido ao facto da anterior difusão contar com um problema técnico, quanto ao seu acesso, que se encontra agora resolvido.
O questionário encontra-se, assim, disponível para resposta a partir do seguinte link: https://forms.office.com/e/fUAqtYFca9
Neste sentido, solicito, uma vez mais, a difusão do susodito link por todo o efetivo policial do COMETLIS (agentes, chefes e oficiais), de modo a salvaguardar um maior número de respostas ao mesmo.
Obrigado pela atenção dispensada.
Com os meus melhores cumprimentos,

Pedro Miguel Nunes Barreiros Afonso
Aspirante a Oficial de Polícia
M/ 158336

Pedro Miguel N. Barreiros Afonso

Aspirante a Oficial de Polícia

T: +351 938 551 732
E: pmafonso@psp.pt
XXXVI CFOP

policiasegurancapublica

POLÍCIA
SEGURANÇA PÚBLICA

Instituto Superior de Ciências Policiais e Segurança Interna

Rua 1º de Maio, nº 3, 1349-040 Lisboa
www.psp.pt

PT

Apêndice I – Testes de Normalidade

Tabela 15

Variável "Idade" - Kolmogorov-Smirnov e Shapiro-Willk

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Idade	Statistic	df	Sig.	Statistic	df	Sig.
CompCyber	Entre 18	,304	75	,000	,774	75	,000
	Entre 26	,270	86	,000	,825	86	,000
	Entre 36	,210	121	,000	,867	121	,000
	Entre 46	,228	102	,000	,869	102	,000
	Mais de	,230	21	,005	,731	21	,000
Atitudes	Entre 18	,220	75	,000	,796	75	,000
	Entre 26	,117	86	,006	,929	86	,000
	Entre 36	,134	121	,000	,896	121	,000
	Entre 46	,145	102	,000	,925	102	,000
	Mais de	,172	21	,104	,887	21	,020

Tabela 16

Variável "Carreira Atual" - Kolmogorov-Smirnov e Shapiro-Willk

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Carreira Atual	Statistic	df	Sig.	Statistic	df	Sig.
CompCyber	Agente d	,219	249	,000	,878	249	,000
	Chefe de	,279	100	,000	,829	100	,000
	Oficial	,215	56	,000	,880	56	,000
Atitudes	Agente d	,117	249	,000	,901	249	,000
	Chefe de	,138	100	,000	,877	100	,000
	Oficial	,112	56	,076	,927	56	,002

Apêndice J – Tabelas *Quick Rerence Guide* (Questões 52 e 53)

Tabela 17

Questão 52 – Quick Reference Guide

	N	%
Concordo totalmente	219	54,1
Concordo	182	44,9
Discordo	4	1,0
Discordo totalmente	0	0
Total	405	100,0

Tabela 18

Questão 53 – Quick Reference Guide

	N	%
Concordo totalmente	75	18,5
Concordo	310	76,5
Discordo	19	4,7
Discordo totalmente	1	,2
Total	405	100,0

Apêndice K – Material de apoio (SPSS)

Figura 7

Amostras independentes (Comportamentos e Faixas Etárias)– Teste Kruskal-Wallis

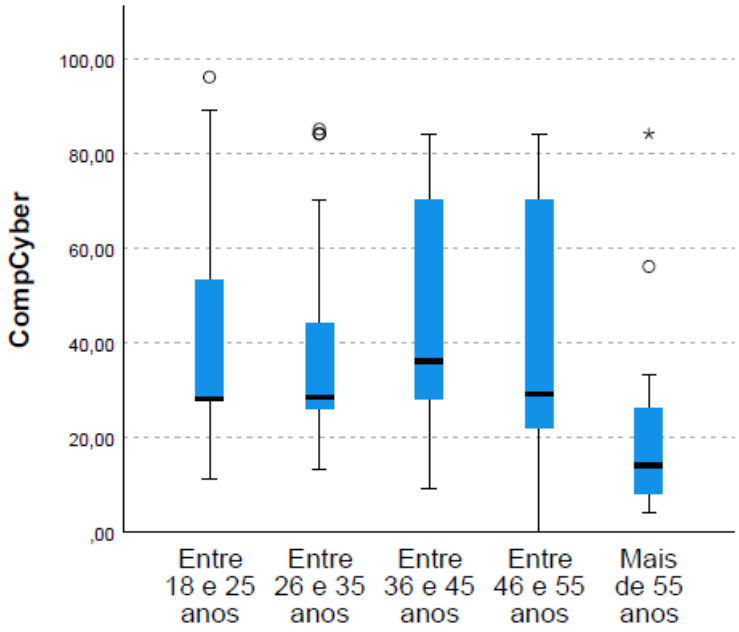


Tabela 19

Teste Kruskal Wallis - Ranks

	Idd	N	Mean Rank
CompCyber	Entre 18 e 25 anos	75	208,34
	Entre 26 e 35 anos	86	191,66
	Entre 36 e 45 anos	121	228,58
	Entre 46 e 55 anos	102	203,85
	Mais de 55 anos	21	78,81
	Total	405	
Atitudes	Entre 18 e 25 anos	75	246,43
	Entre 26 e 35 anos	86	229,25
	Entre 36 e 45 anos	121	176,74
	Entre 46 e 55 anos	102	175,60
	Mais de 55 anos	21	224,79
	Total	405	

Tabela 20

Teste Kruskal Wallis - Ranks

	Carreira Atual	N	Mean Rank
CompCyber	Agente de Polícia	249	204,22
	Chefe de Polícia	100	195,55
	Oficial de Polícia	56	210,87
	Total	405	
Atitudes	Agente de Polícia	249	202,96
	Chefe de Polícia	100	208,22
	Oficial de Polícia	56	193,88
	Total	405	

Tabela 21

Comparação entre pares – Variáveis "Comportamentos" e "Faixas Etárias"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.
Mais de 55 anos-Entre 26 e 35 anos	112,853	28,276	3,991	,000
Mais de 55 anos-Entre 46 e 55 anos	125,043	27,838	4,492	,000
Mais de 55 anos-Entre 18 e 25 anos	129,530	28,680	4,516	,000
Mais de 55 anos-Entre 36 e 45 anos	149,773	27,462	5,454	,000
Entre 26 e 35 anos-Entre 46 e 55 anos	-12,190	17,007	-,717	,474
Entre 26 e 35 anos-Entre 18 e 25 anos	16,677	18,354	,909	,364
Entre 26 e 35 anos-Entre 36 e 45 anos	-36,920	16,385	-2,253	,024
Entre 46 e 55 anos-Entre 18 e 25 anos	4,487	17,670	,254	,800
Entre 46 e 55 anos-Entre 36 e 45 anos	24,730	15,615	1,584	,113
Entre 18 e 25 anos-Entre 36 e 45 anos	-20,243	17,072	-1,186	,236