ABRIL 2022

ESTUDO SOBRE O ENSINO PÓS-SECUNDÁRIO E O ENSINO SUPERIOR DE CIBERSEGURANÇA EM PORTUGAL

OBSERVATÓRIO
DE CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

ABRIL 2022

ESTUDO SOBRE O ENSINO PÓS-SECUNDÁRIO E O ENSINO SUPERIOR DE CIBERSEGURANÇA EM PORTUGAL

OBSERVATÓRIO
DE CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

U.PORTO
FACULDADE DE PSICOLOGIA
E DE CIÊNCIAS DA EDUCAÇÃO
UNIVERSIDADE DO PORTO

CIIE
CENTRO DE INVESTIGAÇÃO & INTERVENÇÃO EDUCATIVAS

FCT
Fundação
para a Ciência
e a Tecnologia

ABRIL 2022

ESTUDO SOBRE O ENSINO PÓS-SECUNDÁRIO E O ENSINO SUPERIOR DE CIBERSEGURANÇA EM PORTUGAL

OBSERVATÓRIO DE CIBERSEGURANÇA

COORDENADORES
Amélia Veiga
Pedro Ferreira

EQUIPA
Marta Sampaio
José Pedro Amorim
João Moisés Cruz
Mariana Fonseca

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de Cibersegurança

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU

FICHA TÉCNICA

AUTORIA DO ESTUDO
Coordenadores:
Amélia Veiga
Pedro Ferreira

Equipa:
Marta Sampaio
José Pedro Amorim
João Moisés Cruz
Mariana Fonseca

TÍTULO
Estudo sobre o Ensino Pós-Secundário e o Ensino Superior em Portugal

EDIÇÃO
CIIE/FPCEUP (Universidade do Porto) e CNCS

DESIGN
Frederico Lencastre e CNCS

ÍNDICE

ABREVIATURAS

A3ES → Agência de Avaliação e de Acreditação do Ensino Superior

ANQEP → Agência Nacional para a Qualificação e o Ensino Profissional

CET → Cursos de Especialização Tecnológica

CNAEF → Classificação Nacional das Áreas de Educação e Formação

CNQ → Catálogo Nacional de Qualificações

CTeSP → Curso Técnico Superior Profissional

DET → Diploma de Especialização Tecnológica

DGEEC → Direção-Geral de Estatísticas da Educação e Ciência

DGES → Direção-Geral do Ensino Superior

ECTS → Sistema Europeu de Créditos Curriculares

EFA → Cursos de Educação e Formação de Adultos

QNQ → Quadro Nacional de Qualificações

RENATES → Registo Nacional de Teses e Dissertações

RGPD → Regulamento Geral sobre a Proteção de Dados

UC → Unidades Curriculares

UFCD → Unidades de Formação de Curta Duração

SUMÁRIO EXECUTIVO

O *Estudo sobre o Ensino Pós-secundário e o Ensino Superior de Cibersegurança em Portugal* caracteriza os cursos em cibersegurança e a implantação de conteúdos de cibersegurança em cursos e ciclos de estudo da área das Ciências Informáticas.

O estudo incide sobre a análise dos objetivos, conteúdos e os resultados de aprendizagem dos cursos e ciclos de estudo de cibersegurança e identifica o número de estudantes a frequentar, diplomados/as e a evolução do número, bem como o registo numa área científica das dissertações de mestrado e teses de doutoramento, ao longo dos últimos 10 anos. Com uma vocação exploratória, o Estudo analisa também as perspetivas dos diretores dos cursos e dos ciclos de estudo de nível superior sobre as componentes da formação técnica, ética e legal, as necessidades do mercado de trabalho e os desafios que se colocam à formação na área de cibersegurança ao nível da investigação e inovação.

DESTAQUES

Considerando o número de Cursos de Especialização Tecnológica (CET) do ensino pós-secundário com conteúdos específicos de cibersegurança, implantados na área das Ciências Informáticas, verifica-se que, em 2021, os 3 CET existentes deste caráter são oferecidos por 13 entidades distintas e em 37 locais diferentes por todo o país, ainda que com um maior registo na Região Centro, e em seguida na Região Sul. Nestes cursos, identificaram-se 3 Unidades de Formação de Curta Duração (UFCD) com referência à cibersegurança e/ou segurança informática. No que toca a cursos da área de cibersegurança, verifica-se a existência de um CET, em 2021, oferecido por 5 entidades diferentes e em 11 locais distintos, com especial incidência na Região Norte e Centro do país. Neste CET, foram identificadas 10 Unidades de Formação de Curta Duração (UFCD) de cibersegurança, ou com conteúdos especialmente relacionados, e uma transversalidade manifesta destes conteúdos relativamente às UFCD gerais.

No ensino superior foram identificados 246 cursos não conferentes de grau (CTeSP) e ciclos de estudo na área científica de Ciências Informáticas. Destes 246 cursos, 109 cursos e ciclos de estudo (37 CTeSP, 26 Licenciaturas, 33 Mestrados e 3 Doutoramentos) contêm, nos seus planos de estudo, unidades curriculares com conteúdos diretamente relacionados com a cibersegurança e/ou segurança de informação. A formação universitária concentra-se no norte do país e a formação politécnica abrange todo o território nacional. No total, foram identificadas 147 unidades curriculares com conteúdos de cibersegurança nos planos de estudo dos 109 cursos/ciclos de estudo. O número total de inscritos/as nestes cursos/ciclos de estudo, em 2020/2021, é de 7707 (6583 homens e 1124 mulheres), 1287 frequentam os CTeSP, 5024 as Licenciaturas, 1140 os Mestrados e 256 os Doutoramentos. Quanto ao número de diplomados/as, no ano letivo de 2019/2020, era de 1498 estudantes diplomados/as (1267 homens e 231 mulheres), sendo que 412 se diplomaram em CTeSP, 574 em Licenciaturas, 493 em Mestrados e 19 em Doutoramentos.

Em Portugal, especificamente da área de cibersegurança e/ou segurança de informação, em 2021, existem 20 cursos/ciclos de estudo (9 CTeSP, 1 licenciatura, 9 mestrados e 1 doutoramento). Nestes cursos, em 2020/2021, estavam inscritos/as 718 estudantes (654 homens e 58 mulheres) e, em 2019/2020, diplomaram-se 152 estudantes (137 homens e 13 mulheres). No que diz respeito ao número de dissertações de mestrado e de teses de doutoramento em curso ou concluídas, na área de cibersegurança, foram identificados 337 registos, entre 2003 e 2021.

A relevância da área científica de Ciências Informáticas na estrutura curricular dos 20 cursos/ciclos de estudo da área de cibersegurança é preponderante e as áreas científicas com menos expressão são as Línguas, o Direito e a Gestão. No que se refere às teses de doutoramento e às dissertações de mestrado, o seu registo em áreas científicas e tecnológicas diversifica-se, abrangendo, por exemplo, a Ciência Política e Cidadania, o Direito, a Gestão e Administração.

Relativamente às perceções dos diretores de cursos/ciclos de estudos destaca-se: (i) a ideia de que a componente da ética e do direito é desenvolvida numa perspetiva de aplicação prática, em articulação com o que é visto como uma necessidade do mercado de trabalho; (ii) os CTeSP e Licenciaturas respondem às necessidades percebidas no mercado de trabalho por parte das escolas, no entanto, as empresas/organizações nem sempre revelam um nível de consciencialização muito elevado relativamente à necessidade de cibersegurança; (iii) a componente de investigação e inovação é mais forte nos mestrados e doutoramento, dada a natureza destas formações.

Considera-se que as conclusões deste Estudo podem contribuir para o desenvolvimento de uma estratégia de formação em cibersegurança, ancorada, no entanto, na necessidade de melhorar a qualidade de informação pública disponível sobre os conteúdos dos cursos e dos ciclos de estudo. Este último aspeto, é crucial para a identificação da presença da cibersegurança e/ou segurança informática em cursos e ciclos de estudos de áreas científicas distintas das de Ciências Informáticas. De facto, o registo de dissertações de mestrado e de teses de doutoramento, abrangendo um vasto leque de áreas científicas, sugere a presença da cibersegurança em ciclos de estudo noutras áreas científicas para além das Ciências Informáticas.

INTRODUÇÃO

Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 assume como objetivos estratégicos: (i) maximizar a resiliência, (ii) promover a inovação e (iii) gerar e garantir recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço. No âmbito da estratégia europeia para a cibersegurança, as lacunas nas competências em cibersegurança, bem como o reforço da investigação e da inovação neste domínio, têm vindo a ganhar importância. Neste sentido, a articulação das estratégias europeia e nacional permitiram definir uma orientação traduzida em seis eixos de intervenção, entre os quais, no âmbito deste estudo, se destacam dois: prevenção, educação e sensibilização, e da investigação, desenvolvimento e inovação, nos quais o estudo, sobre o ensino pós-secundário e o ensino superior na área temática da cibersegurança em Portugal, se inclui.

Assim, com o objetivo de ajudar a traçar o panorama tanto no que diz respeito à formação dirigida a profissionais ou futuros profissionais em cibersegurança, como a outros profissionais que se cruzam com a área temática da cibersegurança, sobretudo através de disciplinas específicas, no seu percurso formativo, foram identificados, analisados e caracterizados os cursos de especialização tecnológica, de nível pós-secundário não superior, os cursos de técnico superior profissional de ensino superior e os ciclos de estudo conferentes de grau, em Portugal.

Dando continuidade e aprofundando o trabalho realizado no *Relatório Cibersegurança em Portugal - Sociedade 2021*, do Observatório de Cibersegurança, este estudo visou os seguintes objetivos:

1. Identificar no ensino pós-secundário os Cursos de Especialização Tecnológica na área de cibersegurança e cursos que tenham UFCD da área de cibersegurança nos planos de estudo;

2. Caracterizar os cursos e ciclos de estudo de cibersegurança de nível pós-secundário e superior, tendo em conta os objetivos, conteúdos e os resultados de aprendizagem e a implantação dos conteúdos de cibersegurança nos cursos e ciclos de estudo da área científica de Ciências Informáticas;

3. Identificar os cursos/ciclos de estudo de nível superior de cibersegurança, incluindo número de estudantes a frequentar, diplomados/as e evolução do número e registo numa área científica das dissertações de mestrado e teses de doutoramento, ao longo dos últimos 10 anos;

4. Analisar as perspetivas dos diretores dos cursos e dos ciclos de estudo de cibersegurança sobre as componentes da formação técnica, ética e legal, as necessidades do mercado de trabalho e os desafios que se colocam à formação na área temática de cibersegurança ao nível da investigação e inovação.

Com vocação exploratória e de reconhecimento do lugar que a educação e formação nesta área ocupa no sistema educativo português, o estudo parte do que é possível saber-se a partir de informação pública (e.g., Direção-Geral do Ensino Superior [DGES], Direção-Geral de Estatísticas da Educação e Ciência [DGEEC], Agência de Avaliação e de Acreditação do Ensino Superior [A3ES], Agência Nacional para a Qualificação e o Ensino Profissional [ANQEP], Catálogo Nacional de Qualificações, *websites* de instituições de ensino superior), procurando também integrar uma perspetiva que ajude a ler as tendências e a projetar o futuro.

Em linha com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, o estudo possibilitará a construção de uma imagem situada da educação e formação na área temática de cibersegurança em Portugal, contribuindo para a consciencialização sobre a necessidade de alargar e reforçar as competências e os conhecimentos em cibersegurança na educação e formação de professores/as, estudantes e de diversos atores da sociedade.

Uma análise mais aprofundada obrigou a olhar para os cursos de nível pós-secundário, bem como para os conteúdos das unidades curriculares e para os resultados de aprendizagem dos cursos de ensino superior na área temática de cibersegurança. Um conhecimento e reconhecimento situado implicou também a análise das perspetivas que agentes-chave têm relativamente à área de formação e à profissão no contexto atual em Portugal. Neste estudo, foi dada preferência a atores institucionais que, pelas posições que ocupam, se espera que tenham acesso a visões e perspetivas coletivas e de representação. Assim, foram privilegiados, enquanto interlocutores, os/as diretores/as de ciclos de estudo e de cursos oferecidos pelas instituições de ensino superior.

Este Relatório está organizado em três partes. Na primeira, faz-se a caracterização da formação em cibersegurança de nível pós-secundário, incluindo os CET com referência a conteúdos da área de cibersegurança, presentes em cursos da área das Ciências Informáticas. A distribuição geográfica dos cursos, as componentes de aprendizagem, os objetivos e os conteúdos da formação são também descritos.

No que diz respeito ao ensino superior, na segunda parte, os ciclos de estudo e os cursos de cibersegurança são analisados, tendo em consideração também a área das Ciências Informáticas, e são descritos em função do número de inscritos/as e diplomados/as e da evolução do número de dissertações de mestrado e de teses de doutoramento em cibersegurança, nos últimos 10 anos.

Por último, a caracterização dos cursos em cibersegurança oferecidos pelas instituições de ensino superior é feita com base na sua estrutura curricular, no plano de estudos, nos objetivos do curso e nos resultados de aprendizagem das unidades curriculares. As componentes de formação técnica, ética e legal, do mercado de trabalho, e da investigação e inovação orientaram o conhecimento situado da cibersegurança na formação superior em Portugal, mobilizando as perspetivas dos diretores de cursos sobre estas mesmas componentes.

No final do relatório, inclui-se uma nota sobre a metodologia desenvolvida que, de forma articulada e complementar, permitiu a prossecução dos diferentes objetivos do estudo.

CARACTERIZAÇÃO DOS CURSOS DE CIBERSEGURANÇA DE NÍVEL PÓS-SECUNDÁRIO E A SUA IMPLANTAÇÃO NA ÁREA DAS CIÊNCIAS INFORMÁTICAS

MARIANA FONSECA
JOSÉ PEDRO AMORIM
PEDRO FERREIRA

Cursos de Especialização Tecnológica em Ciências Informáticas

A pesquisa de Cursos de Especialização Tecnológica (CET) foi feita a partir da base de dados da Direção-Geral do Ensino Superior (DGES), onde são referidos todos os CET existentes em Portugal, de todas as áreas. Com base nas palavras-chave "cibersegurança"; "segurança informática"; "segurança de informação"; "segurança de redes" e "sistemas de informação" (ver nota metodológica), verificou-se que a área a aparecer mais frequentemente foi a de Ciências Informáticas. Assim, optou-se pela análise de cursos de cibersegurança e cursos com Unidades de Formação de Curta Duração (UFCD) e/ou conteúdos referentes à área da cibersegurança e segurança informática. No universo dos cursos da área das Ciências Informáticas identificaram-se 3 CET com conteúdos da área de cibersegurança e segurança informática. Estes mesmos 3 CET - Aplicações Informáticas de Gestão; Gestão de Redes e Sistemas Informáticos; e Tecnologias e Programação de Sistemas de Informação - são oferecidos por diferentes entidades formadoras, tendo sido contabilizadas um total de 37 ocorrências destes cursos (como se contabiliza na tabela 1) em diferentes locais espalhados pelo país.

Tratam-se, portanto, de 3 cursos diferentes oferecidos por 13 instituições distintas[1] e lecionados em vários locais de 12 distritos de Portugal (ver tabela 1 e figura 1). Em termos geográficos, é na região Centro que, notoriamente, se encontra a maior parte da oferta formativa, com o distrito da Guarda, e as suas 11 ocorrências, a destacar-se de forma clara. Com menos incidência, mas ainda com algum destaque, temos a Região Sul que aparece com 9 ocorrências, sendo que 6 delas se encontram no distrito de Lisboa. Já na Região Norte, observa-se uma menor presença, com os distritos do Porto e de Aveiro a registarem apenas 3 ocorrências cada.

Formação	Instituição	Local / Locais
Aplicações Informáticas de Gestão (2)	FORESP – Associação para a Formação e Especialização Tecnológica (Escola Tecnológica de Vale de Cambra)	Arouca, Vale de Cambra
Gestão de Redes e Sistemas Informáticos (18)	ATEC – Associação de Formação para a Indústria	Palmela
	Centro de Emprego e Formação Profissional de Beja	Beja
	Centro de Emprego e Formação Profissional de Lisboa	Lisboa
	Centro de Emprego e Formação Profissional de Setúbal e do Seixal	Setúbal, Seixal
	CITEFORMA – Centro de Formação Profissional dos Trabalhadores de Escritório, Comércio, Serviços e Novas Tecnologias	Lisboa
	ENTA – Escola de Novas Tecnologias dos Açores	Ponta Delgada
	FORESP – Associação para a Formação e Especialização Tecnológica (Escola Tecnológica de Vale de Cambra)	Vale de Cambra
	INOVINTER – Centro de Formação e de Inovação Tecnológica	Covilhã
	NOVOTECNA – Associação para o Desenvolvimento Tecnológico	Aveiro, Águeda, Castelo Branco, Coimbra, Covilhã, Guarda, Leiria, Seia, Viseu

[1] O curso Aplicações Informáticas de Gestão, no entanto, é apenas promovido pela FORESP.

Tecnologias e Programação de Sistemas de Informação (17)	AFTEBI – Associação para a Formação Tecnológica e Profissional da Beira Interior	Covilhã, Fundão, Guarda
	ATEC – Associação de Formação para a Indústria	Porto
	Centro de Emprego e Formação Profissional de Évora	Évora
	Centro de Emprego e Formação Profissional de Sintra	Sintra
	CINEL – Centro de Formação Profissional da Indústria Eletrónica, Energia, Telecomunicações e Tecnologias da Informação	Lisboa
	CITEFORMA – Centro de Formação Profissional dos Trabalhadores de Escritório, Comércio, Serviços e Novas Tecnologias	Lisboa
	NOVOTECNA – Associação para o Desenvolvimento Tecnológico	Aveiro, Águeda, Castelo Branco, Coimbra, Covilhã, Guarda, Leiria, Seia, Viseu

Tabela 1: CET que incluem conteúdos de cibersegurança; entidades promotoras e locais de funcionamento
Fonte: Lista CET (DGES, 2021) disponível em: https://www.dges.gov.pt/pt/pagina/cursos-de-especializacao-tecnologica-cet

Figura 1: Distribuição geográfica da oferta dos CET que incluem UFCD/conteúdos de cibersegurança.

No Catálogo Nacional de Qualificações (CNQ), fonte privilegiada para consulta dos CET, encontram-se os planos de estudos dos cursos, juntamente com as informações das UFCD que neles são incluídas. No plano de estudos destes três CET, foram identificadas três UFCD com conteúdos referentes à área da cibersegurança ou da segurança informática, são elas: 5109 "Políticas de Segurança"; 5079 "Políticas de Segurança dos Sistemas Informáticos e de Redes"; e 5419 "Seguranças em Sistemas Informáticos". Assim, procedeu-se à análise dos seus objetivos e conteúdos programáticos, de forma a entender a presença da cibersegurança e segurança informática nos CET da área de Ciências Informáticas (ver tabela 2).

UFCD	Objetivos	Conteúdos
5109 "Políticas de segurança"	• Definir e analisar as exigências de segurança de um sistema informático. • Implementar uma estratégia de segurança para uma arquitetura cliente/servidor.	(…) • Proteção de dados armazenados (Criptografia) • Proteção da transmissão de dados (…) • Planificação para a implementação da segurança • Cópias de Segurança • Ameaças externas
5079 "Políticas de Segurança dos Sistemas Informáticos e de Redes"	• Definir os princípios da arquitetura cliente/servidor. • Estabelecer ligações com servidores remotos. • Definir e aplicar políticas de segurança. • Definir e aplicar estratégias coerentes de cópias de segurança de dados.	(…) • Proteção de dados armazenados (Criptografia) • Proteção da transmissão de dados • Planificação para a implementação da segurança • Cópias de Segurança • Ameaças externas
5419 "Seguranças em Sistemas Informáticos"	• Identificar as noções básicas de segurança e os diferentes aspetos relacionados com as mesmas. • Interpretar tráfego de rede utilizando ferramentas de monitorização apropriadas e identificar anomalias decorrentes de ataques ou tentativas de ataques. • Definir e implementar um processo de segurança em redes.	• Conceitos gerais sobre segurança da informação • Vulnerabilidades, ameaças e ataques • Políticas de segurança e mecanismos de segurança • Segurança em sistemas distribuídos (…)

Tabela 2: Apresentação dos objetivos e conteúdos programáticos das UFCD destacadas
Fonte: https://catalogo.anqep.gov.pt/[2]

Observando o plano geral destas três UFCD, percebe-se que existe um foco na implementação da segurança informática, através de políticas de segurança, como sugerem as suas designações. Todavia, é de notar, ainda, a importância da gestão dos processos informáticos para que essas políticas e estratégias possam ser aplicadas, como se verifica na UFCD 5109 "Políticas de segurança". A questão da proteção de dados verifica-se fulcral, acrescentando a importância das cópias de segurança (UFCD 5109 "Políticas de segurança" e 5079 "Políticas de Segurança dos Sistemas Informáticos e de Redes") e das vulnerabilidades na perspetiva do combate, monitorização e prevenção, e da implementação de processos de segurança (UFCD 5419 "Seguranças em Sistemas Informáticos"). Todas estas UFCD, que podem ser incluídas nos planos curriculares de vários CET, possuem uma relação direta com a cibersegurança e a segurança informática.

[2] Trata-se, em bom rigor, de informação citada da fonte referida. Dispensamos o uso de aspas apenas para facilitar a leitura.

Curso de Especialização Tecnológica de cibersegurança

Integrado na área das Ciências Informáticas, há um CET da área de cibersegurança que é promovido por 5 entidades distintas, em 11 locais diferentes (ver tabela 3 e figura 2), o que, em relação ao ano de 2020, representa o surgimento de uma nova oferta deste curso, em Tomar, promovida pelo Centro de Emprego e Formação Profissional do Médio Tejo, como se apresenta no *Relatório Cibersegurança em Portugal - Sociedade 2021*, do Observatório de Cibersegurança.

Formação	Instituição	Local / Locais
Cibersegurança	ATEC – Associação de Formação para a Indústria	Palmela
Cibersegurança	Centro de Emprego e Formação Profissional de Coimbra	Coimbra
Cibersegurança	Instituto Profissional de Tecnologias Avançadas para a Formação, Lda	Porto
Cibersegurança	NOVOTECNA – Associação para o Desenvolvimento Tecnológico	Águeda, Aveiro, Castelo Branco, Coimbra, Covilhã, Guarda, Leiria, Seia e Viseu
Cibersegurança (NOVO)	Centro de Emprego e Formação Profissional do Médio Tejo	Tomar

Tabela 3: Oferta de CET de Cibersegurança em Portugal em 2021
Fonte: Lista CET (DGES, 2021) disponível em: Cursos de Especialização Tecnológica – CET | DGES

Não deixa de ser curioso, todavia, o aparecimento de mais uma entidade promotora do CET de cibersegurança na Região Centro. Mais uma vez, esta região destaca-se claramente, neste caso, como aquela em que há mais oferta deste CET, em 11 locais distintos. Na Região Norte e na Região Sul, este curso existe em apenas um local de cada Região. Os distritos com mais ocorrências são os de Aveiro, Castelo Branco, Coimbra e Guarda, com 2 locais cada. Os distritos de Leiria, Porto, Santarém, Setúbal e Viseu têm esta oferta formativa em apenas um local. De registar que o distrito de Lisboa, onde se concentram diversos serviços e instituições governativas, não regista nenhum CET nesta área (ver figura 2), contrariamente ao que se verificou na análise do CET de Ciências Informáticas com conteúdos de cibersegurança.

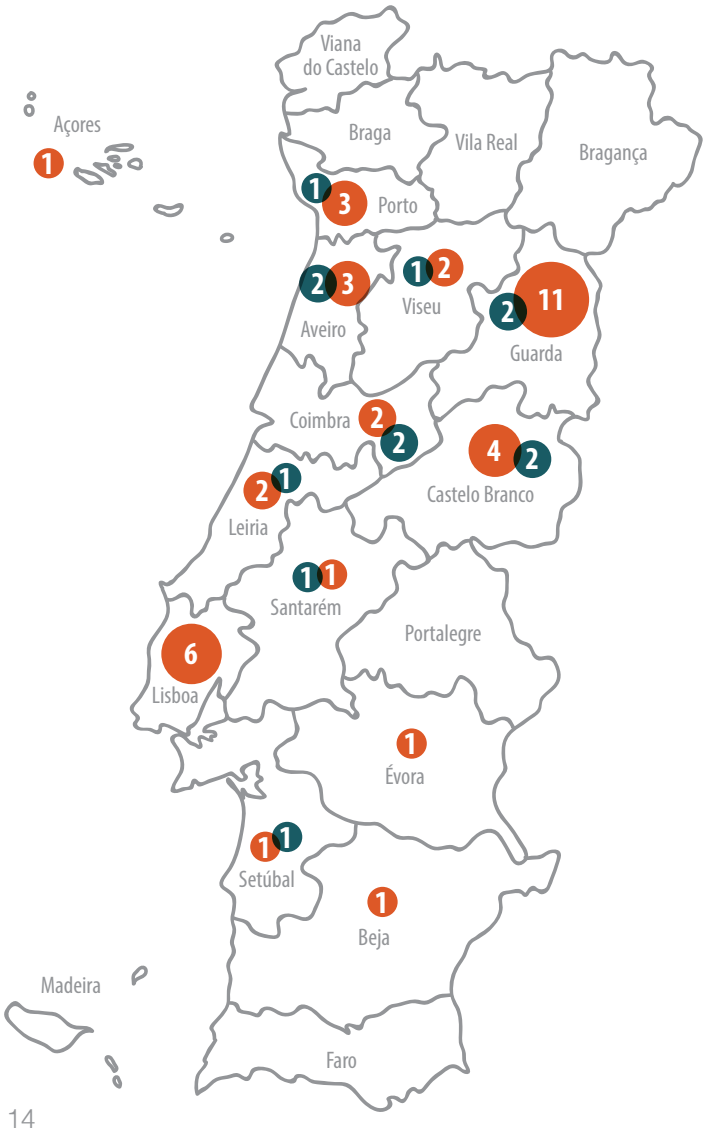


Figura 2:
- Distribuição geográfica da oferta dos CET que incluem UFCD/conteúdos de cibersegurança.
- Distribuição geográfica dos CET de cibersegurança.

Semelhante aos CET anteriores, o CNQ apresenta o plano de estudos do CET de cibersegurança, juntamente com as informações das UFCD planeadas. Tendo isto em consideração, o Curso de Técnico/a Especialista em Cibersegurança, com o código 481344, apresenta um programa com três componentes de aprendizagem: as competências escolares, as competências profissionais e a formação em contexto de trabalho. Na tabela 3, apresentam-se as competências escolares e profissionais, assim como os pontos de créditos associados às UFCD que delas fazem parte. No que diz respeito às competências escolares, estas agregam quatro UFCD de formação geral e científica que, no seu total, somam 15 pontos de créditos. Já nas competências profissionais, estão presentes 22 UFCD de caráter técnico-prático e mais ligadas à área da cibersegurança propriamente dita, sendo que 10 dessas UFCD foram alvo de análise (ver UFCD destacadas a negrito na tabela 4) precisamente por contemplarem, na sua designação ou nos conteúdos programáticos, a cibersegurança. Além disso, é de referir que, neste conjunto alargado de UFCD, se observa uma maior atribuição de pontos de crédito em 8 dessas UFCD, agregando 4,50 pontos de crédito cada. Por fim, e também apresentada no CNQ, há ainda a formação em contexto de trabalho que se baseia numa aplicação dos conhecimentos adquiridos, tendo como objetivo:

> *"(...) aplicar conhecimentos e saberes adquiridos às atividades práticas do respetivo perfil profissional e executar atividades sob orientação, utilizando as técnicas, os equipamentos e os materiais que se integram nos processos de produção de bens ou de prestação de serviços."*
>
> (ANQEP, Técnico/a Especialista em Cibersegurança[3]).

Competências	UFCD (código e designação)	Peso (pontos de crédito)
Competências Escolares	5064 "Matemática"	15
	0683 "Ética e deontologia profissionais"	
	3769 "Probabilidades e estatística"	
	5065 "Empresa – Estruturas e funções"	
Competências Profissionais[4]	5117 "Primeiros conceitos de programação e algoritmia e estruturas de controlo num programa informático"	2,25
	9187 "Legislação, segurança e privacidade"	2,25
	5745 "Inglês Técnico"	4,50
	5089 "Programação - Algoritmos"	2,25
	5410 "Bases de dados - Conceitos"	2,25
	5113 "Sistema operativo cliente (plataforma proprietária)"	2,25
	5114 "Sistema operativo servidor (plataforma proprietária)"	2,25
	5101 "Hardware e redes de computadores"	2,25
	5102 "Redes de Computadores (avançado)"	2,25
	5104 "Instalação de redes locais"	4,50
	5106 "Serviços de rede"	2,25
	5892 "Modelos de gestão de redes e de suporte a clientes"	2,25
	9188 "Fundamentos de Cibersegurança"	2,25

[3] https://catalogo.anqep.gov.pt/qualificacoesDetalhe/1587
[4] Destaque a negrito as UFCD que foram alvo de análise.

	9189 "Tecnologias de análise de evidências"	4,50
	9190 "Introdução à programação aplicada à Cibersegurança"[5]	2,25
	9191 "Introdução às técnicas de análise de evidências"	4,50
	9192 "Análise de vulnerabilidades – iniciação"	4,50
	9193 "Análise de vulnerabilidades – desenvolvimento"	4,50
	9194 "Introdução à Cibersegurança e à ciberdefesa"	4,50
	9195 "Enquadramento operacional da Cibersegurança"	4,50
	9196 "Cibersegurança ativa"	4,50
	9197 "*Wargamming*"	4,50

Tabela 4: Descrição do plano de estudos do CET de cibersegurança
Fonte: Técnico/a Especialista em Cibersegurança

Para aprofundar a análise, importa olhar para os objetivos e conteúdos programáticos das dez UFCD destacadas (ver tabela 4). Percebe-se, desde logo, que há UFCD que parecem ter um foco mais geral e outras um mais específico. Assim, as UFCD 9188 "Fundamentos de Cibersegurança" e 9194 "Introdução à Cibersegurança e à ciberdefesa" propõem uma abordagem geral ao tema, enquanto as restantes – 9187 "Legislação, segurança e privacidade", 9189 "Tecnologias de análise de evidências", 9191 "Introdução às técnicas de análise de evidências", 9192 "Análise de vulnerabilidades - iniciação", 9193 "Análise de vulnerabilidades - desenvolvimento", 9195 "Enquadramento operacional da Cibersegurança", 9196 "Cibersegurança ativa" e 9197 "*Wargamming*" – focam aspetos mais concretos ou aplicados à prática.

UFCD	Objetivos	Conteúdos programáticos
9187 "Legislação, segurança e privacidade"	• Identificar os conceitos fundamentais de direitos, liberdades e garantias, internacionais e nacionais. • Identificar legislação nacional e comunitária de proteção de dados (LPDP). • Interpretar a legislação nacional sobre manuseamento de informação classificada (SEGNAC). • Interpretar a legislação nacional sobre cibercriminalidade.	• Princípios da Declaração Universal dos Direitos Humanos • Direito de imagem • Princípios da Carta dos Direitos Fundamentais da União Europeia aplicados à Cibersegurança (…) • Conceitos de privacidade, dados pessoais e dados sensíveis • Conceitos nacionais e comunitários em matéria de administração eletrónica e proteção de dados: – Direito de informação – Direito de acesso – Direito de oposição – Direito de retificação e eliminação – Código de Procedimento Administrativo • Conceitos de cibercrime • Conceitos de competências de investigação criminal em cibercriminalidade

[5] Apesar de esta UFCD mencionar "cibersegurança" na sua designação, ela não foi explorada da mesma forma que as restantes, uma vez que se verificou que os seus conteúdos programáticos estão sobretudo ligados à programação e não especificamente à cibersegurança ou à segurança informática.

9188 "Fundamentos de Cibersegurança"	• Identificar os fundamentos da cibersegurança. • Reconhecer os diferentes tipos de ameaças cibernéticas. • Reconhecer o perfil e a motivação dos ataques cibernéticos. • Desenvolver mecanismos de proteção do local de trabalho face aos diferentes tipos de malware.	• Ameaças cibernéticas (…) • Mercado negro da internet • *Spam* e *phishing* • Classes populares de malware: – *Bankers* (PC, dispositivos móveis, pontos de venda, ATM) – *Mobile* – *Exploits* – *Ransoms* – *Spies* • Técnicas modernas de distribuição de ameaça • Armas cibernéticas – ameaças avançadas persistentes (APT) e ameaças industriais • Segurança contra ameaças cibernéticas no posto de trabalho
9189 "Tecnologias de análise de evidências"	• Identificar as fontes de informação mais relevantes usadas na análise de evidências para os principais tipos de incidentes. • Reconhecer a alto nível expressões regulares e sua representação nas linguagens mais comuns de *scripting*. • Identificar a estrutura e propriedades dos elementos de informação relevantes a extrair dessas fontes de informação. (…) • Identificar as principais fontes de informação pública sobre vulnerabilidades, reputação e ameaças. (…) • Reconhecer a alto nível o funcionamento de sistemas *Security Information and Event Management* SIEM.	(…) • Fontes públicas de informação sobre IPs e sua reputação • Fontes de informação sobre vulnerabilidades em formato CVE (*Common Vulnerabilities and Exposures*) • Arquitetura e funcionamento para análise de evidências: – *SyslogNG* – *LogStash* – *Splunk* – ESPER – OSSIM • Deteção e análise de BOTNETs usados em ataques "*brute force*"
9191 "Introdução às técnicas de análise de evidências"	• Elaborar *scripts*, utilizando uma linguagem moderna de *scripting*, de extração, filtragem e normalização de informação de logs aplicacionais e de sistema. (…) • Reconhecer e validar endereços de email com autenticação. • Reconhecer, resolver e normalizar URLs, domínios e IPs ou ranges de IPs (v4 e v6). (…)	(…) • Tipos mais comuns de codificação de *strings* em *logs* (…) • Introdução a outras bibliotecas relevantes e sua aplicação em cibersegurança (…)

9192 “Análise de vulnerabilidades – iniciação”	• Identificar o conjunto de vulnerabilidades *web* inventariadas pelo *Open Web Application Security Project* (OWASP). • Identificar as técnicas mais comuns na deteção de vulnerabilidades OWASP. • Ler *scripts* simples em *JavaScript* e PHP e analisar falhas de segurança. • Utilizar ferramentas de busca e análise de vulnerabilidades OWASP e interpretar os resultados obtidos.	• As top 10 vulnerabilidades *Web* inventariadas pelo *Open Web Application Security Project* (OWASP) (...) • Análise de *scripts JavaScript* com vulnerabilidades • Análise de *scripts* PHP com vulnerabilidades (...) • Utilização do ZAP e *OpenVAS* na descoberta e análise de vulnerabilidades em *websites*
9193 “Análise de vulnerabilidades – desenvolvimento”	• Identificar as boas práticas de segurança na configuração e gestão de sistemas de rede e de IT e seus protocolos operacionais. • Identificar vulnerabilidades em equipamentos de rede. • Identificar vulnerabilidades em servidores Linux/Unix e Windows. • Interpretar o dicionário público “CVE” (*Common Vulnerabilities and Exposures*) com informação de referência sobre vulnerabilidades conhecidas. • Aplicar as técnicas, baseadas em agentes, na deteção de vulnerabilidades de segurança em servidores Linux/Unix e Windows. • Aplicar as técnicas, baseadas em sondas de rede, na descoberta de vulnerabilidades de segurança em equipamentos de rede e servidores Linux/Unix e Windows. • Utilizar as ferramentas de busca e análise de vulnerabilidades em redes e servidores e interpretar os resultados obtidos.	• Introdução às boas práticas gerais na configuração e gestão de plataformas de rede e IT • Ferramentas de deteção e gestão de vulnerabilidades (...) • Configuração e gestão de plataformas de rede: – Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE – Segurança na sua configuração e gestão – Aplicação de *scans* NESSUS (...)
9194 “Introdução à Cibersegurança e à ciberdefesa”	• Identificar e caracterizar as componentes tangíveis e intangíveis do ciberespaço. • Identificar as potenciais ciberameaças e os riscos individuais. • Identificar as boas práticas associadas à cibersegurança e à ciberdefesa. • Identificar a natureza transversal das ciberameaças e o seu impacto global.	• Introdução ao ciberespaço e terminologia • Impacto e boas práticas individuais de cibersegurança – Desktop e *web* • Regulação e enquadramento legal do ciberespaço – Lei do cibercrime – Leis internacionais – Conflitos armados no ciberespaço • Impacto e boas práticas de segurança das redes sociais

9194 "Introdução à Cibersegurança e à ciberdefesa"	• Caracterizar os constrangimentos operacionais decorrentes do enquadramento legal aplicável à cibersegurança (direito nacional) e ciberdefesa (direito internacional). • Reconhecer a importância da ciberdefesa das organizações tanto numa perspetiva nacional como internacional. • Identificar as políticas de cibersegurança e ciberdefesa. • Reconhecer as potenciais ameaças cibernéticas e riscos para as organizações. • Identificar as responsabilidades do indivíduo e o seu papel enquanto agente ativo da cibersegurança e ciberdefesa das organizações.	• Estratégia Nacional de cibersegurança e de ciberdefesa • Cibersegurança em operações militares e ciberdefesa • Compreensão e avaliação do ambiente da ameaça cibernética (…) • Gestão dinâmica do risco • Política de cibersegurança das organizações • Finalidade e nível de ambição • Objetivos a atingir • Linhas de ação e definição de prioridades • Controlo de execução e alinhamento das ações a desenvolver.
9195 "Enquadramento operacional da Cibersegurança"	• Identificar ameaças à cibersegurança. • Comparar ferramentas de autenticação. • Utilizar sistemas de deteção de intrusão. • Identificar e utilizar a criptografia e assinaturas digitais. • Descrever os fundamentos da segurança da rede. • Distinguir o *hacking* do *hacking* ético.	• Segurança da informação: – Relatórios de ameaças de segurança – Vulnerabilidades *web* mais relevantes – Terminologias comuns – Elementos de segurança da informação – Estatísticas relacionadas com a segurança – Ataque em *sites* de redes sociais para roubo de identidade (…) • Criptografia • Servidores e aplicações *web* • Redes wireless • Sistema de deteção de intrusão • Ciclo *hacking* • *Hacking* ético • Segurança na rede: – Mapeamento internet protocol para OSI – Ameaças de segurança sobre uma rede – Políticas de segurança de rede • Segurança nos protocolos de rede
9196 "Cibersegurança ativa"	• Descrever a resposta a incidentes na informática forense. • Identificar evidências digitais. • Utilizar ferramentas de análise e recolha de *logs* e mecanismos de salvaguarda. • Identificar evidências de incidentes informáticos • Elaborar relatórios de investigação forense	• Redes privadas virtuais: – Virtual Private Network (VPN) – Caraterísticas – Segurança – Introdução ao *Internet Protocol Security* (IPSec) – Serviços IPSec – A combinação de VPN e Firewalls – Vulnerabilidades VPN • Segurança de redes wireless • Segurança de voz sobre IP (…)

9197 "*Wargamming*"	• Desenvolver os procedimentos de segurança de informação de acordo com o tipo de ameaças e incidentes. • Caracterizar os diferentes tipos de operações em redes de computadores no contexto da cibersegurança e ciberdefesa. • Instalar e parametrizar ferramentas destinadas a garantir a cibersegurança e a ciberdefesa em contexto de ambiente de simulação virtual (*Cyber Range*).	• Aspetos diferenciadores da cibersegurança e ciberdefesa • Impacto estratégico e operacional das ciberameaças • Operações em redes de computadores: – Defesa – Ataque – Exploração • Identificação de dados críticos para as organizações • A cadeia de ataque (*KillChain*) • Articulação entre defesa e ataque: – Prevenir – Detetar – Responder • Conhecimento das redes da organização • Defesa em profundidade • Definição de métricas • Desenvolvimento de cenários de cibersegurança e ciberdefesa – Construção de narrativas de acontecimentos – Identificação de incidentes associados a uma situação de crise – Identificação de objetivos e possíveis audiências de treino • Enquadramento da utilização de exercícios de simulação ("*Capture the Flag*" e "*Red and Blue*")

Tabela 5: Apresentação dos objetivos e conteúdos programáticos das UFCD destacadas
Fonte: Técnico/a Especialista em Cibersegurança[6]

Não obstante, há uma transversalidade inequívoca de alguns tópicos. As questões legais, por exemplo, surgem na UFCD 9187 "Legislação, segurança e privacidade", que lhes é especificamente dedicada, e na UFCD 9194 "Introdução à Cibersegurança e à ciberdefesa", que se refere à regulação e ao enquadramento legal do ciberespaço, bem como da política de ciberdefesa das organizações – e 9195 "Enquadramento operacional da Cibersegurança", que inclui as políticas de segurança de rede. Mais evidente, porém, é a transversalidade das ameaças e vulnerabilidades, que estão presentes na UFCD 9188 "Fundamentos de Cibersegurança", sob a forma mesma de ameaças, mas também de mercado negro da Internet, *spam*, *phishing* e *malware*; 9189 "Tecnologias de análise de evidências", onde se pretende identificar fontes de informação para analisar evidências, vulnerabilidades e ameaças; 9192 "Análise de vulnerabilidades – iniciação" e 9193 "Análise de vulnerabilidades – desenvolvimento", com referência aos vários tipos de vulnerabilidades *web* e da sua análise, num nível de iniciação e num nível avançado; 9194 "Introdução à Cibersegurança e à ciberdefesa", novamente, em que também se pode identificar o ambiente da ameaça cibernética; 9195 "Enquadramento operacional da Cibersegurança", com várias referências: relatórios de ameaças de segurança, vulnerabilidades *web* mais relevantes, ataque em *sites* de redes sociais para roubo de identidade, sistema de deteção de intrusão,

[6] À semelhança da tabela 2, apresentada anteriormente, trata-se de uma citação da fonte referida. Dispensamos o uso de aspas apenas para facilitar a leitura.

hacking, ameaças de segurança sobre redes; 9196 "Cibersegurança ativa", que, por sua vez, inclui uma componente ligada à investigação e segurança forense para que, através da identificação de evidências digitais de ataques/incidentes informáticos (trabalhando com as VPN e as suas vulnerabilidades), seja possível criar uma resposta a estes ataques informáticos na informática forense; e, por fim, a UFCD 9197 "*Wargamming*", que contempla o desenvolvimento de procedimentos de cibersegurança e ciberdefesa, com base em operações de defesa/ataque. Todas estas informações podem ser consultadas na tabela 5.

De forma geral, verifica-se uma forte articulação entre as dez UFCD, uma vez que agregam conteúdos relevantes do ponto de vista da cibersegurança, tanto ao nível técnico e prático, como ao nível ético. Os objetivos e conteúdos programáticos de todas estas UFCD demonstram, num primeiro momento, a importância dos direitos e liberdades, e da proteção de dados, fazendo referência a documentos nacionais e internacionais, no caso da UFCD 9187 "Legislação, segurança e privacidade", nomeadamente o Regulamento Geral sobre a Proteção de Dados (RGPD), a Carta dos Direitos Fundamentais da União Europeia aplicados à Cibersegurança e, ainda, a Declaração Universal dos Direitos Humanos. Neste sentido, as UFCD seguintes demonstram, em geral, a articulação entre a teoria e a prática, isto é, exploram e reconhecem as ameaças cibernéticas, as vulnerabilidades e evidências presentes nos diversos sistemas de informação (UFCD 9188 "Fundamentos de Cibersegurança"; 9192 "Análise de vulnerabilidades – iniciação"; 9193 "Análise de vulnerabilidades – desenvolvimento") para proteger os direitos e dados, e evitar o não cumprimento de leis. Através desse procedimento, procura entender-se como reagir e proteger os sistemas de ameaças e ataques, baseando-se quer naquilo que têm sido os incidentes informáticos, quer na identificação de fontes seguras e de linguagens modernas de *scripting* (UFCD 9189 "Tecnologias de análise de evidências"; 9191 "Introdução às técnicas de análise de evidências").

No que corresponde à componente mais específica, é possível verificar que a lógica de proteção-resposta-solução-reflexão se apoia em elementos de formação técnica que contemplam a gestão de sistemas informáticos e a utilização de ferramentas digitais importantes para torná-los ou mantê-los seguros, como se constata nas UFCD 9194 "Introdução à Cibersegurança e à ciberdefesa", 9195 "Enquadramento operacional da Cibersegurança" e 9196 "Cibersegurança ativa". Já na UFCD 9197 "*Wargamming*", muito relacionada com a cibersegurança e a ciberdefesa, constam objetivos e conteúdos destinados a desenvolver estratégias de defesa perante ameaças cibernéticas, através de simulações e de uma preparação para ataques e incidentes informáticos reais. Em suma, e apesar de a componente técnica estar mais presente nestas dez UFCD destacadas, verifica-se, ainda assim, uma vasta presença de objetivos e conteúdos relacionados com a ética e o direito, com a prática da segurança no ciberespaço e com o *hacking* ético.

CONCLUSÃO

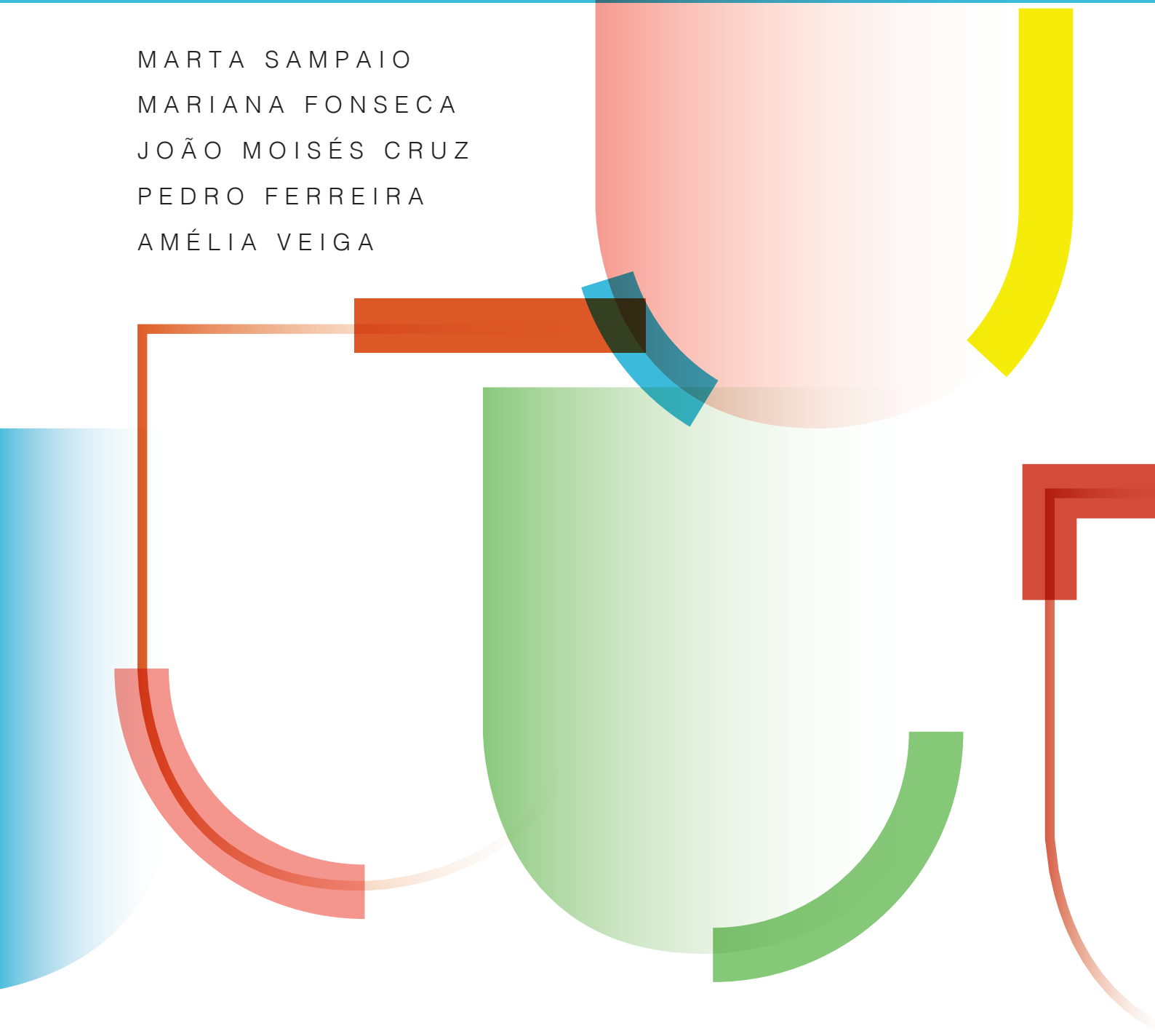
No universo dos cursos CET da área das Ciências Informáticas, e com conteúdos de cibersegurança, encontraram-se, em 2021, 3 cursos diferentes oferecidos por 13 instituições distintas: "Aplicações Informáticas de Gestão", "Gestão de Redes e Sistemas Informáticos" e "Tecnologias e Programação de Sistemas de Informação". No plano de estudos destes três CET, foram identificadas 3 UFCD com conteúdos referentes à área da cibersegurança ou da segurança informática. Observando o plano geral destas três UFCD, percebe-se a valorização da implementação de políticas de segurança, da proteção de dados, das políticas de cópias de segurança e da atenção às vulnerabilidades na perspetiva do combate, monitorização e prevenção.

Para além desta oferta, há um CET em Cibersegurança que em 2021 é promovido por 5 entidades distintas, em 11 locais diferentes. O Curso de Técnico/a Especialista em Cibersegurança, com o código 481344, inclui nas suas componentes de aprendizagem 10 UFCD que contemplam, na sua designação ou nos conteúdos programáticos, a cibersegurança. A análise destas UFCD permitiu verificar uma forte articulação entre as dimensões técnicas, práticas e éticas da cibersegurança. Nos seus objetivos e conteúdos programáticos é valorizada a questão dos direitos e liberdades, e da proteção de dados, fazendo referência a documentos de regulamentação nacionais e internacionais. Para além disso, são exploradas formas de reagir e proteger os sistemas de ameaças e ataques, em larga medida apoiadas numa formação técnica que contempla a gestão de sistemas informáticos e a utilização de ferramentas digitais que permitam torná-los ou mantê-los seguros.

Será importante ir observando se a criação de novas formações a este nível, ou se a transformação das existentes, trará o alargamento das questões abordadas para incluir áreas menos presentes como por exemplo a cibersegurança dos sistemas de controlo industrial e de tecnologias ligadas à *internet das coisas* (*internet of things*, IOT).

CARACTERIZAÇÃO DOS CURSOS E DOS CICLOS DE ESTUDO DA ÁREA DE CIBERSEGURANÇA NO ENSINO SUPERIOR E A SUA IMPLANTAÇÃO NAS CIÊNCIAS INFORMÁTICAS

MARTA SAMPAIO
MARIANA FONSECA
JOÃO MOISÉS CRUZ
PEDRO FERREIRA
AMÉLIA VEIGA



No que ao estudo da Cibersegurança no ensino superior diz respeito, um dos primeiros passos implicou identificar as áreas de educação e formação em que esta se encontrava mais presente. Ao analisar-se o número dos cursos e ciclos de estudo pesquisados em cada uma das áreas CNAEF (através de palavras-chave como, por exemplo, "cibersegurança"; "segurança informática"; "segurança de informação"; "segurança de redes" e "sistemas de informação" - ver nota metodológica), verificou-se que a área "481 - Ciências Informáticas" congrega a grande maioria (75,7%; n= 246). Pela relevância desta área, optou-se então pela análise mais aprofundada dos cursos e dos ciclos de estudo que dela fazem parte.

Sendo este o universo no qual a pesquisa de conteúdos de cibersegurança iria ser feito, e até porque foi necessária a triangulação de dados de fontes diferentes para chegarmos à lista final dos cursos e ciclos de estudo de ensino superior inscritos na área das ciências informáticas e em funcionamento, foi importante começar por uma sistematização da informação sobre estes cursos e pela caracterização dos mesmos (ver Apêndice III). Assim, verificou-se que estes 246 cursos/ciclos de estudo são lecionados em instituições de ensino universitárias e politécnicas, de natureza pública e privada. A sua distribuição geográfica é representada na figura 3.

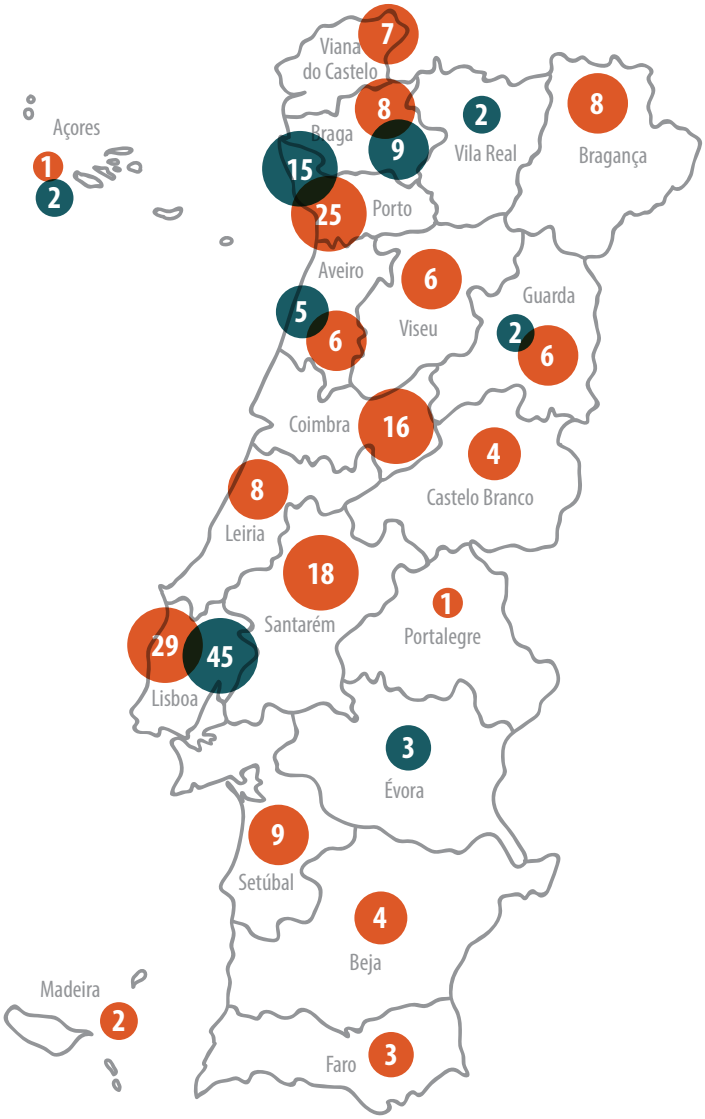


Figura 3:

- Distribuição geográfica, por distrito ou região autónoma, dos cursos/ciclos de estudo de na área CNAEF de Ciências Informáticas oferecidos em instituições de **ensino politécnico**.
- Distribuição geográfica, por distrito ou região autónoma, dos ciclos de estudo na área CNAEF de Ciências Informáticas oferecidos em instituições de **ensino universitário**.

Acompanhando a tendência nacional de litoralização de acesso a bens e serviços, educação, saúde, infraestruturas de transporte (Conselho Nacional de Educação, 2018), entre outros, grande parte da oferta destes cursos e ciclos de estudo encontra-se na faixa litoral do país, com maior incidência nos distritos de Lisboa, Porto e Coimbra. Tal é especialmente evidente para os ciclos de estudo das instituições de ensino universitário, amplificado pela litoralização das próprias instituições, mas é também claro para os cursos e ciclos de estudo em instituições de ensino politécnico, pese embora a muito maior distribuição geográfica neste caso. É ainda nas instituições politécnicas de Lisboa que se encontram mais cursos, no entanto, para além de Coimbra, surgem também agora Aveiro, Santarém, e Braga como distritos onde há 10 ou mais cursos/ciclos de estudo. A tabela 6 apresenta esta distribuição por tipo de ensino e setor.

	Público		Privado		
	Universitário	Politécnico	Universitário	Politécnico	**TOTAL**
Açores	1		1		2
Aveiro	5	6			11
Beja		4			4
Braga	9	8			17
Bragança		8			8
Castelo Branco		4			4
Coimbra	3	16			19
Évora	2				2
Faro		3	1		4
Guarda	2	6			8
Leiria		8			8
Lisboa	38	18	7	11	74
Madeira		2			2
Portalegre		1			1
Porto	6	11	9	14	40
Santarém		12		6	18
Setúbal		9			9
Viana do Castelo		7			7
Vila Real	2				2
Viseu		6			6
	68	**129**	**18**	**31**	**246**

Tabela 6: Distribuição dos cursos e ciclos de estudo da área das ciências informáticas por tipo de ensino e setor

A oferta de ensino nesta área distribui-se em percentagens relativamente semelhantes entre Licenciaturas (25,2%; n=62) e Mestrados (28,9%; n = 71), mas com uma maior expressão para os CTeSP (39,0%; n= 96). O número de Doutoramentos é bastante menor (6,9%; n= 17). Estes cursos são maioritariamente oferecidos por instituições públicas (80,1%; n=197).

Compreendendo-se a importância desta área para o ensino da cibersegurança, procedeu-se à identificação, neste universo, dos cursos/ciclos de estudo da área de Ciências Informáticas, dos cursos/ciclos de estudo que incluem Unidades Curriculares (UC) e/ou conteúdos de cibersegurança ou de segurança informática, sempre com base nas palavras-chave que deram suporte ao desenvolvimento da pesquisa.

Caracterização dos cursos e dos ciclos de estudo com conteúdos de cibersegurança e segurança de informação no ensino superior

Dos 246 cursos/ciclos de estudo identificados na área de Ciências Informáticas, existem 109 que contêm nos seus planos de estudo UC e/ou conteúdos diretamente relacionados com a cibersegurança e/ou segurança informática (ver Apêndice V). Em termos da sua distribuição por curso/ciclos de estudo temos um total de 37 CTeSP, 36 Licenciaturas, 33 Mestrados e 3 Doutoramentos. A distribuição geográfica destes 109 cursos/ciclos de estudo, por tipo de ensino, está representada nas figura 4.

Figura 4:
- Distribuição geográfica, por distrito ou região autónoma, dos cursos/ciclos de estudo com UC e/ou conteúdos relacionados com a cibersegurança e/ou segurança informática oferecidos em instituições de **ensino politécnico**.
- Distribuição geográfica, por distrito ou região autónoma, dos cursos/ciclos de estudo com UC e/ou conteúdos relacionados com a cibersegurança e/ou segurança informática oferecidos em instituições de **ensino universitário**.

No que ao ensino universitário diz respeito, sobressai a oferta existente no distrito de Lisboa, uma vez que agrega 26 destes cursos/ciclos de estudo. Relativamente ao ensino politécnico, os cursos/ciclos de estudo oferecidos distribuem-se geograficamente de uma forma mais equilibrada.

A análise realizada permite ainda concluir que existem 18 cursos/ciclos de estudos no ensino politécnico privado, 43 cursos/ciclos de estudos no ensino politécnico público, 16 cursos/ciclos de estudos no ensino universitário privado e 32 ciclos de estudos no ensino universitário público. A distribuição destes pelo tipo e graus de ensino pode ser encontrada na tabela 7.

Tipo de Ensino/IES	Curso/grau	Nº de cursos/ciclos de estudo	Total
Politécnico Privado	CTeSP	13	18
	Licenciatura	2	
	Mestrado	3	
Politécnico Público	CTeSP	24	43
	Licenciatura	12	
	Mestrado	7	
Universitário Privado	Licenciatura	11	16
	Mestrado	5	
Universitário Público	Licenciatura	11	32
	Mestrado	18	
	Doutoramento	3	
TOTAL			**109**

Tabela 7: Caracterização geral de cursos/ciclos de estudo classificados na área das Ciências Informáticas, com UC e/ou conteúdos de cibersegurança e/ou segurança informática

A tabela 7 evidencia um maior número de CTeSP no politécnico público (n=24), ao mesmo tempo que, no setor privado, o número destes cursos ultrapassa os ciclos de estudo conferentes de grau (n=13). Além disso, e apesar de esta análise se focar apenas nos cursos que contêm algum tipo de referência à cibersegurança e/ou segurança informática, um outro aspeto a destacar é o número de ciclos de estudo de Licenciatura ser equivalente no ensino universitário privado e público (n=11), mas o número de Mestrados no ensino universitário público ser superior (n=18) relativamente à oferta no setor privado (n=5).

No que diz respeito aos conteúdos que fazem referência à cibersegurança e/ou segurança informática, estas aparecem, sobretudo, nas UC destes cursos/ciclos de estudos. No total, contabilizaram-se 147 UC[7] com algum tipo de referência a um destes conceitos, ou adjacentes, sendo que as UC que aparecem com mais frequência são "Segurança Informática"[8], com 19 ocorrências (13%),

[7] De notar que há UC incluídas nesta análise que são opcionais ou que apenas estão integradas em ramos específicos dos cursos/ciclo de estudos em questão. Ainda assim, parece ser importante tê-las em conta já que, mesmo não abrangendo necessariamente a totalidade dos/as estudantes inscritos, configuram possibilidades de formação na área da cibersegurança que estão presentes para os/as estudantes destes cursos/ciclos de estudo.

[8] Para o efeito, foram contabilizadas UC com o mesmo nome, de diferentes anos, e com pequenas alterações na sua designação, por exemplo "Segurança da Informação".

e “Segurança em Sistemas Informáticos”[9], com 13 ocorrências (9%). A seguir a estas duas, as que aparecem com mais frequência são as UC de “Segurança de Redes”[10], com 10 ocorrências (7%), de “Cibersegurança”, com 6 ocorrências (4%), e, ainda, de “Segurança”, com 4 ocorrências (3%). As restantes UC (n=95), que designamos como “Outras denominações” na análise, correspondem a UC como “Segurança na *Web*”, “Gestão de Sistemas de Informação”, “Cibersegurança Forense”, “Segurança em Software”, ou variantes destes termos, com uma ocorrência inferior a 4 cada e, por essa razão, foram incluídas no gráfico de forma conjunta. De notar que as questões específicas da segurança dos sistemas de controlo industriais, assim como o que envolve a segurança de tecnologias ligadas à *internet das coisas* (IOT), parecem estar menos presentes. Estes dados podem ser visualizados no gráfico 1.

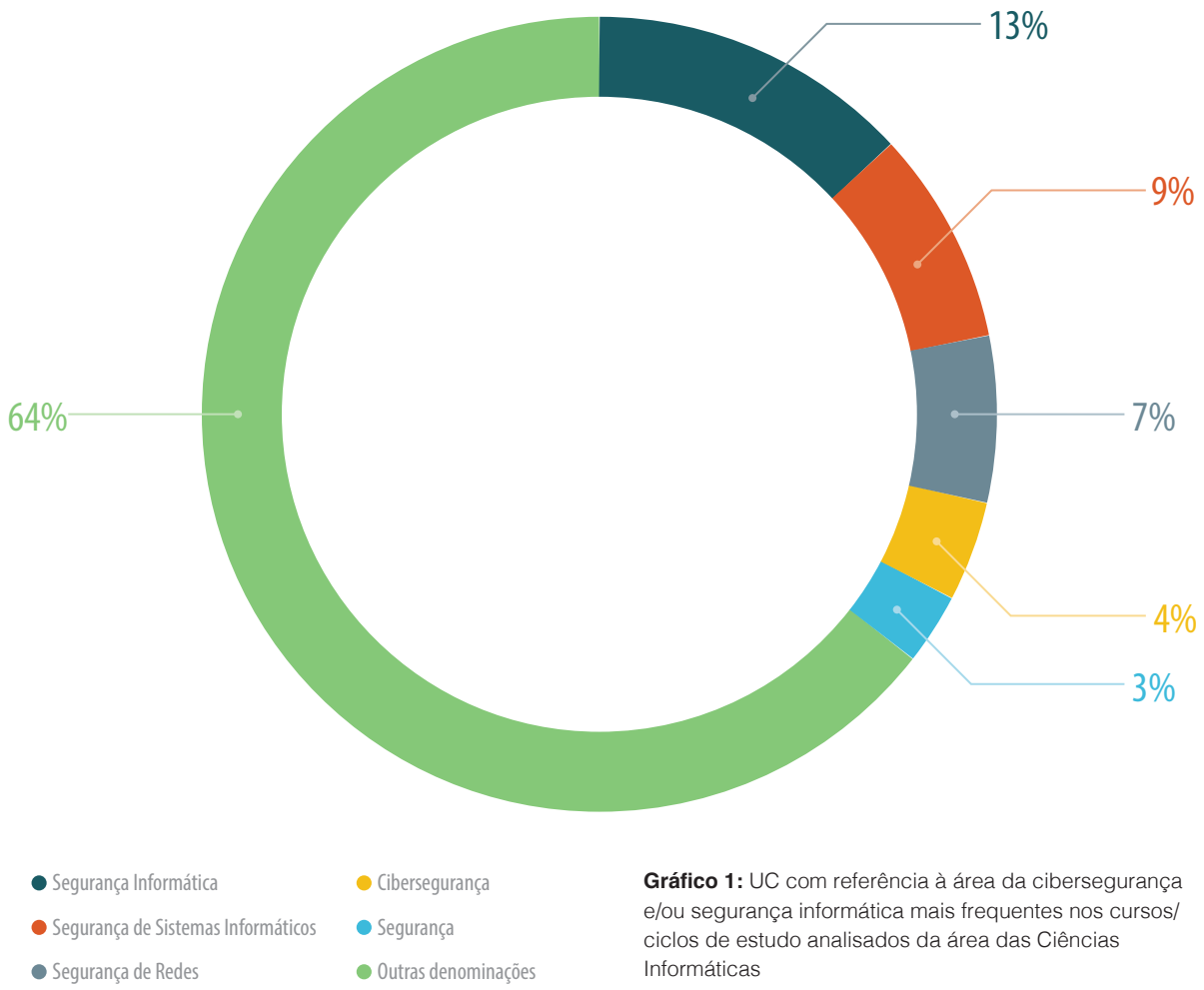


Gráfico 1: UC com referência à área da cibersegurança e/ou segurança informática mais frequentes nos cursos/ciclos de estudo analisados da área das Ciências Informáticas

Nos 109 cursos/ciclos de estudos da área das Ciências Informáticas com UC e/ou conteúdos da área de cibersegurança, estão inscritos/as 7707 estudantes distribuídos pelos diferentes graus de ensino, tal como é apresentado no gráfico 2 (CTeSP n=1287, 16,7%; Licenciatura n=5024, 65,2%; Mestrado n=1140, 14,8%; Doutoramento n=256; 3,3%). O gráfico 2 contempla também a distribuição por sexo sendo possível verificar que de entre os/as 7707 inscritos/as, apenas 1124 são do sexo feminino (14,6%), o que demonstra a sua baixa frequência em cursos/ciclos de estudo da área das Ciências Informáticas. A representação do sexo feminino é especialmente baixa nos CTeSP (n=65; 5,0%) e nas Licenciaturas (n=739; 14,7%), aumentando um pouco nos Mestrados (n=268; 30,7%) e nos Doutoramentos (n=52; 20,3%).

[9] Para o efeito, foram contabilizadas UC com o mesmo nome, de diferentes anos, e com pequenas alterações na sua designação, por exemplo “Segurança de Sistemas Informáticos”, “Segurança e Sistemas Informáticos”, “Segurança de Sistemas de Informação”.

[10] Para o efeito, foram contabilizadas UC com o mesmo nome, de diferentes anos, e com pequenas alterações na sua designação, por exemplo “Segurança em Redes”.

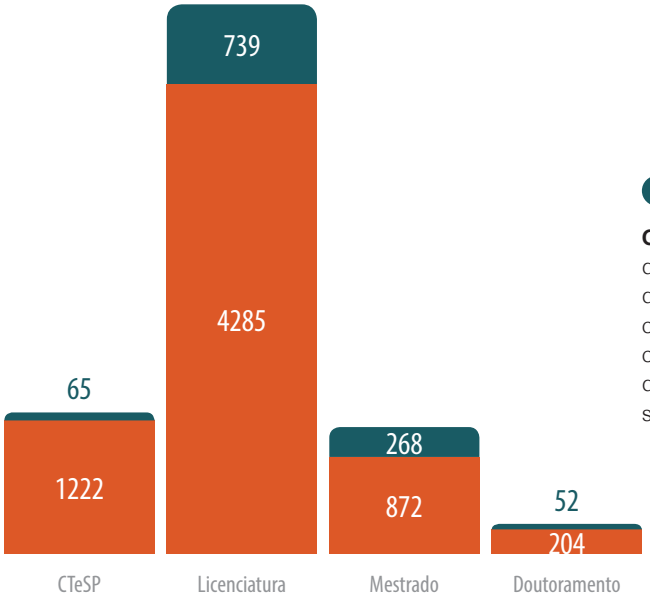


Gráfico 2: Distribuição de inscrições por graus de ensino e sexo nos 109 cursos/ciclos de estudo com conteúdos na área de cibersegurança e segurança de informação

De um modo geral, verifica-se que o maior número de estudantes inscritos/as se concentra no ensino politécnico público (n=3346) e no ensino universitário público (n=3020). Tal como é detalhado na tabela 8, nos CTeSP identifica-se um maior número de inscritos/as no ensino politécnico público (n=767) do que no ensino politécnico privado (n=520). No que diz respeito às Licenciaturas, existe uma maior concentração de inscritos/as no ensino politécnico público (n=2389) e no ensino universitário público (n=1941). Em relação aos Mestrados, há mais estudantes inscritos/as no ensino universitário público (n=823) do que nos restantes tipos/setores de ensino. Os Doutoramentos são ministrados apenas no ensino universitário público onde se encontra o total de 256 inscritos/as.

Tipo de Ensino/Setor	Curso/Grau	Sexo Masculino	Sexo Feminino	Total Inscritos/as
Politécnico Privado	CTeSP	503	17	520
	Licenciatura	71	6	77
	Mestrado	53	5	58
Politécnico Público	CTeSP	719	48	767
	Licenciatura	2072	317	2389
	Mestrado	149	41	190
Universitário Privado	Licenciatura	558	59	617
	Mestrado	51	18	69
Universitário Público	Licenciatura	1584	357	1941
	Mestrado	619	204	823
	Doutoramento	204	52	256
TOTAL		6583 (85,4%)	1124 (14,6%)	7707

Tabela 8: Distribuição do nº de inscritos/as em cursos/ciclos de estudo da área das Ciências Informáticas com UC ou conteúdos referentes à área de cibersegurança e segurança de informação por tipo de ensino, por setor, por curso/grau e por sexo

No que diz respeito ao número de diplomados/as nos cursos/ciclos de estudo da área das Ciências Informáticas com UC ou conteúdos da área de cibersegurança, no ano letivo de 2019/2020 diplomaram-se 1498 estudantes distribuídos pelos diferentes graus de ensino, tal como é apresentado no gráfico 3. Dos 1498 diplomados/as, identificam-se 412 em CTeSP (28%), 574 em Licenciaturas (38%), 493 em Mestrados (33%) e 19 em Doutoramentos (1%). Verifica-se também, e uma vez mais, um baixo número de mulheres diplomadas, apenas 231 (15%) em relação aos 1267 (85%) estudantes de sexo masculino diplomados. Dessas 231, 25 diplomaram-se em CTeSP (6%), 88 em Licenciaturas (15%), 116 em Mestrados (24%) e 2 em Doutoramentos (11%), tal como é apresentado no gráfico 3.

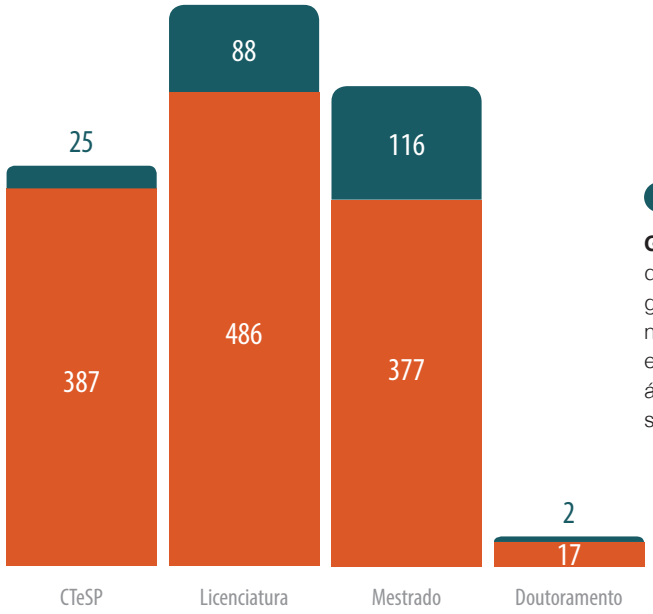


Gráfico 3: Distribuição de diplomados/as por graus de ensino e sexo nos 109 cursos/ciclos de estudo com conteúdos na área de cibersegurança e segurança de informação

Numa visão global, e como é detalhado na tabela 9, existe um maior número de diplomados/as no ensino universitário público (n=633) e no ensino politécnico público (n=582). No que toca aos CTeSP, o número de diplomados/as é mais alto no ensino politécnico público (n=247) do que no ensino politécnico privado (n=165). Ao nível da Licenciatura, o maior número de diplomados/as é no ensino politécnico público (n=280) e o mais baixo no ensino politécnico privado (n=11), com uma larga diferença. No que diz respeito aos Mestrados destaca-se, claramente, o número de diplomados/as no ensino universitário público (n=434), contrastando com o baixo número de diplomados no ensino universitário privado (n=4). Por fim, no grau de Doutoramento identificam-se 19 diplomados/as todos/as no ensino universitário público.

Tipo de Ensino/Setor	Curso/Grau	Sexo Masculino	Sexo Feminino	Total Diplomados/as
Politécnico Privado	CTeSP	155	10	165
	Licenciatura	10	1	11
	Mestrado[11]	–	–	–
Politécnico Público	CTeSP	232	15	247
	Licenciatura	239	41	280
	Mestrado	40	15	55
Universitário Privado	Licenciatura	90	13	103
	Mestrado	4	0	4

[11] Não foi possível encontrar dados de diplomados/as em nenhum dos Mestrados que contêm UC ou conteúdos referentes à área de cibersegurança e segurança de informação.

Universitário Público	Licenciatura	147	33	180
	Mestrado	333	101	434
	Doutoramento	17	2	19
TOTAL		1267 (84,6%)	231 (15,4%)	1498

Tabela 9: Distribuição do nº de diplomados/as em cursos/ciclos de estudo da área das Ciências Informáticas com UC ou conteúdos referentes à área de cibersegurança e segurança de informação por tipo de ensino, por setor, por curso/grau e por sexo

É importante notar que algumas UC incluídas na análise são opcionais ou estão integradas apenas em ramos específicos dos cursos/ciclos de estudos pelo que poderão não ser frequentadas por todos/as os/as estudantes. O número de inscritos/as e diplomados/as de cursos/ciclos de estudo com UC ou conteúdos de cibersegurança podem também sofrer variações devido ao facto de não aparecerem, nas bases de dados públicas, dados para todos os cursos/ciclos de estudo destacados com UC e/ou conteúdos da área de cibersegurança.

Caracterização dos cursos e dos ciclos de estudo em cibersegurança e segurança de informação no ensino superior

Focando naquela que é a oferta específica em Cibersegurança e Segurança de Informação em Portugal em 2021, e tal como apresenta a tabela 10, foram identificados 20 cursos/ciclos de estudo: 9 CTeSP, 1 Licenciatura, 9 Mestrados e 1 Doutoramento. Em comparação com o ano de 2020, foram identificadas 4 novas ofertas, nomeadamente, 3 novos CTeSP e 1 novo mestrado, como se refere no *Relatório Cibersegurança em Portugal – Sociedade 2021*, do Observatório de Cibersegurança.

Grau	Ciclo de Estudos	Instituição
Curso Técnico Superior Profissional	Cibersegurança	Instituto Politécnico da Guarda – Escola Superior de Tecnologia e Gestão
	Cibersegurança	Instituto Politécnico da Bragança – Escola Superior de Tecnologia e Gestão
	Cibersegurança	Instituto Politécnico da Lusofonia – Escola Superior de Engenharia e Tecnologias
	Cibersegurança (NOVO)	Instituto Superior de Tecnologias Avançadas de Lisboa – Escola Superior de Ciência e Tecnologia
	Cibersegurança, Redes e Sistemas Informáticos	Instituto Politécnico do Porto – Escola Superior de Tecnologia e Gestão
	Cibersegurança, Redes e Sistemas Informáticos	Instituto Politécnico Jean Piaget do Sul – Escola Superior de Tecnologias e Gestão Jean Piaget
	Cibersegurança, Redes Informáticos (NOVO)	Instituto Politécnico de Leiria – Escola Superior de Tecnologia e Gestão
	Segurança e Proteção de Dados para Sistemas de Informação (NOVO)	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior Profissional
	Redes e Segurança Informática	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior Profissional
Licenciatura	Segurança Informática em Redes de Computadores	Instituto Politécnico do Porto – Escola Superior de Tecnologia e Gestão

Mestrado	Cibersegurança	Instituto Politécnico de Viana do Castelo – Escola Superior de Tecnologia e Gestão de Viana do Castelo
	Cibersegurança	Universidade de Aveiro
	Cibersegurança e Informática Forense	Instituto Politécnico de Leiria – Escola Superior de Tecnologia e Gestão de Leiria
	Cibersegurança e Auditoria de Sistemas Informáticos (NOVO)	Instituto Superior Politécnico Gaya
	Segurança de Informação e Direito no Ciberespaço	Universidade de Lisboa – Faculdade de Direito e Instituto Superior Técnico com Instituto Universitário Militar – Escola Naval
	Segurança Informática	Universidade de Coimbra – Faculdade de Ciências e Tecnologia
	Segurança Informática	Universidade de Lisboa – Faculdade de Ciências
	Segurança Informática	Universidade do Porto – Faculdade de Ciências
	Engenharia de Segurança Informática	Instituto Politécnico de Beja – Escola Superior de Tecnologia e Gestãp
Doutoramento	Segurança de Informação	Universidade de Lisboa – Instituto Superior Técnico

Tabela 10: Cursos/Ciclos de Estudo da área de cibersegurança e segurança de informação em Portugal

No ano letivo de 2020/2021, estes cursos/ciclos de estudo contaram com 718 inscrições: 309 (43,04%) em CTeSP, 119 (16,57%) na Licenciatura, 284 (39,55%) nos Mestrados e 6 (0,84%) no Doutoramento. Tomando como referência os valores de 2020, o valor do número de inscritos/as apresenta uma tendência crescente – um aumento de 82 inscritos/as –, não havendo, no entanto, um aumento na percentagem de inscritas do sexo feminino, como se refere no *Relatório Cibersegurança em Portugal – Sociedade 2021*, do Observatório de Cibersegurança. Como o gráfico 4 deixa claro, a percentagem de inscritas do sexo feminino é muito baixa, ainda mais baixa do que os 10% de 2019/2020, representando apenas 8,08% (n=58) das inscrições nestes cursos/ciclos de estudo no ano letivo 2020/2021. Resulta da análise que a área da cibersegurança e da segurança de informação é uma área em crescimento que permanece numa tendência crescente de inscritos/as, mas que, como outras nas *Science*, *Technology*, *Engineering* e *Mathematics* (STEM), ainda atrai poucas estudantes do sexo feminino, algo que poderá merecer atenção e intervenção no futuro.

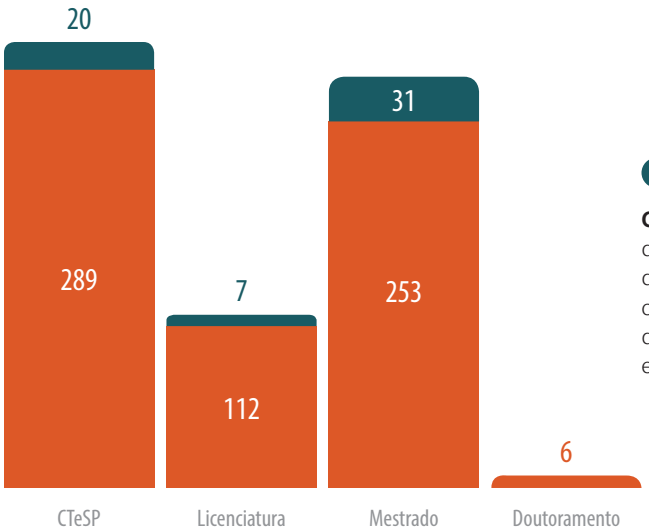


Gráfico 4: Distribuição de inscrições por graus de ensino e por sexo em cursos e ciclos de estudo da área de cibersegurança e segurança de informação

No que ao número de diplomados/as diz respeito (referente ao ano letivo 2019/2020), diplomaram-se nestes cursos/ciclos de estudo 152 pessoas: 79 em CTeSP, 6 na Licenciatura, 65 nos Mestrados e 1 no Doutoramento. O gráfico 5 apresenta a distribuição de diplomados/as por graus de ensino e sexo. A percentagem de mulheres diplomadas é também baixa, um total de 14 diplomadas (9,21%), em linha com as baixas percentagens dos últimos anos, indo de encontro aos valores reportados no *Relatório Cibersegurança em Portugal – Sociedade 2021*, do Observatório de Cibersegurança. Pode notar-se que, mantendo-se baixa, a percentagem de diplomadas é mais elevada para o grau de Mestrado (18,18%) e especialmente baixa nos cursos CTeSP (3,95%).

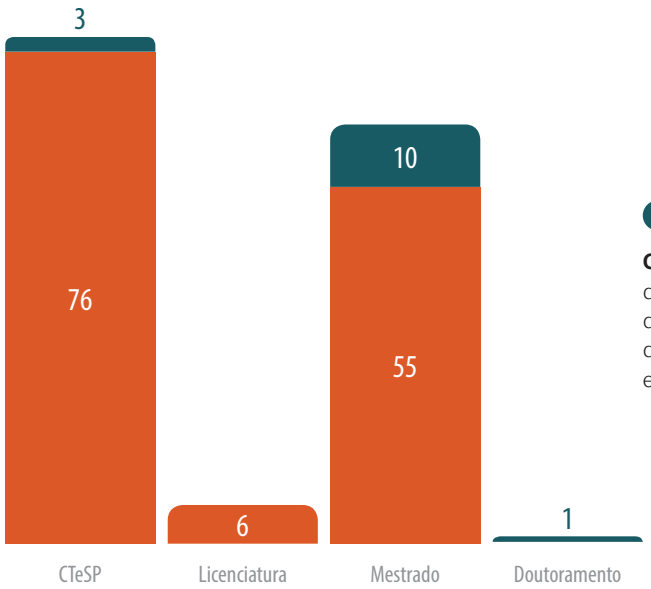


Gráfico 5: Distribuição de diplomados/as por graus de ensino e sexo em cursos da área de cibersegurança e segurança de informação

No que diz respeito à evolução do número de dissertações de mestrado e de teses de doutoramento com referência às questões da cibersegurança e/ou da segurança informática, com base nas palavras-chave já mencionadas, e através de consulta na plataforma RENATES (ver nota metodológica), foi possível confirmar a existência de 337 registos de dissertações e teses em curso ou concluídas desde 2003.

Como mostra o gráfico 6, existem 284 dissertações de mestrado concluídas entre 2010 e 2021. O número de dissertações de mestrado concluídas teve uma subida mais acentuada entre 2014 e 2015 – de 19 para 37 – e atingiu o seu pico em 2019, com 45 dissertações.

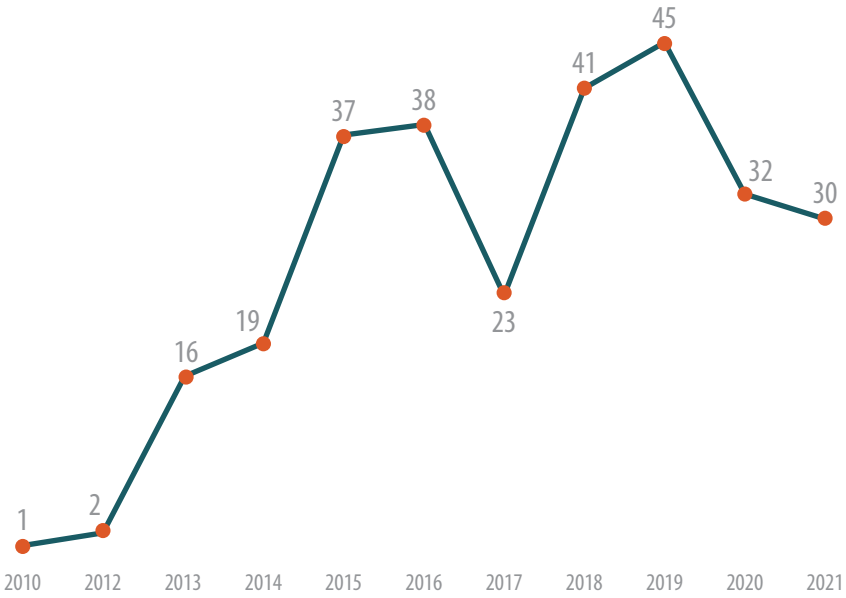


Gráfico 6: Número de dissertações de mestrado concluídas com referência à cibersegurança e/ou à segurança informática entre 2010 e 2021

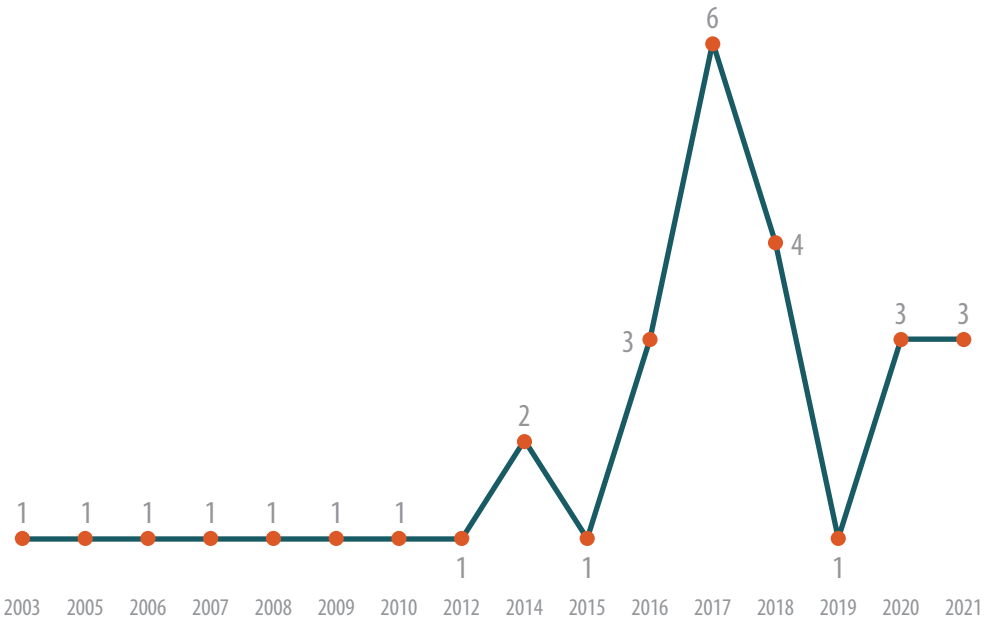


Gráfico 7: Número de teses de doutoramento concluídas com referência à cibersegurança e/ou à segurança informática entre 2003 e 2021

Pesquisando as teses de doutoramento, existem 53 registos, sendo que 22 estão em curso. Das 31 já concluídas, e depois de uma década com uma média de 1 tese concluída por ano (entre 2003 e 2013), o pico foi atingido em 2017, com 6 teses concluídas.

Focando-nos nas dissertações de mestrado e teses de doutoramento acima referidas e concluídas na área de cibersegurança, a maioria foi também realizada por homens (ver gráfico 8). Das 284 dissertações, 175 foram realizadas por homens e 109 por mulheres. Quanto às 31 teses de doutoramento concluídas, 24 foram realizadas por homens e apenas 7 por mulheres.

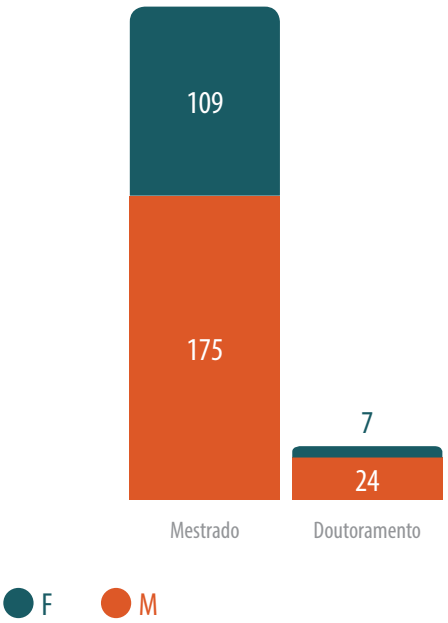


Gráfico 8: Distribuição de dissertações de mestrado e teses de doutoramento concluídas, com referência à cibersegurança e/ou à segurança informática, por graus de ensino e sexo

CONCLUSÃO

No que toca à implantação da Cibersegurança no ensino superior, dos 246 cursos/ciclos de estudo identificados na área de Ciências Informáticas, verificou-se que existem 109 que contêm nos seus planos de estudo UC e/ou conteúdos diretamente relacionados com a cibersegurança: 37 CTeSP, 36 Licenciaturas, 33 Mestrados e 3 Doutoramentos.

A oferta específica de cursos/ciclos de estudo em Cibersegurança e Segurança de Informação em Portugal em 2021 é composta por 20 cursos/ciclos de estudo – 9 CTeSP, 1 Licenciatura, 9 Mestrados e 1 Doutoramento – o que significa um aumento de 3 novos CTeSP e 1 novo mestrado relativamente a 2020. O número de inscritos/as nestes cursos/ciclos de estudo, que mantém uma tendência crescente, foi de 718 estudantes – 309 (43,04%) em CTeSP, 119 (16,57%) na Licenciatura, 284 (39,55%) nos Mestrados e 6 (0,84%) no Doutoramento. Os/as diplomados/as, em 2019/2020, foram 152: 79 em CTeSP, 6 na Licenciatura, 65 nos Mestrados e 1 no Doutoramento. A percentagem de inscritas do sexo feminino é muito baixa (n=58; 8,1%), tal como a das mulheres diplomadas (n=14; 9,21%), em linha com as baixas percentagens de outros anos e sugerindo a necessidade de ações visando a atração de candidatas a estas formações.

Se entre as ofertas de cursos/ciclos de estudo da área das Ciências Informáticas com UC ou conteúdos de Cibersegurança há equilíbrio entre o número de CTeSP, Licenciaturas e Mestrados, na oferta de cursos/ciclos de estudo em Cibersegurança é notório o menor número de Licenciaturas e o maior peso dos CTeSP e dos Mestrados na formação.

A pesquisa de dissertações de Mestrado e de teses de Doutoramento registadas na plataforma RENATES permitiu identificar 53 teses de Doutoramento (desde 2003), 31 concluídas e 22 em curso, e 284 dissertações de Mestrado (desde 2010) com referência às questões da Cibersegurança e/ou da Segurança Informática.

CARACTERIZAÇÃO DA EDUCAÇÃO E FORMAÇÃO NA ÁREA DE CIBERSEGURANÇA NO ENSINO SUPERIOR

JOÃO MOISÉS CRUZ
MARIANA FONSECA
AMÉLIA VEIGA

Para a análise dos cursos em cibersegurança e segurança da informação em Portugal considera-se: (i) a estrutura curricular dos cursos/ciclos de estudo, (ii) o número de créditos ECTS que o estudante deve reunir em cada uma delas, (iii) o plano de estudos, (iv) os objetivos do curso, e (v) os resultados de aprendizagem das UC.

A estrutura curricular de um CTeSP ou de um ciclo de estudos (Licenciatura, Mestrado e Doutoramento) refere-se ao conjunto de áreas científicas (e.g., Artes e Humanidades; Ciências Sociais, Comércio e Direito; Ciências, Matemática e Informática; Engenharia, Indústrias Transformadoras e Construção) e respetivas UC acompanhadas do número de créditos ECTS que o/a estudante deve completar para obter o grau académico ou concluir o curso. O número de créditos ECTS é a unidade de medida do trabalho do estudante sob todas as suas formas. Em Portugal, um crédito equivale a cerca de 27 horas de trabalho do/a estudante, cabendo, no entanto, a cada instituição de ensino superior definir essa equivalência.

Desta forma, ao analisar estes cursos/ciclos de estudo importa, em primeiro lugar, perceber que áreas científicas têm mais e menos peso, em termos de número de créditos ECTS, uma vez que estes, ao refletirem o volume de trabalho do/a estudante, remetem para a importância atribuída a determinada área científica na estrutura curricular dos cursos/ciclos de estudos já identificados (ver tabela 10). Em segundo lugar, importa analisar os planos de estudos e os conteúdos que serão caracterizados mais adiante, por curso/ciclo de estudo.

Nas figuras seguintes, apresentam-se as áreas científicas com mais e menos peso expresso pelo número de créditos ECTS nos cursos/ciclos de estudo oferecidos pelas instituições de ensino politécnico e universitário. Note-se que a estrutura curricular mais detalhada de cada curso/ciclo de estudos se encontra em apêndice (ver Apêndice VI), onde é possível consultar a estrutura curricular completa e a distribuição do número de créditos ECTS, por todas as UC.

No que toca à análise da estrutura curricular dos cursos/ciclos de estudo oferecidos no ensino politécnico, nos setores público e privado, é possível perceber (ver gráfico 9) que a área de Ciências Informáticas predomina em todos e que a área científica das Humanidades – que abrange, por exemplo, as Línguas, a Filosofia e Ética – assume uma importância residual nas respetivas estruturas curriculares destes cursos.

Gráfico 9: Áreas científicas com mais e menos peso em ECTS nos cursos e ciclos de estudo em cibersegurança oferecidos no ensino politécnico

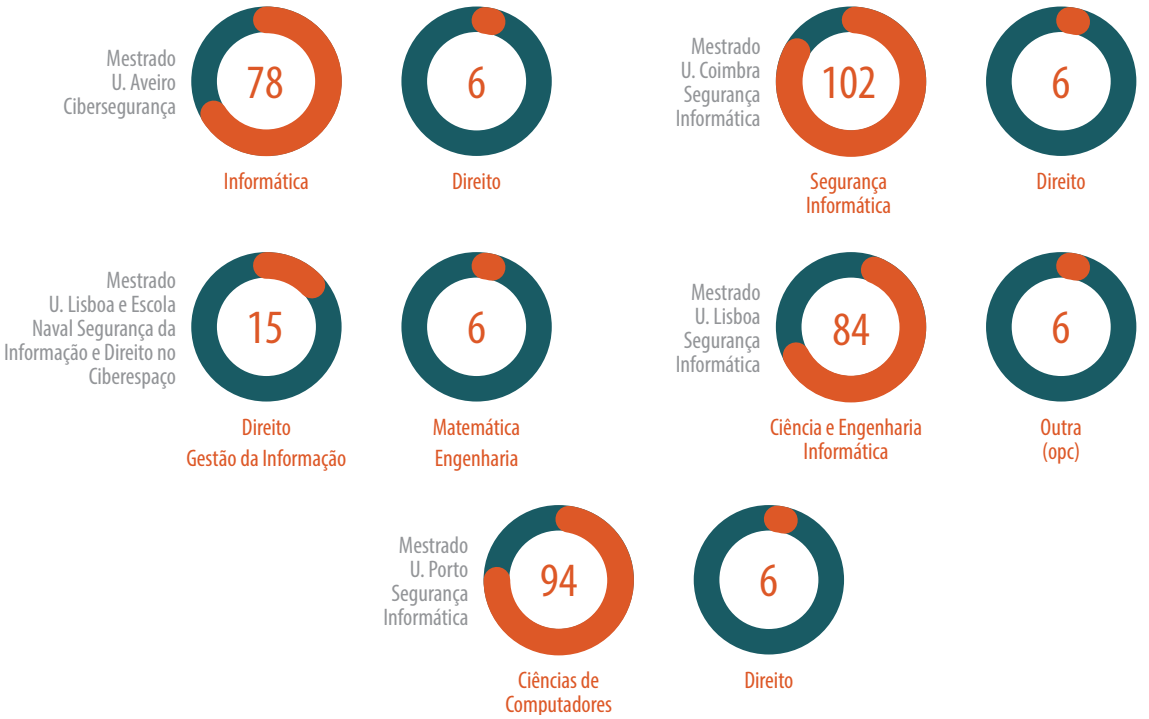


Gráfico 10: Áreas científicas com mais e menos peso em ECTS ciclos de estudo em cibersegurança e segurança de informação oferecidos no ensino universitário público (com a exceção do doutoramento[12])

[12] A especificidade da oferta ao nível de doutoramento, este congrega os 210 ECTS em torno da realização da Tese, faz com que não seja informativo colocá-lo neste gráfico.

Por sua vez, na análise das estruturas curriculares dos ciclos de estudo oferecidos pelas universidades, no setor público, verifica-se que a oferta se restringe quase exclusivamente ao nível do mestrado, havendo um doutoramento em segurança da informação.

Apesar de diferente da oferta no ensino politécnico, a área científica da Informática e Segurança Informática continua a ter uma maior expressão com destaque, igualmente, para as Ciências de Computadores. Aqui, a área científica de Direito, apesar de presente na maioria dos ciclos de estudo, é também aquela que tem menos expressão na estrutura curricular destes ciclos de estudo.

A oferta ao nível do doutoramento é focada, maioritariamente, no desenvolvimento de áreas científicas interdisciplinares na área da Segurança da Informação que congregam 210 ECTS do total de 240.

No que se refere às dissertações de mestrado e às teses de doutoramento concluídas e em curso na área de cibersegurança, podemos observar que as áreas dos domínios científicos e tecnológicos das Ciências da Computação e da Informação, Eletrónica e Automação e Segurança Militar, continuam a ser as áreas em que a cibersegurança tem maior expressão, como se encontra representado no gráfico 11. Contudo, é interessante verificar que estes trabalhos também refletem a importância de outras áreas, designadamente a Ciência Política e Cidadania, Direito, Gestão e Administração e Proteção de Pessoas e Bens.

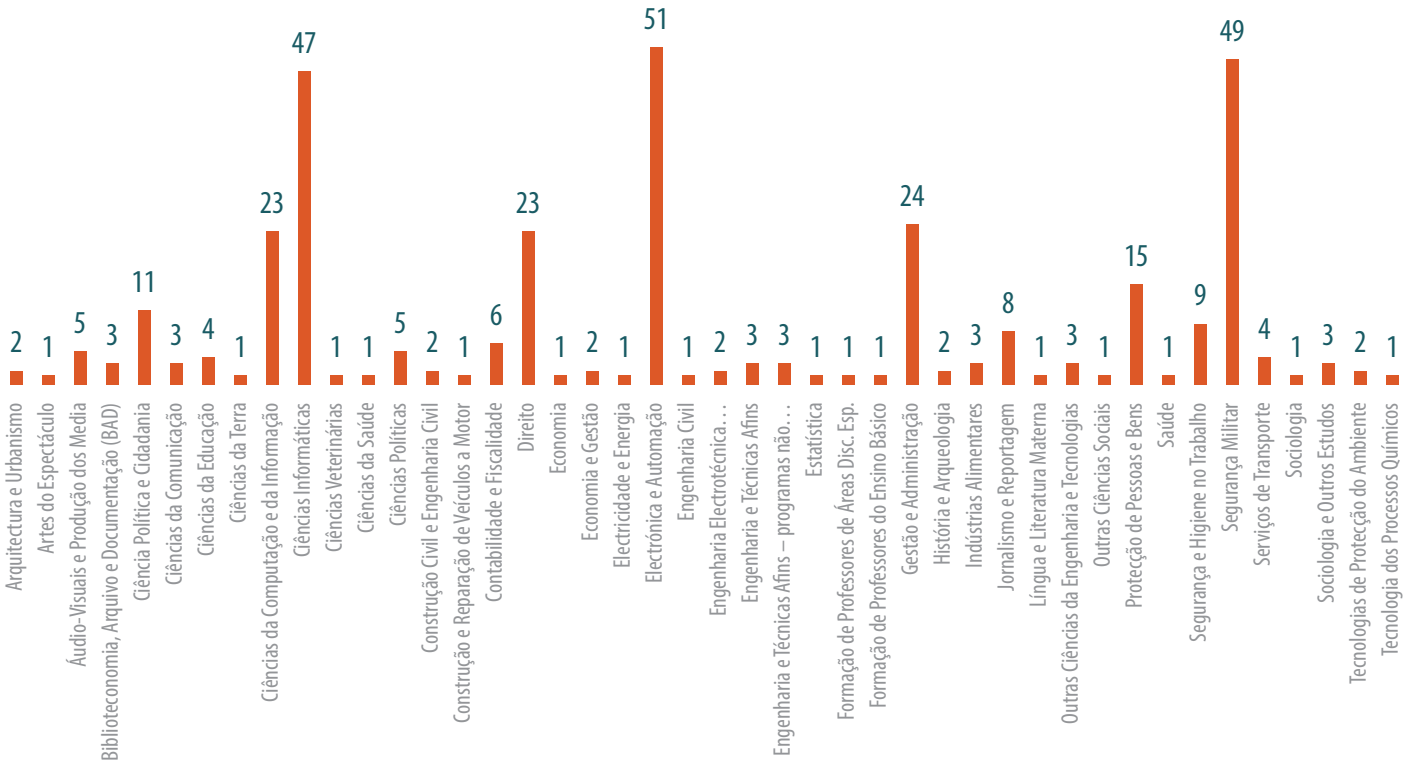


Gráfico 11: Dissertações de mestrado e teses de doutoramento na área de cibersegurança em curso e concluídas, entre 2003 e 2021, por áreas científicas

De seguida, a análise dos cursos/ciclos de estudos em cibersegurança (já apresentados na tabela 10) debruça-se sobre os planos de estudos, os objetivos do curso/ciclo de estudos, e dos resultados de aprendizagem das UC. O plano de estudos corresponde a um conjunto organizado de unidades curriculares que um/a estudante deve realizar para obter aprovação para obter um grau académico ou concluir um curso. Esta análise é complementada pelas entrevistas realizadas junto dos diretores do curso e está orientada pelas componentes da formação técnica, ética e legal, do mercado de trabalho/organizacional, e da investigação e inovação.

CTeSP

Os CTeSP em Cibersegurança existentes em Portugal são um total de 9, oferecidos pelo ensino politécnico, nos setores público e privado. A análise que se segue procura olhar para os planos de estudos, as UC, os conteúdos abordados em cada uma delas, bem como os resultados da aprendizagem de cada um dos 9 CTeSP, à luz das componentes técnicas, ética e legal, das necessidades do mercado de trabalho/organizacionais, bem como da investigação, com o intuito de aprofundar o conhecimento sobre estes cursos.

Formação técnica, ética e legal

A componente de formação técnica tem um peso muito grande na estrutura curricular, como se pode ver pela área científica dominante nestes cursos, as Ciências Informáticas (como mostra o gráfico 7 anteriormente apresentado). Esta componente traduz-se em conhecimentos e competências concretas nesta área e que são fundamentais na construção dos cursos CTeSP em Cibersegurança e Segurança da Informação.

Antes de mais, tendo em consideração a perceção de alguns entrevistados, ela serve para introduzir os/as estudantes a conceitos relacionados com a segurança, tais como "confidencialidade, integridade ou disponibilidade" (Entrevistado 4). Posteriormente, abordam-se algumas áreas basilares, sendo elas as áreas de Redes, Sistemas e Programação. Esta abordagem é, principalmente, de cariz introdutório e falamos, por exemplo, na componente de Redes, das suas vertentes de implementação, gestão e manutenção. A componente de Sistemas é abordada, fundamentalmente, ao nível da instalação, configuração e administração. Finalmente, em termos de Programação, falamos, por exemplo, da programação de *scripts* e da programação aplicada à segurança. Ainda dentro das componentes técnicas abordadas nos CTeSP, importa referir alguns conhecimentos mais complexos que são abordados após estes temas introdutórios. São exemplos a administração e gestão de Bases de Dados, a Criptografia, a Análise Forense Digital, Compliance e *Ethical Hacking*, bem como competências de identificação de vulnerabilidades e resposta a incidentes. Com efeito, como é referido pelo entrevistado 3, estão presentes um "conjunto de áreas como *ethical hacking*, a componente dos ataques que podem ser feitos e com que objetivos, como é que poderão ser feitos, a componente de recuperação de desastres, por exemplo, em infraestruturas, a componente ligada às certificações e ao *compliance*", ideia reforçada pelo entrevistado 2 quando afirma: "abordamos várias UC que falamos de *hacking*, anti-*hacking*, análise forense e resposta a incidentes".

As unidades curriculares que constituem o plano de estudos destes cursos parecem ir de encontro às áreas científicas mais relevantes, como se pode ver pelas unidades curriculares de "Fundamentos de Redes e Sistemas", "Segurança em Redes e Sistemas Informáticos", "Administração de Bases de Dados", "Análise de Vulnerabilidades", "Introdução à Cibersegurança", "Introdução à Programação de *Scripts*", "Introdução aos Sistemas Informáticos", "Introdução às Redes", "Programação Aplicada à Cibersegurança", "Análise Forense" ou "*Ethical Hacking*".

As componentes de ética e do direito estão presentes em praticamente metade dos cursos CTeSP analisados, e todos os diretores de curso as referem como essenciais numa formação em cibersegurança. Esta componente, na perceção dos entrevistados 2 e 4, está presente, essencialmente, em unidades curriculares que tratam assuntos relacionados com a privacidade, proteção de dados e RGPD e é abordada com o objetivo de introduzir questões legais relacionadas com a cibersegurança, bem como traduzir esse conhecimento ao nível do trabalho numa organização, nomeadamente a utilização dos conhecimentos de privacidade e tratamento de dados no mercado de trabalho. Na verdade, como é mencionado pelo entrevistado 4,

> *"(...) se houver esta temática nos percursos académicos, penso que teremos profissionais mais bem preparados para, posteriormente, no mercado de trabalho, já levarem consigo estes cuidados que são necessários no tratamento de dados e o cuidado necessário implica todo um conjunto de ferramentas e metodologias que devem ser utilizadas e seguidas no tratamento de dados para que as tarefas que desempenham se mantenham dentro da legalidade."*

Esta componente legal não é abordada de forma muito aprofundada, na medida em que o que se pretende é um conhecimento geral destas questões e da sua aplicação nas empresas, e não uma discussão dessas questões, como refere o entrevistado 4, quando afirma que "é dado um foco maior a conceitos relacionados com a Segurança Informática. A parte da legislação é uma parte bastante mais reduzida, pois o que pretendemos é que eles estejam mais focados na área técnica", e confirmado pelo entrevistado 1, que perceciona a necessidade de encontrar um equilíbrio entre as várias componentes como um desafio, de facto, "pesar este tipo de coisas não é fácil, especialmente a um nível muito técnico, também não é expectável que pessoas a este nível técnico sejam elas a fazer a decisão". Avançam-se, ainda, alguns motivos para estas UC não serem abordadas, ou não estarem mais presentes nas estruturas curriculares, como se pode perceber nas palavras do entrevistado 2:

> *"Não lhe sei dizer com certeza que foi por isto ou por aquilo, mas recordo-me que há várias opções que tivemos de tomar, do ponto de vista de escolher uma determinada UC em detrimento de outras porque não conseguimos incluir, no espaço que temos de 3 semestres, todas as vertentes, temos de fazer a escolha. Imagino que seja essa a razão de não termos uma cadeira de Ética."*

Algumas unidades curriculares desta componente são, por exemplo, "Normas de Segurança e Privacidade", "Direito Aplicado à Proteção de Dados Pessoais - RGPD", "Segurança e Direito da Informação" ou "Noções Fundamentais de Direito".

Destacam-se, também, algumas áreas científicas referentes às Humanidades e às outras Ciências Sociais, nomeadamente a Língua Portuguesa e a Língua Inglesa. A abordagem a estas áreas é construída, também ela, na relação com o mercado de trabalho, isto é, abordam-se conceitos sobre comunicação em contexto profissional ou técnico nestas duas línguas, como fazer apresentações orais e escritas ou preparar um *curriculum vitae*. As UC são, por exemplo, "Comunicar em Língua Portuguesa", "Comunicar em Língua Inglesa" ou "Inglês Técnico".

As necessidades do mercado de trabalho

A componente do mercado de trabalho tem uma forte articulação com a componente técnica e está, a par desta, muito presente na formação dos CTeSP. Isto acontece, desde logo, porque o principal objetivo destes cursos é formar trabalhadores/as de primeira linha que sejam rapidamente integrados no mercado de trabalho. Assim, grande parte dos conceitos e das competências técnicas, que se pretende que os/as estudantes adquiram no decorrer do curso, têm uma enorme aplicabilidade nos contextos de trabalho, isto é, pretende-se que os conhecimentos, competências e capacidades resultantes da aprendizagem dos conteúdos das unidades curriculares se destinem a aplicar e a integrar no tecido empresarial. Esta posição é corroborada pelo entrevistado 3, ao referir que "[o] objetivo do curso é dar a capacidade às pessoas para entrarem no mercado de trabalho. O mercado de trabalho está sedento de recursos com capacidades, com *know how*".

Mais ainda, em todas as entrevistas realizadas aos diretores de curso, a relação estreita entre a construção do curso e o mercado de trabalho foi evidenciada, na medida em que as decisões

tomadas ao nível da estruturação curricular, do plano de estudos, dos conteúdos a abordar e das competências a adquirir, têm uma forte influência do mercado de trabalho. De facto, há uma ênfase muito forte nas competências essenciais que os/as estudantes têm de possuir para vir a ocupar um cargo de primeira linha nas empresas. O curso deverá não só fornecer bases técnicas que lhes permitam integrar as empresas, como desenvolver o processo de aprendizagem já com um ponto de vista muito prático e muito voltado para aquilo que é expectável que encontrem em contexto de trabalho. Na prática, tal como referido pelo entrevistado 1, "nós quando desenhamos este curso, e qualquer tipo de unidade que tenha a ver com segurança, que finalmente conseguimos incorporar noutros cursos, unidades de segurança, tem sempre a ver com as competências desejáveis pelo mercado".

Ao nível do plano de estudos, a articulação dos cursos com o mercado de trabalho prende-se, em termos concretos com as funções a exercer, com a criação de ambientes seguros para as redes empresariais, com a segurança nas empresas, com a procura de respostas aos desafios colocados em ambiente de trabalho, com a instalação e gestão de infraestruturas de redes locais, com a identificação e mitigação de ameaças às empresas. No final de todos os cursos CTeSP, há um estágio curricular que visa, precisamente, a integração nas empresas e o envolvimento nas atividades anteriormente descritas. Durante o estágio, o/a estudante mobiliza as competências adquiridas no curso, preparando-se para desenvolver a sua atividade profissional na primeira linha da segurança e administração de redes e sistemas, e reforçando a ligação dos cursos ao mercado de trabalho, como nos disse o entrevistado 4, "o último semestre é um estágio, o que significa que os estudantes nessa altura estão a realizar um projeto numa entidade de acolhimento, uma empresa, uma instituição", e o entrevistado 2 "foi o auscultar do mercado, dos nossos parceiros, porque o nosso CTeSP tem depois também um estágio profissional, 720h, e então nesse sentido há uma receptividade de algumas empresas nesta área."

Contudo, nem todas as empresas valorizam, ainda, a necessidade da cibersegurança, ou não possuem recursos para tal, como refere o entrevistado 3:

> *"Algumas empresas já o fazem, e quando estamos a falar de empresas que estão no mercado, estando em Portugal, já estão num mercado global, têm obrigações de* compliance *para isso, ou então, que já sofreram do seu próprio problema. Eu diria que atualmente andamos à volta dos 10%, 15% de empresas que já pensam nisso, já é muito bom. E temos, claramente, que dar o salto, 80% das empresas têm que fazer isso. É óbvio que nas microempresas será muito difícil, mas as médias e grandes têm que ter alguém dessa área, ou subcontratar alguém que os ajude a traçar esse caminho."*

Investigação e inovação

A componente de investigação acaba por não estar muito presente nestes cursos, uma vez que o que se pretende, como já referido, é a formação de profissionais que possam ser rapidamente integrados no mercado de trabalho. Desse modo, privilegia-se a aquisição de competências que permitam aos/às estudantes dar respostas às necessidades de primeira linha das empresas, e não desenvolver investigação numa determinada área da cibersegurança. Ainda assim, é importante destacar a presença de uma UC ligada à Gestão de Projetos, em que se promovem capacidades de conceber, desenvolver e implementar um projeto na área da cibersegurança. O projeto, a ser implementado em contexto de trabalho, funciona como uma forma de aplicar os conhecimentos já adquiridos. Em relação aos temas de investigação na área temática de cibersegurança, parece-nos relevante salientar que o entrevistado 3 refere a necessidade de pensar a investigação ao nível tecnológico, dos processos e das pessoas. Esta ideia é corroborada pelo entrevistado 1, quando refere que, "hoje em dia, tudo é digital e a partir desse momento o impacto

que tem um ativo mal protegido ou com uma análise de risco mal efetuada pode ter impacto diretamente no cidadão, até na sua integridade física". Ainda dentro deste ponto, o fator humano é frequentemente referido como fundamental para a investigação, nomeadamente a forma como os ataques e as vítimas pensam e a sensibilização que tem que ocorrer, junto dos/as cidadãos/ãs comuns, para estas temáticas. A questão dos processos de privatização e proteção de dados, bem como a articulação da técnica com o direito, também são identificadas como temáticas centrais. A nível tecnológico, e com uma vertente mais aplicada, isto é, mais relacionada com as empresas e com a futura utilização no mercado de trabalho, são referidas as seguintes: computação quântica, "digitalização robótica" (Entrevistado 1), "segurança das aplicações que devem ou têm de ter para que não sejam vulneráveis a ataques e alterações de dados" (Entrevistado 2).

O que resulta da análise é que as componentes técnica e de mercado de trabalho dominam a formação CTeSP em cibersegurança, uma vez que o objetivo destes cursos é a rápida integração no mercado de trabalho, fornecendo aos/às estudantes noções básicas e competências técnicas que lhes permitam integrar uma primeira linha nas organizações.

Licenciatura

A Licenciatura em Segurança Informática em Redes de Computadores é oferecida por um politécnico do setor público e é a única licenciatura oferecida em Portugal em cibersegurança e segurança de redes.

Formação técnica, ética e legal

A componente técnica é muito forte, quer no plano de estudos, quer nos objetivos do próprio ciclo de estudos. Desde logo, as áreas científicas com mais peso são as de "Tecnologias da Informação", "Engenharia de Computadores" e "Ciências da Computação". Além disso, é uma formação que assenta, sobretudo, nas áreas de Programação, com unidades curriculares como "Fundamentos da Programação"; Administração de Redes, com unidades curriculares como "Redes de Computadores I e II"; e Administração de Sistemas, de que são exemplo as UC de "Introdução aos Sistemas Computacionais" e "Sistemas Operativos", de resto como se pode constatar pela perceção do entrevistado 5, "conhecimentos básicos de programação (...), [é] importante tocar a componente de administração de redes (...) e a componente de administração de sistemas é outra das componentes que é importante". Além destas competências básicas em programação, redes e sistemas, pretende-se que os/as estudantes possuam competências técnicas e operacionais ao nível da segurança informática, tais como segurança de redes, segurança de sistemas e tolerância a falhas. Finalmente, outra vertente da formação tem que ver com o *pentesting* e *ethical hacking* (UC "Testes de Penetração e *Hacking* Ético"), Criptografia (UC "Criptografia Aplicada"), gestão da segurança da informação (UC "Sistemas de Gestão de Segurança da Informação") e análise forense (UC "Análise Forense Digital"), como diz o entrevistado 5, afirmando que a Licenciatura faz referência à

> "*segurança das redes, à segurança dos sistemas, aos sistemas redundantes, à tolerância a falhas. Estou a falar desse tipo de conhecimento que é fundamental. Às questões do* pentesting, ethical hacking, *saber exatamente executar os procedimentos, numa componente mais operacional e aí sim, por acaso na licenciatura... uma componente de sistemas de gestão de segurança de informação. Portanto, aqui entramos mais no campo da* governance."

Na componente da ética e do direito surge, na Licenciatura, uma UC designada por "Ética e Legislação Informática", onde se abordam, precisamente, as questões relacionadas com a legislação e a ética na área da informática. Relativamente à ética, é importante considerar que os/as profissionais vão ter acesso a dados e vulnerabilidades e, por isso, é essencial que sejam profissionais eticamente sólidos, conforme referido pelo entrevistado 5: "um profissional que atua nesta área tem obviamente que ter comportamentos éticos sólidos, porque vão ter acesso a vulnerabilidades, vão ter acesso a dados, que de certa forma têm que ser bem protegidos e não podem ser usados depois de má-fé" (Entrevistado 5).

A questão da legislação prende-se com a compreensão, quer dos requisitos a cumprir, quer das consequências por não os cumprir, e também as questões relacionadas com o RGPD e privacidade dos dados. É, assim, um conhecimento legal aplicado ao contexto de trabalho, isto é, quando estiverem a trabalhar na área, até onde é que podem ir para não ultrapassar os limites legais, quer da pessoa, quer da organização. Assim, tal como percecionado pelo entrevistado 5,

> *"a componente da legislação, também é fundamental para que eles percebam também as consequências, não só os requisitos a que as são obrigados. É essencial ter conhecimento daquilo que realmente é requerido que as organizações atendam; mas também depois a componente de consequências da sua parte, no caso de não atuarem de uma forma legal."*

As necessidades do mercado de trabalho

Outro ponto de destaque é a relação da formação com o mercado de trabalho, mais concretamente com o setor empresarial, uma vez que "o curso realmente está montado para responder a essas necessidades de trabalho" (Entrevistado 5). Esta relação pode verificar-se através da "ministração conjunta deste curso por professores da carreira académica e por especialistas que exercem atividades profissionais em empresas" (Entrevistado 5). Assim, assume-se que a formação criada é voltada para o mercado de trabalho, com uma forte componente prática, verificada pela aposta num modelo de estudo de "aprender fazendo", com recurso a "laboratórios de informática o mais possível semelhantes aos que se encontram no mercado de trabalho" (Entrevistado 5).

Apontando, agora, para o trabalho concreto a desenvolver dentro das empresas, a licenciatura, na perceção do entrevistado 5, visa formar profissionais para "auxiliar as empresas a lidar com o crescente número de ataques informáticos", procura reduzir o "esforço (monetário e temporal) de integração dos recém-licenciados no mercado do trabalho", bem como, e a um nível mais técnico, formar licenciados capazes de "desenvolver e testar *software* com princípios de programação segura, reduzindo assim falhas ao nível do *software* e evitando que estas sejam exploradas por *hackers* informáticos", ou seja, "o objetivo é mesmo preparar as pessoas para que, se são chamadas a uma organização, que sintam que têm as competências para executar esse trabalho" (Entrevistado 5).

Contudo, e como já referimos, nem todas as empresas entendem a necessidade de valorizar a cibersegurança nos seus negócios, como refere o entrevistado 5:

> *"O paradigma tem vindo a mudar, é certo. Mas eu acho que ainda há muito, muito a fazer. Eu entendo o lado das organizações na sua maioria, o negócio deles não é a cibersegurança, a cibersegurança é uma necessidade, e muita das vezes essa necessidade ainda decorre de um incidente. É, e ainda estamos nesse ponto. (...) Agora, se há assim um investimento mais efetivo, pelo menos por parte das PME, em termos de cibersegurança, em ter uma postura mais proativa, monitorização, deteção de incidentes e resposta a incidentes, ainda há um percurso a fazer."*

Investigação e inovação

Finalmente, a presença da componente de investigação acaba por não ser muito forte porque, tal como nos CTeSP, o objetivo do ciclo de estudos é a formação de profissionais que possam rapidamente integrar o mercado de trabalho. Assim, a licenciatura pretende fornecer uma formação em diversas componentes da área temática da cibersegurança para que, numa primeira fase, os/as estudantes possam integrar o mercado de trabalho e especializar-se naquilo que a empresa pretende ou, numa segunda fase, prosseguir para uma especialização de mestrado e, então aí, aprofundar mais, numa perspetiva académica e científica, um determinado tema. Concluindo, a licenciatura não privilegia a realização de investigação na área temática da cibersegurança, mas fornece algumas bases dessa mesma área temática para que, no futuro, os/as estudantes se possam especializar. Com efeito, com uma vertente aplicada, tal como referido pelos entrevistados 1 e 2 dos CTeSP a "junção de cibersegurança à componente data *analytics*" (Entrevistado 5), análise de vulnerabilidades nas plataformas que são lançadas, bem como a exploração dessas vulnerabilidades e, finalmente, "toda a parte de engenharia reversa, de *threat hunting*, caçadores de ameaças, de plataformas que permitam e facilitam essa busca" (Entrevistado 5) emergem como temas de investigação. Um último ponto também referido tem que ver com as organizações e a *governance*, uma vez que, "precisamos que as organizações tenham procedimentos mais bem definidos" (Entrevistado 5).

Mestrados

Os Mestrados na área da Cibersegurança e Segurança da Informação oferecidos em Portugal são 9, e são oferecidos quer pelo ensino universitário, quer pelo politécnico, tanto público como privado. A formação de Mestrado pretende ser um aprofundamento de conhecimentos na área da cibersegurança, a partir de um conjunto alargado de temáticas e, apesar de terem alguns pontos em comum, cada curso aborda questões específicas e diferentes. Por este motivo, a sistematização da análise focar-se-á em alguns pontos comuns de modo a caracterizar os Mestrados nesta área.

Antes de prosseguir para a referida análise, importa referir que os Mestrados de Cibersegurança e de Segurança de Informação são cursos de especialização, ou seja, pressupõem que já haja algumas bases técnicas de informática, que depois serão aprofundadas para a Cibersegurança. De facto, como refere o entrevistado 6, "o importante para mim é que realmente seja de uma abrangência multidisciplinar. Isso é um aspeto importante até porque o tipo de alunos que nós recebemos no mestrado oriundos de uma licenciatura é muito diversificado".

Formação técnica, ética e legal

A componente técnica é, tal como nos cursos CTeSP e na Licenciatura, dominante na formação dos Mestrados. Verifica-se que as áreas técnicas são as que têm mais peso no total de número de créditos ECTS. Os entrevistados afirmaram que, antes de mais, os/as estudantes devem possuir conhecimentos de Redes, Sistemas e Programação e que, num nível aprofundado de Mestrado, a Criptografia é fundamental, bem como a Criptografia aplicada à Cibersegurança. Outro aspeto fundamental da componente técnica dos Mestrados em funcionamento, e que foi referido nas entrevistas, é o desenvolvimento de competências de Gestão e Avaliação de Segurança Informática, do ponto de vista da confidencialidade, integridade, autenticidade e disponibilidade, bem como Sistemas de Deteção de Fraudes e Intrusões e de Avaliação e Gestão de Risco. As áreas de Fundamentos, de Infraestruturas e de Desenvolvimento de *Software* são, também, percebidas como fulcrais. A Administração de Sistemas, a Segurança das Redes

e a Análise Forense Digital são outras áreas que devem ser tidas em conta. Algumas UC que refletem estas áreas fulcrais de um mestrado em cibersegurança ou segurança da informação são, por exemplo, "Conceção e Desenvolvimento de *Software* Seguro", "Segurança em Sistemas de Informação", "Administração Segura de Sistemas Informáticos", "Criptografia Aplicada", "Análise e Exploração de Vulnerabilidades" ou "Análise e Gestão de Risco em Segurança Informática".

Em termos éticos e legais, o foco está no conhecimento desses mesmos aspetos, na sua relação com a Segurança da Informação, quer a nível nacional, quer a nível europeu. Pretende-se que os/as estudantes compreendam a linguagem jurídica e que utilizem os instrumentos legais, jurisprudenciais e doutrinais com relevância para a solução de uma questão concreta. Os conteúdos abordados são baseados nas questões de RGPD e da Privacidade e Proteção de Dados Pessoais. Apesar de ser uma questão que todos os diretores de curso entrevistados consideram central, a forma como é abordada nos diversos planos de estudo é diferente. Ao passo que alguns mestrados possuem UC específicas para trabalhar as questões éticas e legais (e.g. "Direito da Cibersegurança"), outros optam por abordar as questões legais de uma forma transversal, ou seja, abordar essas questões à medida que vão surgindo nas áreas mais técnicas e nas diferentes UC. Nesses casos, a opção foi que "essa vertente mais de Direito acompanhasse os conhecimentos que as pessoas têm na área de informática e não propriamente que fosse uma área distinta do resto do curso" (Entrevistado 6). Esta opção por uma abordagem transversal que evita UC específicas sobre questões éticas e legais deve-se, segundo os diretores entrevistados, a um esforço de aumentar a atratividade do curso, já que a sua perceção é que ter unidades curriculares de direito pode afetar a adesão dos/as alunos/as aos cursos, frequentemente oferecidos em escolas de engenharia.

Tendo isto em consideração, podemos concluir que o Direito é mobilizado de uma forma aplicada, ou seja, procura-se que os/as estudantes conheçam os aspetos legais da cibersegurança e as suas implicações, e que os possam mobilizar nas organizações, como é referido pelo entrevistado 11, que indica que, a "abordagem à legislação que é feita, [tendo em conta] os deveres e os direitos dos indivíduos, as implicações que cada ação relacionada com a cibersegurança pode ter para a prática profissional dos futuros profissionais" (Entrevistado 11). Algumas UC da área científica do Direito presentes nos mestrados são, por exemplo, "Direito da Cibersegurança", "Direito e Privacidade", "Direito na Segurança Informática e no Cibercrime" ou "Direito e Organização da Segurança".

As necessidades do mercado de trabalho

A componente do mercado de trabalho possui, também, uma forte presença na organização curricular dos mestrados a vários níveis, como se pode verificar pela identificação do principal objetivo, que na perceção do entrevistado 11 é o de "preparar profissionais, no sentido de lhes dar bases para poderem resolver determinada situação ou proporem determinada solução" (Entrevistado 11). Para começar, 3 entrevistados revelam que existe uma forte presença de representantes do setor empresarial, quer no desenho dos projetos curriculares, quer na participação em algumas aulas, o que indica, desde logo, uma relação estreita entre a formação académica e a sua relevância para o mercado de trabalho. De facto, o entrevistado 6 refere que "nós temos um conjunto de monitores empresariais que colaboram connosco em termos de cada UC (...) Portanto, eles são incorporados como monitores, como oradores convidados, mas não são docentes" (Entrevistado 6). Além disso, a ligação com o tecido empresarial das diferentes regiões é fomentada e reforçada através da colocação de estudantes como estagiários/as nas empresas, e levando a cabo projetos e seminários, assim facilitando um "contacto muito grande com o ecossistema de empresas", como refere o entrevistado 10.

Olhando agora para o plano de estudos, para os conteúdos e resultados de aprendizagem, há, desde logo, uma componente ligada à gestão e administração de empresas, ou seja, relativa ao desempenho de funções, dentro da organização, na área de Segurança Informática. Assim,

desenvolvem-se competências como a resolução de problemas e capacidade de trabalhar em equipa, gerir sistemas de comunicação de informação, bem como competências de tomada de decisão, de gestão de projetos nas empresas, a compreensão aprofundada dos aspetos organizativos dos centros de operações de segurança ou a transferência de conhecimentos para as organizações. Em termos técnicos, pretende-se que os/as graduados/as possam aplicar as competências adquiridas no mercado de trabalho, nomeadamente um conhecimento aprofundado nas várias temáticas abordadas, dotando-os/as de capacidades de liderança de equipas e implementação de projetos, de resto como é referido pelo entrevistado 12, "é uma área que também tem uma componente organizacional, de gestão de empresas, ou seja, como é que eu vou gerir a minha empresa de maneira a que seja segura".

Contudo, e também ao nível do mestrado, é notório que as empresas ainda não reconhecem, nem valorizam, a necessidade de ter ativos de cibersegurança nos seus quadros, como refere o entrevistado 6:

> *"Apesar de a cibersegurança ser um tema que está na ordem do dia, as próprias instituições empresariais não estão muito preparadas nem suscetíveis para elas. Porquê? Porque dizem que não trabalham na área de cibersegurança. O que me parece uma resposta um bocado estranha porque a cibersegurança atinge todas as organizações. Eles só vão precisar quando tiverem um incidente, mesmo em organizações com alguma dimensão, o que é claramente preocupante."*

Investigação e inovação

Finalmente, a componente de investigação tem uma valorização relativamente forte nos mestrados, uma vez que estes ciclos de estudo fomentam o desenvolvimento de capacidades de liderar equipas de investigação, de realizar investigação aplicada à cibersegurança ou de conceber soluções inovadoras nos domínios de redes e sistemas. Em termos curriculares, há unidades curriculares, como, por exemplo, "Metodologias de Investigação", "Fundamentos de Investigação Científica" e, posteriormente, a própria Dissertação, onde se trabalham as questões específicas de elaboração de um trabalho de investigação, desde a metodologia, à recolha bibliográfica, à estruturação do documento científico e à sua comunicação. Assim, os mestrados visam, além da componente de integração de líderes com conhecimentos profundos das temáticas da cibersegurança nas empresas, incentivar à realização de trabalho de investigação na área da cibersegurança com vista à inovação. De facto, a emergência da *governance*, já referida pelo diretor de Licenciatura (Entrevistado 5), é corroborada pelo entrevistado 10, quando refere que

> *"faz falta muita investigação e muito desenvolvimento para facilitar a vida a empresas mais médias ou mais pequenas. É preciso mais ferramentas para automatizar, é preciso mais coisas para simplificar. Faz muita falta trazer questões de segurança às empresas mais pequenas e médias, trazer ferramentas de automatização, de sistemas mais simples."*

Por outro lado, e referindo-se a um tópico que o entrevistado 3 sobre a investigação ao nível das pessoas identifica, o Entrevistado 11 corrobora a ideia, uma vez que considera fundamental proteger os/as cidadãos/ãs de ataques, principalmente num ambiente de "intensa circulação de dados pessoais, imagens, vídeos, documentos na Internet, nas redes sociais e nos sistemas públicos" (Entrevistado 11).

Doutoramento

O Doutoramento em Segurança da Informação é atualmente o único doutoramento em Cibersegurança e Segurança da Informação no país. Tal como fizemos para os outros graus, debruçamos a nossa análise nas componentes técnica e científica, da ética e de direito, do mercado de trabalho e de investigação.

Formação técnica, ética e legal

A componente técnica e científica é a componente mais presente na parte curricular deste doutoramento, tendo por objetivo o desenvolvimento de uma especialização aprofundada num determinado tema. Assim, há, desde logo, uma componente muito forte de Lógica e Computação, com UC como "Lógica e Verificação de Modelos", que visa fornecer conhecimentos sobre programação lógica e aplicá-la à verificação de *software* e *hardware*, "Teoria da Computabilidade, Complexidade e Informação", que pretende fornecer o domínio dos conceitos, das técnicas, dos resultados fundamentais e das aplicações significativas das teorias da computabilidade e da complexidade, e "Tópicos Avançados em Segurança da Informação", onde se pretende que os/as doutorandos/as estabeleçam contacto com este tema especializado de investigação.

Outra componente importante é a componente de Arquitetura e Sistemas Operativos, com UC como "Segurança Informática em Redes e Sistemas", que visa fornecer ao/à doutorando/a um conjunto de conceitos, metodologias e ferramentas de segurança de computadores e redes, que lhe permitirá abordar o tema da segurança no contexto de um conjunto de alargado tecnologias, e "Tolerância, Deteção e Resposta a Intrusões", através da qual se pretende que os/as estudantes conheçam os principais paradigmas, modelos e ferramentas para gerir intrusões em sistemas e aplicações distribuídas.

Finalmente, a componente de Programação também tem um peso importante, com UC como "Segurança em Linguagens de Programação", onde se pretende que os/as doutorandos/as dominem a aplicação de princípios de segurança em linguagens de programação, com ênfase no controlo do fluxo de informação, e "Modelos Computacionais em Segurança", que visa dominar os modelos computacionais de conceção e de análise de protocolos de segurança e perspetivar desenvolvimentos futuros.

A componente da ética e do direito, neste ciclo de estudos, é desenvolvida de uma forma transversal e não através de UC específicas, isto é, à medida que se vão abordando os conceitos técnicos, vai-se expandindo o conhecimento sobre as questões éticas e legais que determinado tipo de conteúdo técnico levanta. Não é, assim, dominante ou prioritária a discussão da legislação e das questões éticas, mas estas são abordadas no sentido de saber aquilo que se deve ter em conta quando determinadas questões, como a privacidade, são tratadas. Com efeito, na perceção do entrevistado 12, "acabamos por dizer: atenção que aquilo que nós estamos a ensinar é para fazer o bem, para proteger sistemas, no entanto algumas dessas coisas que ensinamos podem ser usadas para o outro lado. Não todas, há coisas que podem ser usadas de outra maneira, não para proteger, mas para atacar".

As necessidades do mercado de trabalho

A componente do mercado de trabalho/organizacional não parece ser tão relevante quanto nos restantes graus, como de resto seria expectável, pois o doutoramento, na perceção do entrevistado 12, "tem uma vertente muito científica e menos aplicada. Portanto, eu estaria a mentir se dissesse que nós nos preocupamos demasiado com as necessidades do mercado de trabalho".

Investigação e inovação

Finalmente, a componente de investigação é a mais relevante no doutoramento e é central na medida em que este grau visa proporcionar "formação sólida nas matérias relevantes para a investigação em segurança informática (...), o contacto com a frente de onda de investigação e desenvolvimento no domínio, bem como a realização de investigação com vista a contribuições originais significativas" (Entrevistado 12). Assim, pretende-se, fundamentalmente, "formar cientistas e pessoas que saibam a fundo um tema focado e que saibam investigar na área da cibersegurança e chegar a resultados profundos do ponto de vista científico e tecnológico" (Entrevistado 12).

Além do que já foi referido, algumas UC contribuem, precisamente, para fomentar essa investigação, quer ao nível do saber técnico específico, quer ao nível dos processos e procedimentos de investigação. A UC de "Tópicos Avançados em Segurança da Informação" visa, precisamente, o contacto com tema especializado de investigação em segurança da informação. Há, para além desta UC, uma forte presença nas outras unidades curriculares do desenvolvimento de competências que permitam desenvolver investigação nas áreas técnicas abordadas nessas mesmas unidades curriculares.

Há ainda uma UC de "Ensino e Divulgação Científica", na qual são abordados tópicos que incluem a preparação e lecionação de aulas, gestão do tempo, ensino em laboratório e/ou aulas práticas (resolução de problemas). São utilizados, como elementos de formação, a supervisão e a classificação de trabalhos de laboratório, a elaboração e classificação de trabalhos de casa e de testes e exames. Pretende-se desenvolver capacidade de comunicação útil em áreas como ensino, apresentações de trabalhos científicos e/ou técnicos, formação de carácter profissionalizante. Finalmente, há a UC de "Seminário de Investigação", que fomenta a realização de apresentações em eventos da especialidade, bem como que os/as doutorandos/as contactem com tópicos de investigação recente em Segurança de Informação.

CONCLUSÃO

A análise dos cursos/ciclos de estudo em Cibersegurança permitiu perceber que são as áreas científicas das Ciências Informáticas, da Segurança Informática e das Ciências da Computação aquelas que têm maior peso na estrutura curricular de CTeSP, Licenciatura e Mestrados. Marcando presença frequente, mas com um peso curricular baixo, estão as áreas científicas das Humanidades e mais especificamente a do Direito.

A caracterização dos cursos/ciclos de estudos na área de cibersegurança evidencia a preponderância das questões técnicas específicas e a valorização da presença, ainda que em muito menor grau, da ética e da componente legal. O foco na adequação às necessidades do mercado de trabalho é transversal (à exceção do Doutoramento), ainda que mais marcado nos níveis mais baixos de formação (CTeSP e Licenciatura). Existindo uma clara perceção de que o campo de atuação dos profissionais com formação em Cibersegurança está em expansão, ainda que haja muito a fazer ao nível da sensibilização, as dinâmicas de transformação desse mesmo mercado de trabalho, ligadas aos desafios e adaptações que as questões de cibersegurança parecem exigir, coloca as empresas e a sociedade em geral num contexto em que a investigação, a inovação e a capacidade de gestão da segurança e do risco, mais valorizadas nos Mestrados e Doutoramento, se tornam também essenciais.

O trabalho realizado explora de forma sistemática o ensino da Cibersegurança no que toca a ciclos de estudo conferentes de grau (Licenciaturas, Mestrados e Doutoramentos) e inclui ainda a análise dos cursos CTeSP, também oferecidos por instituições de ensino superior. A continuação do trabalho de análise e caracterização da formação em Cibersegurança em instituições de ensino superior poderia passar por incluir as perspetivas de estudantes, assim como por olhar para as ofertas das instituições ao nível da formação contínua, incluindo pós-graduações. Em ambos os casos, esse estudo necessitaria de um tempo mais alargado que esperamos venha a existir em estudos futuros.

PERSPETIVAS ATUAIS E FUTURAS SOBRE A FORMAÇÃO EM CIBERSEGURANÇA

A nível europeu, a Comissão Europeia[13] está determinada a implementar a Década Digital, até 2030, em torno de quatro pilares: as competências, as infraestruturas digitais seguras e sustentáveis, a transformação digital das empresas e a digitalização dos serviços públicos.

O presente estudo, ao traçar um retrato da educação e formação na área temática de cibersegurança, em Portugal, contribui para a articulação das estratégias europeia e nacional, no âmbito da prevenção, educação e sensibilização e da investigação, desenvolvimento e inovação, em linha com os pilares acima referidos.

A nível nacional, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, bem como os resultados do presente estudo, pedem atenção para a relevância da articulação entre as instituições e organizações posicionadas a nível nacional e a sua interação com as instituições envolvidas na formação e educação na área temática da cibersegurança. Por seu turno, ao nível institucional, a importância desta articulação coloca desafios ao futuro da educação e formação nesta área temática, que se aborda mais adiante.

No quadro de uma ***Cidadania digital: direitos e princípios para os europeus***, desenhada no âmbito da estratégia da Década Digital 2030, emergem a liberdade de expressão, de estabelecimento e de exercício de uma atividade *online*, a proteção de dados pessoais e da vida privada e a proteção da criação intelectual das pessoas no espaço *online*, como direitos digitais. Como princípios, destacam-se o ambiente *online* seguro e de confiança, a educação e competências digitais universais, os princípios éticos para algoritmos centrados no ser humano e a proteção e capacitação das crianças no espaço *online*.

Do ponto de vista da educação e da formação na área temática da cibersegurança, o reconhecimento destes direitos e a inclusão destes princípios colocam desafios adicionais aos níveis nacional, institucional e individual. Com efeito, a universalização das competências digitais e da educação e a partilha de princípios éticos para algoritmos centrados no ser humano, por exemplo, destacam a cibersegurança e a importância do retrato do presente estudo sobre a educação aos níveis pós-secundário e superior, evidenciando a formação dirigida a profissionais da área, sustentada em indicadores relacionados com: i) número de CET do ensino pós-secundário e de cursos/ciclos de estudo do ensino superior de cibersegurança e da área das Ciências Informáticas com UFCD e/ou conteúdos referentes à área de cibersegurança; ii) número de inscritos/as nos cursos/ciclos de estudo do ensino superior de cibersegurança e da área das Ciências Informáticas com conteúdos da área de cibersegurança; iii) número de diplomados/as dos cursos/ciclos de estudo do ensino superior de cibersegurança e da área das Ciências Informáticas com conteúdos da área de cibersegurança; iv) número de teses de doutoramento e de dissertações de mestrado em curso, ou concluídas, por sexo e por registo na área científica e tecnológica em apreço; e v) relevância das diversas áreas científicas para a estrutura curricular dos cursos/ciclos de estudo no ensino superior, medida pelo número de créditos ECTS.

Neste sentido, tendo em consideração a centralidade que os pilares da Década Digital 2030 e a promoção de uma cidadania digital vão assumindo, os desafios que se colocam à formação na área da cibersegurança coloca os organismos e as instituições de ensino superior no cerne do estabelecimento de parcerias efetivas de cooperação com os mercados de trabalho global, europeu, nacional e local, e com a sociedade.

De igual modo, os desafios institucionais colocam-se também no possível envolvimento dos '*stakeholders*' externos, posicionados a diferentes níveis, num processo conjunto de conceção de problemas e de soluções, no que diz respeito à implementação de projetos curriculares e de resultados de aprendizagem centrados na promoção de conhecimentos e desenvolvimento

[13] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt#proximas-etapas

de competências, que permitam aos/às graduados/as e profissionais a resolução de problemas inerentes a contextos de trabalho, de estudo, e societais diversos.

A nível nacional, mantém-se uma tendência de evolução positiva visível no aumento do número de cursos/ciclos de estudo de cibersegurança, sobretudo em instituições de ensino superior, bem como no aumento de inscritos, e permanecem elevados (quando comparados com anos anteriores) os números de diplomados/as e de dissertações de mestrados e de teses de doutoramento. O número de mulheres inscritas e diplomadas permanece baixo, fortalecendo a ideia de que é ainda importante reforçar políticas de aproximação das mulheres da formação e da profissionalidade nestas áreas. Em 2020/21, a oferta educativa ao nível do ensino pós-secundário e do ensino superior é constituída por 11 cursos/ciclos de estudo de cariz profissionalizante (incluindo um CET[14], nove CTeSP e uma Licenciatura) e 10 ciclos de estudo com características de uma formação altamente especializada (contabilizando nove Mestrados e um Doutoramento), que permite aos graduados gerir e transformar contextos de trabalho complexos e que exigem novas abordagens e estratégias. Esta informação é relevante, tendo em consideração que na Europa existe um problema de compatibilização das competências e da formação com as necessidades do mercado de trabalho[15], o que por vezes resulta numa secundarização dos sistemas educativos às necessidades percebidas do mercado de trabalho.

Com efeito, as perspetivas atuais sobre a formação em cibersegurança evidenciam que a formação técnica específica tem um peso muito forte em todos os cursos/ciclos de estudos. As áreas científicas predominantes em todos os graus são aquelas relacionadas com a Informática e, logo por aí, temos uma ideia sobre de que ponto de vista é que a formação superior em cibersegurança é abordada. Ao nível dos conteúdos, ou da construção de uma formação em cibersegurança, a base parte sempre das componentes de Redes, Sistemas e Programação, assim como alguns conceitos básicos de segurança, a saber: confidencialidade, integridade ou disponibilidade. Esta apresenta-se como a base técnica específica de uma formação em cibersegurança. A partir daqui o foco pode virar-se para vários níveis de especialização, entre os quais a Administração e Gestão de Bases de Dados, Criptografia, Análise Forense Digital, *Compliance*, *Pentesting* e *Ethical Hacking*, Identificação de Vulnerabilidades, Resposta a Incidentes, Tolerância a Falhas, Gestão da Segurança da Informação. A análise da formação em cibersegurança revelou, também, que as questões da ética e do Direito são muitas vezes referidas, aparecendo como parte da formação, mais frequentemente incluída de forma transversal nos currículos, incluída noutras unidades curriculares ou de formação. A esse nível, é transversal o foco na privacidade, na proteção de dados e RGPD. Mais ainda, trabalham-se bastante as questões éticas de forma aplicada, o que é indicativo da importância conferida ao saber agir respeitando as normas legais em contexto de trabalho. Assim, é necessário compreender que a cibersegurança é um campo que trabalha com dados e com questões sensíveis e, portanto, tem de existir uma conduta eticamente responsável no tratamento desses dados e o conhecimento, em termos legais, de como é possível movimentarem-se na realização do trabalho nas empresas. Olhando para as temáticas mais presentes nos cursos/ ciclos de estudo analisados, e tendo em conta até possíveis necessidades presentes e futuras do mercado de trabalho, podemos notar que há ainda algumas áreas da cibersegurança que parecem ter menos atenção (e.g. segurança de sistemas de produção industrial) e que haverá certamente desenvolvimentos futuros que serão importantes de acompanhar.

Relativamente à relação com o mercado de trabalho, a análise da formação em cibersegurança revelou que o foco nas necessidades do mercado de trabalho está muito presente, e que estas têm um peso muito grande nesta formação, desde logo porque existe o objetivo expresso de formar

[14] Esta oferta é multiplicada já que este CET, como mostrámos, é atualmente oferecido por diferentes entidades em múltiplas localidades

[15] https://www.cedefop.europa.eu/en/publications/8088.

ativos capazes de desempenhar as funções pretendidas de acordo com estas necessidades. Há uma ligação muito forte ao tecido empresarial, porque é com vista à integração no mesmo que a formação em cibersegurança, ao nível de CTeSP, Licenciatura e Mestrado é desenhada, ainda que com o intuito de desempenhar funções diferentes. Os CTeSP e a Licenciatura serão integrados numa primeira linha de ação, concretamente e de forma resumida, na administração de redes e sistemas, ao passo que os Mestrados terão, desejavelmente, funções de gestão de equipas e tomada de decisão. A relação entre academia e mercado de trabalho torna-se, ainda, visível no papel atribuído à realização de estágios, bem como pela influência das organizações na criação dos planos curriculares e na participação em algumas aulas. Contudo, a análise da formação em cibersegurança também mostrou que, na perspetiva dos diretores de curso/ciclos de estudo, nem todas as empresas têm capacidade, ainda, para recrutar pessoas para gabinetes de cibersegurança, quer seja por falta de recursos, quer seja porque ainda não valorizam a cibersegurança como área essencial de manutenção de uma empresa, só recorrendo à sua função depois dos ataques informáticos/cibernéticos acontecerem e não como modo de os prevenir. Assim, o caminho de valorização da cibersegurança como essencial para as empresas está ainda a ser percorrido. Esta questão é especialmente importante também quando se olha para a necessidade de articular a formação em cibersegurança com os pilares da Década Digital 2030, designadamente o das competências e o da transformação digital das empresas.

Do ponto de vista da formação avançada e da educação contínua, a combinação dos objetivos dos cursos e ciclos de estudo analisados com as orientações estratégicas institucionais de prosseguimento de estudos de licenciatura, mestrado e de doutoramento, inscreve-se num contexto europeu e nacional marcado pelas mudanças demográficas, pela pressão do mercado de trabalho e pelos desafios e oportunidades atuais da Década Digital 2030. A diferenciação da oferta educativa, abrangendo a educação contínua, ao mesmo tempo que tira partido das transformações digitais que potenciam o crescimento dos modelos híbridos de educação e formação presencial e a distância, contribui para a criação de cursos de educação contínua dirigidos a estudantes e profissionais da cibersegurança.

A nível individual, a adaptação às dinâmicas sociais, culturais, tecnológicas exigem a participação ativa digital dos/as cidadãos no desenho de experiências de aprendizagem que se revelem cruciais para os contextos de trabalho. Neste sentido, estas iniciativas podem contrabalançar a oferta educativa pré-determinada pelas instituições de ensino superior.

Estes desenvolvimentos fomentam uma visão do futuro relacionada com a expansão da área temática da cibersegurança que, ao ultrapassar os limites, por exemplo, da área científica das Ciências Informáticas, vista como uma 'disciplina', induz o crescimento da cibersegurança como uma área transdisciplinar. De facto, há indicadores relacionados com a estrutura curricular dos cursos/ ciclos de estudo e com a produção de dissertações de mestrado e teses de doutoramento que evidenciam que diversas 'disciplinas' confluem para a área temática da cibersegurança, potenciando a abertura dessas 'disciplinas' para a formação e educação em cibersegurança. Esta possibilidade permite formar e educar cidadãos/ãs capazes de acompanhar não só os desenvolvimentos na área tecnológica, mas também encontrar soluções para problemas complexos que emergem do confronto das 'disciplinas' e que nos dão uma visão mais alargada da natureza dos próprios problemas.

A análise da componente de investigação na formação em cibersegurança não está muito presente ao nível de CTeSP e Licenciatura porque o foco está totalmente voltado para o mercado de trabalho. Ao nível do Mestrado, acaba por estar mais presente porque, como é um nível de maior especialização, importa conhecer com mais profundidade os assuntos referentes à área temática da cibersegurança e porque há opção de se fazer dissertação em vez de estágio. No doutoramento, é a componente mais forte da formação. Esta componente é abordada, de forma geral, a dois níveis: o primeiro relaciona-se com a componente técnica e visa o aprofundamento

científico de um determinado tema. O segundo prende-se com a realização formal do trabalho, desde a pesquisa bibliográfica, estrutura formal de um trabalho, à sua posterior comunicação.

As perspetivas veiculadas pelos diretores de curso/ciclos de estudo sobre o papel da investigação revelam que esta se assume como um processo fundamental de conhecimento dos fenómenos e de problematização das realidades. Desse modo, as perceções dos diretores de curso permitem-nos sistematizar alguns dos temas mais relevantes de investigação na área temática da cibersegurança, por um lado, e, por outro lado, também se pode pensar em investigação aplicada, ou seja, o desenvolvimento de soluções que depois são utilizadas no mercado de trabalho. Além disso, a investigação potencia a inovação e a reflexão sobre processos, o que é fundamental quando se está a falar de uma área que é tão difícil de controlar e tão suscetível à ocorrência de ataques potencialmente nocivos para os/as cidadãos/ãs. Falando, precisamente, de potenciais ataques aos/às cidadãos/ãs, as questões de RGPD, de privacidade e proteção dos dados assumem-se como um fator fundamental no qual é preciso investir tempo e recursos, principalmente em formas de otimizar a privatização dos dados e proteger as pessoas de potenciais ataques. Neste sentido, vai também ao encontro da necessidade de investigação na área do direito da cibersegurança e da sua relação com a proteção de dados e RGPD. A nível tecnológico, e numa vertente mais aplicada, identificaram-se como áreas fulcrais o *blockchain*, a *machine learning* e inteligência artificial, análise de vulnerabilidades e a resposta a ataques. A nível empresarial, destaca-se a *governance* e o desenvolvimento de mecanismos que facilitem e definam os procedimentos das pequenas e médias empresas.

Por último, uma limitação do estudo prende-se com o facto de não ter sido possível incluir, por constrangimentos de tempo, outras perceções, designadamente de estudantes, graduados, docentes, *stakeholders* externos e representantes do mercado de trabalho de modo a alargar as perspetivas atuais e futuras sobre a formação em cibersegurança. As mesmas limitações de tempo e de acesso aos dados, não viabilizaram a comparação dos resultados deste estudo com outros de carácter internacional com objetivos semelhantes.

Cabe ainda referir que uma outra limitação deste estudo se relaciona com a qualidade da informação pública, uma vez que a informação sobre os cursos/ciclos de estudo muitas vezes não estava atualizada nas diversas plataformas consultadas, pelo que foi necessário fazer a triangulação dos dados relativos aos cursos/ciclos de estudo em funcionamento, de modo a garantir a confiabilidade dos dados analisados e sua validade científica. Apesar destes esforços, não foi sempre possível abranger as tendências nos últimos 5 a 10 anos. Por exemplo, no nível pós-secundário, pelo facto de a informação ser escassa no que se refere ao número de inscritos/as em CET, não foi possível perceber a distribuição entre homens e mulheres nos CET de cibersegurança.

A informação sobre os conteúdos da formação no ensino superior não facilita a sua consulta, pelo facto de a informação estar dispersa, ou ser inexistente nos sítios das instituições de ensino superior. Neste sentido, a otimização de procedimentos e de mecanismos de recolha de dados que permitam o desenvolvimento de estudos longitudinais é crucial para dar continuidade a este estudo.

NOTA METODOLÓGICA

Os procedimentos metodológicos utilizados privilegiaram a recolha e sistematização de informação publicada e/ou publicamente acessível. Para isso, foi essencial identificar as fontes dessa informação, avaliar a sua qualidade e utilidade para os objetivos em questão, e sistematizar os contributos que traziam ao estudo. Isto foi feito adotando uma lógica de continuidade com o que é proposto e apresentado no *Relatório Cibersegurança em Portugal – Sociedade 2021*, do Observatório de Cibersegurança. Desta forma, à data de 30 de novembro de 2021, foram utilizadas as bases de dados oficiais da Direcção-Geral do Ensino Superior (DGES) e da Direcção-Geral de Estatísticas da Educação e Ciência (DGEEC) nas quais se realizaram um conjunto de pesquisas com base nas palavras-chave. Foi, no entanto, necessário suplementar este trabalho recorrendo a outras plataformas oficiais, como a da Agência de Avaliação e Acreditação do Ensino Superior (A3ES) e a da Agência Nacional para a Qualificação e o Ensino Profissional (ANQEP), para alargar a informação recolhida, assim como para poder cruzar e sistematizar a informação encontrada. Foi a partir desses dados, como se explica de forma mais pormenorizada abaixo, que foi possível identificar e caracterizar os cursos/ciclos de estudo de cibersegurança de nível pós-secundário e superior, assim como explorar o lugar que a formação em cibersegurança ocupa noutros cursos da área da informática.

De forma a enquadrar a oferta formativa em cibersegurança, em Portugal, passa-se a apresentar a organização do sistema de ensino, indicando o nível de ensino, o grau que confere o ciclo de estudos, a duração, e o respetivo nível de qualificação, tendo em consideração o Quadro Nacional de Qualificações[16] (QNQ).

Nível de ensino	Não conferente de grau superior	Grau (ciclo de estudos)	Duração em número de créditos[17] e semestres	QNQ
Pós-secundário	CET (Diploma de Especialização Tecnológica)	–	–	5
Superior	CTeSP (Diploma de Técnico Superior Profissional)	–	–	5
	–	Licenciatura (1º ciclo)	180 a 240 créditos entre seis e oito semestres curriculares (universidades) 180 créditos e seis semestres curriculares (politécnicos)	6
	–	Mestrado (2º ciclo)	90 a 120 créditos entre três e quatro semestres curriculares	7
	–	Doutoramento (3º ciclo)	e.g., 60 créditos (parte curricular) 120 créditos (elaboração de tese)	8

Tabela 11: Organização do sistema de ensino para a oferta formativa em cibersegurança

[16] Portaria n.º 782/2009, de 23 de julho.

[17] O crédito é a unidade de medida do trabalho do estudante sob todas as suas formas, designadamente sessões de ensino de natureza colectiva, sessões de orientação pessoal de tipo tutorial, estágios, projetos, trabalhos no terreno, estudo e avaliação. Em Portugal, um crédito equivale a cerca de 27 horas de trabalho do estudante, cabendo, no entanto, a cada instituição de ensino superior, através de um regulamento próprio, estabelecer essa equivalência.

Em relação ao ensino pós-secundário, os Cursos de Especialização Tecnológica (CET)[18] são ministrados, desde 2016, exclusivamente por instituições de caráter não superior, designadamente Centros de Formação Profissional do Instituto do Emprego e Formação Profissional, Escolas Tecnológicas ou outras entidades formadoras acreditadas.

Ao nível do ensino superior, a formação em cibersegurança é oferecida pelas instituições de ensino superior universitárias (Licenciatura, Mestrado e Doutoramento) e politécnicas (cursos técnico superior profissional[19], Licenciatura e Mestrado), nos setores público e privado. No caso dos CTeSP, a formação deve ter em conta as necessidades de formação profissional na região em que as instituições se inserem. Estes cursos permitem aos seus titulares ingressar nos ciclos de estudo de licenciatura e de mestrado integrado, através de um concurso especial de acesso. Esta formação visa dar continuidade aos percursos de formação de caráter profissionalizante, bem como a inserção destes diplomados e diplomadas no mercado de trabalho.

Em relação aos ciclos de estudo, as reformas do ensino superior, na sequência da implementação do Processo de Bolonha, têm vindo a reforçar, desde 2006, o caráter binário do sistema educativo português. Os politécnicos oferecem graus, com base num primeiro ciclo com 180 créditos (3 anos), seguido de um segundo ciclo de 120 créditos. As universidades, por seu turno, oferecem um primeiro ciclo com 180 a 240 créditos e podem, também, oferecer mestrados integrados, em casos tais como Medicina, Ciências Farmacêuticas ou Arquitetura. Um mestrado integrado tem de 300 a 360 créditos (5-6 anos) e pode ser oferecido, apenas, pelas universidades, tal como o grau de doutor. Ainda no âmbito das reformas educativas desencadeadas pelo Processo de Bolonha, os graus conferidos no ensino superior são desenhados tendo em consideração os quadros europeu e nacional de qualificações. Estes referenciais, para o grau de licenciado, definem que o nível de conhecimentos deve ser aprofundado numa determinada área de estudo, o que implica uma compreensão crítica de teorias e princípios. O nível de aptidões deve ser avançado e os licenciados devem revelar a inovação necessária à resolução de problemas complexos e devem ser capazes de gerir atividades ou projetos técnicos ou profissionais complexos, assumindo a responsabilidade em matéria de desenvolvimento profissional, individual e coletivo. Para o grau de mestre, o nível de conhecimento deve ser altamente especializado e na vanguarda de uma determinada área, sustentando a capacidade de reflexão e a consciência crítica. As aptidões e atitudes são também especializadas para a resolução de problemas, integrando conhecimentos de diferentes áreas, por forma a gerir e transformar contextos de estudo ou de trabalhos complexos e a rever o desempenho estratégico de equipas. O grau de doutor é conferido aos que possuam conhecimento de ponta na vanguarda de uma área de estudo. As aptidões e atitudes estão a um nível mais avançado e especializado, incluindo a capacidade de síntese e de avaliação de problemas críticos na área de investigação ou de inovação, suportando a redefinição dos conhecimentos ou das práticas profissionais.

Para caracterizar os cursos de cibersegurança de nível pós-secundário e superior foi ainda necessário recolher os dados relativos aos objetivos, conteúdos e resultados esperados de aprendizagem das suas Unidades de Formação de Curta Duração (UFCD), no caso do nível pós-secundário, recorrendo ao Catálogo Nacional de Qualificações (CNQ) ou unidades curriculares (UC), no caso do ensino superior, recorrendo aos *websites* das instituições responsáveis pelos cursos e recolhendo os dados a partir das fichas de unidade curricular ou informação equivalente disponibilizada. Para os cursos de nível superior, foram ainda recolhidos dados através de entrevistas de diretores de cursos/ciclos de estudo de cibersegurança, importantes não só para complementar a caracterização dos cursos nesta área, como também para analisar os principais desafios que identificam, e o modo como percebem a relação desta área de formação com as necessidades do mercado de trabalho, a investigação e a inovação.

[18] Decreto-Lei n.º 88/2006, de 23 de maio.
[19] Decreto-Lei nº 74/2006, de 24 de março, alterado pelo D.L. nº 63/2016, de 13 de setembro e pelo D.L. nº 65/2018, de 16 de agosto.

Procedimentos para a recolha, sistematização e análise dos dados recolhidos sobre a formação de nível pós-secundário

No que respeita à formação de nível pós-secundário, a nossa análise foca-se nos assim designados Cursos de Especialização Tecnológica (CET). Com uma duração aproximada de um ano, estes cursos conferem o nível 5 de qualificação do Quadro Nacional de Qualificações (QNQ) e um Diploma de Especialização Tecnológica (DET).

Antes disso, porém, importa referir que, numa fase exploratória, a nossa pesquisa abrangeu também outras ofertas do ensino profissional, de nível secundário, como sejam Cursos de Aprendizagem e Cursos Profissionais, para jovens, e Cursos de Educação e Formação de Adultos (EFA).

Pesquisando no Portal da Oferta Formativa[20], pode perceber-se que, na área das Ciências Informáticas[21], existem 74 Cursos de Aprendizagem, 895 Cursos Profissionais e nenhum EFA – nesta área, bem entendido. Limitações de tempo e as dificuldades que o processo implicaria, dadas as singularidades do ensino profissional, fizeram-nos optar por não aprofundar, neste momento, a pesquisa sobre a presença de conteúdos formativos na área de cibersegurança em Cursos de Aprendizagem e Cursos Profissionais, embora nos pareça um trabalho que será importante realizar no futuro.

Com o que apurámos, de resto, é possível perceber que esta é uma área de profissionalização que toma como pessoas destinatárias preferenciais as/os jovens, em detrimento de pessoas adultas. Veja-se, a propósito, o elevado número de Cursos Profissionais (895 cursos, um número mais elevado até do que os 750 cursos na área da Hotelaria e Restauração, por exemplo), e a inexistência de Cursos EFA.

Dando seguimento ao enfoque da pesquisa, consultámos o *site* da DGES para obter informações atualizadas sobre os CET, nomeadamente aceder à lista de todos os cursos existentes, de todas as áreas de educação e formação, em Portugal, neste momento. Na primeira fase, e a partir desta base de dados, começámos por fazer a pesquisa nas designações dos cursos utilizando as palavras-chave: "cibersegurança"; "segurança informática"; "segurança de informação"; "segurança de redes" e "sistemas de informação", mencionadas no *Relatório Cibersegurança em Portugal – Sociedade 2020* (e novamente utilizadas no *Relatório Cibersegurança em Portugal – Sociedade 2021*), do Observatório de Cibersegurança. Desta pesquisa resultou uma base de dados de 117 CET, oferecidos por várias entidades.

Numa segunda fase, o objetivo foi verificar, nesta base de dados, a existência de cursos que consubstanciam a área da cibersegurança ou que a ela faziam referência no plano de estudos ou nos conteúdos programáticos. Com esta análise, percebeu-se que da lista constavam, por um lado, cursos que já não existiam, entidades que já não ofereciam esses cursos ou que já tinham encerrado e, por outro lado, cursos que, efetivamente, não continham tópicos ou temas relacionados com a cibersegurança. Este procedimento resultou num total de 52 ocorrências de CET (ver Apêndices I e II), 13 de Cibersegurança e 39 da área das Ciências Informáticas com conteúdos referentes à cibersegurança, oferecidos nas diferentes localidades do país, para posterior análise.

[20] Disponível em https://www.ofertaformativa.gov.pt/#/pesquisa-cursos-alunos, em 28 de outubro de 2021.

[21] As Ciências Informáticas (código 481) é uma área de educação e formação que pertence à área de estudo de Informática (código 48), que de acordo Classificação Nacional das Áreas de Educação e Formação (CNAEF), classificam os programas de formação, desde 2005 (Portaria nº 53, de 16 de março de 2005). No contexto da avaliação e acreditação dos ciclos de estudo do ensino superior, a A3ES, refere-se às áreas de educação e formação, como áreas científicas que organizam as estruturas curriculares dos ciclos de estudo.

Por fim, na terceira e última fase, e a partir da base de dados anteriormente construída, procedemos à identificação e análise de cursos que mencionassem cibersegurança na sua designação. Foi encontrado um CET – Curso de Técnico/a Especialista em Cibersegurança – que, em 2021, era oferecido por cinco entidades formadoras diferentes, em vários pontos do país. Posteriormente, dada a clara presença da área das Ciências Informáticas, a pesquisa focou-se na existência de conteúdos de cibersegurança em todos os planos de estudo dos CET da área de Ciências Informáticas, com base nas palavras-chave já mencionadas. Assim sendo, e com recurso à plataforma da ANQEP[22] e do CNQ[23], conclui-se que existem 3 CET oferecidos por 13 entidades formadoras, em diferentes locais do país, com 3 UFCD com conteúdos de cibersegurança e segurança informática.

Procedimentos para a recolha, sistematização e análise dos dados recolhidos sobre a formação de nível superior

Numa fase exploratória, a pesquisa relativa aos cursos/ciclos de estudo no ensino superior na área da cibersegurança foi realizada em duas bases de dados disponíveis para consulta pública: no sítio da DGES e da A3ES através de palavras-chave mencionadas no *Relatório Cibersegurança em Portugal – Sociedade 2020* (e novamente utilizadas no *Relatório Cibersegurança em Portugal – Sociedade 2021*), do Observatório de Cibersegurança, nomeadamente "cibersegurança"; "segurança informática"; "segurança de informação"; "segurança de redes" e "sistemas de informação". Nesta primeira fase, e com o cruzamento de informação entre as duas bases de dados já mencionadas, obteve-se um total de 68 cursos/ciclos de estudo distribuídos por CTeSP, Licenciaturas, Mestrados e Doutoramentos nas áreas científicas de "Eletrónica e automação", "Ciências informáticas", "Informática", "Informática - programas não classificados noutra área de formação" e "Segurança militar".

Numa segunda fase, e após uma análise preliminar dos 68 cursos/ciclos de estudo, identificou-se que a área de estudo mais presente é a de "Informática" e as áreas de educação e formação ou áreas científicas relacionadas. Desta forma, a pesquisa foi orientada de acordo com a Classificação Nacional de Áreas de Educação e Formação (CNAEF) e focada na área de estudo "48 – Informática" e nas áreas que a integram. Para este efeito, recorreu-se à consulta da base de dados da Direcção-Geral de Estatísticas da Educação e Ciência (DGEEC), onde é possível realizar a pesquisa através da área CNAEF. Desta pesquisa, obteve-se os seguintes resultados: 8 cursos/ciclos de estudos na área "480 – Informática"; 734 cursos na área "481 – Ciências informáticas"; 8 na área "482 – Informática na ótica do utilizador" e 25 na área "489 – Informática – programas não classificados noutra área de formação". Estas áreas de estudo correspondem às áreas científicas que estruturam o currículo dos cursos e ciclos de estudo do ensino superior.

Dos 843 cursos/ciclos de estudo até este momento identificados, e numa terceira fase da pesquisa, procedeu-se ao cruzamento das informações das três bases de dados indicadas – DGES, A3ES e DGEEC. De facto, grande parte dos cursos/ciclos de estudo encontrados na segunda fase da pesquisa já se encontram descontinuados pelas instituições de ensino superior ou não existe informação sobre eles. Após um processo de confirmação e de agregação de dados, foram identificados 325 cursos/ciclos de estudo oferecidos no ensino superior e foi criada uma base de dados que os carateriza por (1) tipo de ensino – universitário ou politécnico; (2) setor – público ou privado; (3) curso/grau – CTeSP, Licenciatura, Mestrado e Doutoramento; (4) Unidade Orgânica; (5) Distrito; (6) sítio eletrónico; (7) Cursos/Ciclo de Estudos; (8) Área científica de acordo com a CNAEF[24]; (9) créditos de acordo com o sistema europeu de créditos curriculares

[22] https://www.anqep.gov.pt/np4/home.html
[23] https://catalogo.anqep.gov.pt/
[24] Portaria nº 256/2005, de 16 de março.

(ECTS)[25]; (10) informações acerca da acreditação pela A3ES. Esta base de dados foi essencial para se poder pesquisar, caracterizar e analisar a presença de formação em cibersegurança em si mesma, como noutros cursos da área da Informática.

Considerando os 325 cursos/ciclos de estudos, verificou-se que a grande maioria (n=246) são congregados na área de educação e formação de Ciências Informáticas e, por isso, dada a relevância desta área a análise focou-se nestes cursos e ciclos de estudo. Foi ainda necessário, numa última fase, uma revisão para identificar quais destes teriam conteúdos relevantes na área de cibersegurança. Assim, foram identificados 109 cursos/ciclos de estudos desta mesma área que, posteriormente, foram analisados, recorrendo aos respetivos *sites*/fontes das instituições promotoras ou dos próprios cursos/ciclos de estudos e com base, mais uma vez, nas já mencionadas palavras-chave. A partir desta análise, foi criada uma nova base de dados com os cursos/ciclos de estudo de Ciências Informáticas (ver Apêndice III), que dá conta dos 109 cursos/ciclos de estudos, acrescentando as UC e conteúdos programáticos que fazem referência à "cibersegurança", à "segurança informática", à "segurança de sistemas informáticos" e à "segurança de redes".

Posteriormente, pesquisaram-se os cursos oferecidos no ensino superior que se referiam, especificamente, à "cibersegurança" e à "segurança da informação". Foram, assim, encontrados um total de 20 cursos de Cibersegurança: 9 CTeSP, 1 Licenciatura, 9 Mestrados e 1 Doutoramento. Identificados estes cursos/ciclos de estudo, procedeu-se à análise documental nos *sites* dos cursos, construindo-se uma base de dados onde se incluíam as seguintes informações: (i) tipo de ensino, (ii) setor, (iii) instituição, (iv) grau, (v) áreas científicas da estrutura curricular de cada um dos cursos/ciclos de estudo e o número de créditos ECTS de cada uma dessas áreas científicas, (vi) objetivos do curso/ciclo de estudos, (vii) identificação das UC e sua correspondência em relação áreas científicas, bem como o seu peso medido em créditos, e finalmente, (vii) os conteúdos programáticos, (viii) a bibliografia e os (ix) resultados da aprendizagem, expressos em conhecimentos, competências e capacidades, para cada unidade curricular[26]. Importa referir que esta última informação, ou seja, o programa e os resultados da aprendizagem, em alguns cursos/ciclos de estudo, não está disponível nos *sites* das instituições de ensino superior.

A par desta recolha e análise, e de forma a complementar a informação sobre os cursos/ciclos de estudo, procedeu-se à recolha de dados de inscritos/as no ano letivo de 2020/2021 e de diplomados/as no ano letivo de 2019/2020 nos cursos/ciclos de estudos de cibersegurança. A mesma recolha foi realizada para os cursos/ciclos de estudo da área de Ciências Informáticas que contêm conteúdos referentes à área da cibersegurança. Esta recolha foi feita através de duas bases de dados disponibilizadas pela DGEEC, nas quais ambos os grupos (inscritos/as e diplomados/as) se distribuem por diversas categorias, sendo que a destacada, neste caso, foi a referente ao número de inscritos/as ou diplomados/as por sexo. Neste sentido, o levantamento destes dados foi realizado através da aplicação de filtros, nas bases de dados, considerando as designações dos cursos/ciclos de estudo previamente analisados, mas também o tipo de ensino (politécnico/universitário), o setor (privado/público) e, ainda, o grau (CTesP/Licenciatura/Mestrado/Doutoramento). É, no entanto, importante salvaguardar que não foi possível a recolha de alguns dos dados pretendidos por não constarem nas bases de dados, tanto no caso dos/as inscritos/as como no caso dos/as diplomados/as.

Em seguida, e com o intuito de recolher mais informação que permitisse complementar aquela que já havia sido recolhida sobre os cursos/ciclos de estudo que vêm a dar corpo à área temática de cibersegurança, procedeu-se à realização de entrevistas aos diretores de curso dos 20 cursos de Cibersegurança do ensino superior. O guião das entrevistas (disponível no Apêndice IV)

[25] Decreto-Lei nº 74/2006, de 24 de março.

[26] As UC são unidades de ensino e de aprendizagem com objetivos de formação próprios e com resultados expressos ao nível de conhecimento, competências, habilidades, capacidades, atitudes e compreensão que um/a estudante obterá como resultado do seu envolvimento nos processos ensino-aprendizagem e que exprimem as qualificações associadas ao nível da qualificação.

foi construído com base em cinco blocos de temas que foram selecionados a partir da análise de conteúdo dos planos de estudos dos diversos cursos/ciclos de estudo, e pela leitura atenta de legislação e de documentos anteriormente produzidos pelo Observatório de Cibersegurança, de modo a procurar clarificar o ponto de situação da formação em cibersegurança, em Portugal, em diversos níveis de ensino. Os temas do guião das entrevistas são, assim, os seguintes:

- Cibersegurança: definição e objetivos;
- Questões Éticas, do Direito e das Ciências Sociais;
- Mercado de Trabalho;
- Formação em Cibersegurança;
- Investigação e Inovação.

Construído o guião, procedeu-se ao contacto com os diretores de curso, primeiramente, por intermédio do CNCS e, posteriormente, e mediante a disponibilidade dos possíveis entrevistados/as, foram realizadas as entrevistas, com recurso a uma plataforma digital. Entre novembro e dezembro de 2021, foram efetuadas 12 entrevistas com uma ampla representação dos cursos/ciclos de estudo, em termos de distribuição geográfica e de diversidade de instituições universitárias e politécnicas dos setores público e privado, permitindo complementar a caracterização dos cursos/ciclos de estudo e refletir sobre os desafios que se colocam à formação superior na área temática de cibersegurança.

Os dados recolhidos a partir dos planos de estudo e das entrevistas foram analisados com recurso a procedimentos de análise de conteúdo. Para tal, criaram-se categorias de análise, com base nos dados que nos são fornecidos pela análise documental, que procuram orientar a reflexão e sistematizar a informação recolhida, de modo a dar-lhe sentido e a possibilitar a discussão. Essas categorias de análise referem-se às seguintes componentes: (i) técnica, (ii) ética, direito e ciências sociais; (iii) mercado de trabalho/organizacional; (iv) investigação e inovação. Através destas categorias, analisámos os objetivos dos cursos/ciclos de estudos, bem como os conteúdos programáticos e resultados da aprendizagem de cada UC que os compõem. Além disso, utilizando as mesmas categorias de análise, analisaram-se as entrevistas aos diretores de curso, complementando a informação obtida nos planos de estudo, mas indo além disso, ou seja, permitindo-nos ter um olhar mais global do estado atual da formação em cibersegurança, em Portugal, e de perspetivas para o futuro, quer em termos da formação em si, da relação com o mercado de trabalho ou das possibilidades de investigação.

Nesta última fase, foi também construída uma base de dados sobre teses de doutoramento e dissertações de mestrado realizadas em Portugal, a partir da plataforma de Registo Nacional de Teses e Dissertações (RENATES)[27] que permite consultar os registos de teses de doutoramento desde 1970 e os registos de dissertações de mestrado desde 2013. Os termos de pesquisa incluíram as palavras-chave referidas mencionadas no *Relatório Cibersegurança em Portugal – Sociedade 2020* (novamente mencionadas no *Relatório Cibersegurança em Portugal – Sociedade 2021*), do Observatório de Cibersegurança, de resto, o mesmo procedimento para a construção das restantes bases de dados, “cibersegurança”; “segurança informática”; “segurança de informação”; “segurança de redes” e “sistemas de informação”, no campo “Todos os campos de texto” e foram devolvidos 92, 67 e 200 resultados para os três primeiros termos de pesquisa. Para os restantes, foram encontrados demasiados registos de acordo com os critérios indicados, tendo-se optado por analisar, apenas, os registos com os termos “cibersegurança"; "ciberespaço"; "segurança informática". A base de dados, depois de eliminados 22 registos pertencentes a mais do que um termo de pesquisa, é constituída por um total de 337 registos de teses de doutoramento e dissertações de mestrado, em curso ou concluídas.

[27] https://renates2.dgeec.mec.pt/

APÊNDICES

APÊNDICE I
→ Cursos de Especialização Tecnológica (CET) em Cibersegurança em Portugal

APÊNDICE II
→ Cursos de Especialização Tecnológica (CET) da área científica das Ciências Informáticas em Portugal

APÊNDICE III
→ Caracterização dos cursos/ciclos de estudos da área científica de Ciências Informáticas no ensino Universitário e Politécnico

APÊNDICE IV
→ Guião das Entrevistas a Diretores de curso/ciclos de Estudos

APÊNDICE V
→ Estrutura curricular dos cursos/ciclo de estudos de Cibersegurança em Portugal

A consulta dos apêndices encontra-se disponível no *website* do CNCS – Observatório de Cibersegurança